Swift, Andrew

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Friday, January 27, 2012 6:54 AM
To: CTEC
Subject: FW: CCRIC CF12-001 Collectif d'hacktivistes Anonymous – Attaques par déni de service distribué (DSD) en rapport avec le droit d'auteur et la propriété intellectuelle

Categories: ATI PRINT

Classification: UNCLASSIFIED

(English version previously sent)

CTEC expedie le CCRIC BULLETIN CYBERNÉTIQUE CF12-001 Collectif d'hacktivistes Anonymous – Attaques par déni de service distribué (DSD) en rapport avec le droit d'auteur et la propriété intellectuelle

Pour signaler les incidents touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à l'adresse suivante : ctec@cse-cst.gc.ca

Tout ministère du gouvernement qui soupçonne avoir été touché par un incident lié à cette activité est prié de fournir un rapport écrit au CECM-GC.

http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf

Subject: CCRIC CF12-001 Collectif d'hacktivistes Anonymous – Attaques par déni de service distribué (DSD) en rapport avec le droit d'auteur et la propriété intellectuelle

==========
CCRIC – Bulletin cybernétique CF12-001
Date : 26 janvier 2012
==========

PUBLIC CIBLE
==========
Ce bulletin cybernétique est destiné aux professionnels et aux gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales, ainsi que des industries à infrastructure critique et autres industries connexes.

Titre
====
Collectif d'hacktivistes Anonymous – Attaques par déni de service distribué (DSD) en rapport avec le droit d'auteur et la propriété intellectuelle.

Détails

=====

On a porté à l'attention du CCRIC une série d'attaques coordonnées par déni de service distribué (DSD) contre des cibles internationales, y compris des organisations gouvernementales et des entreprises du divertissement dont les efforts sont axés sur l'adoption de lois protégeant le droit d'auteur aux États-Unis, comme la Stop Online Piracy Act (SOPA) et la Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA), ainsi que de l'Accord commercial relatif à la contrefaçon (ACRC).

Il appert qu'Anonymous, un collectif hétéroclite d'« hacktivistes », a annoncé que des attaques seraient portées en réponse à la fermeture de MegaUpload, un site d'hébergement et de partage de fichiers, et aux projets de loi sur le trafic de matériel protégé par le droit d'auteur et de marchandises contrefaites que s'apprêtent à adopter les États-Unis. Des attaques qu'ont signalé par la suite les médias visaient diverses organisations gouvernementales déjà engagées dans le processus de ratification de l'ACRC, à savoir les gouvernements d'Irlande et de Pologne.

[redacted]

De l'information diffusée récemment [redacted] laisse entendre que des hacktivistes surveillent de près la position du Canada. Le gouvernement fédéral souhaite en effet amender la Loi sur le droit d'auteur avec son projet de loi C-11, la Loi sur la modernisation du droit d'auteur, encore à l'étude au Parlement.

[redacted]

Page 3

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

La sélection des cibles, le lancement synchronisé des attaques et d'autres activités liées à ces dernières sont souvent coordonnés par le truchement de sites de média social ou de forums en ligne.

À l'heure actuelle, le CCRIC ne détient aucune information ayant trait à des attaques DSD concrètes contre des organisations du Canada. En revanche, il se peut que des adresses IP dont l'origine peut être retracée au Canada ont servi à lancer les attaques déjà signalées et qu'elles pourraient être de nouveau exploitées dans le même dessein.

Atténuation

Le CCRIC presse les organisations gouvernementales et les entreprises, qui participent de près à la modification de la Loi sur le droit d'auteur et dont les principales activités sont axées sur le matériel qu'elle protège, d'évaluer les risques d'être exposées à des attaques DSD, telles que les décrit le présent document, et de mettre en place les statégies d'atténuation nécessaires pour y faire face.

Différentes stratégies d'atténuation permettent de contrer ces attaques en fonction de leur type et de l'infrastructure de réseau ciblée. En règle générale, la meilleure défense consiste à s'y préparer à l'avance, ce que permet de faire la liste de contrôle suivante :

Préparation

1. Identifier les ressources matérielles les plus cruciales et les services dont elles assurent la prestation.
    - Les derniers correctifs ont-ils été installés?
    - Exécutent-elles des services inutiles comme Telnet, FTP, etc.?

2. De concert avec le fournisseur d'accès Internet (FAI), établir des procédures pour connaître l'étendue du soutien qu'il peut apporter à l'organisation lorsqu'elle fait l'objet d'une attaque DSD. Savoir s'il existe un accord sur les niveaux de services (ANS) et connaître les coûts à assumer.

3. Dresser la liste des personnes-ressources du FAI que l'on peut joindre en tout temps, ainsi que des autres moyens de communiquer avec elles.

4. Bloquer tout trafic qui présente des signes évidents d'usurpation d'identité (p. ex., les adresses IP à l'intérieur du réseau de l'organisation qui ne devraient pas être associées à du trafic entrant ou sortant). Instaurer une liste de filtrage Bogon (plage d'adresses non allouées) au périmètre du réseau.

5. Établir des procédures sur la façon de cloisonner les réseaux de l'organisation en cas d'attaque DSD. Se servir des appareils existants, comme les routeurs et les commutateurs gérés, pour s'en protéger. Dans la mesure du possible, configurer les routeurs du périmètre pour filtrer les services afin de réduire la chargeimposée aux dispositifs de sécurité, tels les pare-feu, qui analysent le trafic.

6. Désactiver tout service inutile et bloquer tout accès non autorisé vers et depuis les hôtes critiques identifiés précédemment.

7. Créer une liste blanche des adresses IP source s'il est nécessaire d'établir un trafic proritaire durant une attaque.

8. Documenter la topologie de réseau, y compris toutes les adresses IP. Tenir cette information à jour.

9. Passer en revue plan de continuité des opérations (PCO) de l'organisation et s'assurer que la haute direction et le service du contentieux comprennent bien ce qu'est une attaque DSD et les rôles et responsabilités qui leur sont dévolus.

10. Comprendre ce que constituent des conditions normales. Établir le niveau de référence du trafic sur le réseau, de la charge de travail imposée aux processeurs, de l'utilsiation des connexions et de la mémoire des hôtes essentiels en situation normale afin que les outils de surveillance du réseau entrent en œuvre lorsqu'une variation anormale se produit.

11. Reconnaître que l'organisation peut être attaquée. Solliciter la direction afin d'obtenir son approbation en vue d'élaborer et de mettre en œuvre des politiques, plans et procédures pour se défendre contre les attaques DSD. Identifier et obtenir les ressources nécessaires pour mettre en œuvre ces politiques, plans et procédures.

12. Attribuer les rôles et responsabilités. Connaître les intervenants dans la défense contre les attaques DSD et s'assurer qu'ils sont au fait de cette responsabilité. Ces personnes devraient appartenir au personnel affecté aux fonctions opérationnelles essentielles, aux opérations de TI, à la sécurité des réseaux et des TI, au service du contentieux et aux relations publiques. Tenir à jour la liste des points de contacts primaires et secondaires. Le réseau étant susceptible d'être en panne, y compris les appareils mobiles, mettre également en place d'autres mécanismes de communication.

13. Effectuer des exercices. Ce n'et plus le temps de faire l'essai des plans et des procédures lorsqu'une attaque se produit.

Identification
****

1. Savoir si l'orgaisation est une victime ciblée ou accidentelle.

2. Comprendre le déroulement logique de l'attaque.

3. Déterminer le trafic dont se sert l'attaquant en identifiant les adresses IP, les ports et les protocoles qu'il exploite.

4. Envisager de recourir à des outils d'analyse du réseau pour déterminer le type de trafic qu'exploite l'attaquant (p. ex., TcpDump, Wireshark, Snort)

5. Consulter les journaux disponibles du serveur pour comprendre la fonctionnement de l'attaque et les cibles visées.

6. Aviser le personnel concerné, notamment celui de la haute direction et du service du contentieux.

Confinement
****

1. Communiquer avec le FAI pour mettre en place un mécanisme de filtrage du trafic.

2. Bloquer le trafic le plus près possible du réseau en nuage (p. ex., avec un routeur, un pare-feu, un équilibreur de charges).

3. Changer l'adresse IP de l'hôte ciblé par l'attaque. Il s'agit là d'une solution provisoire.

4. Si l'attaque vise une application en particulier, envisager sa désactivation.

5. Identifier et corriger la vulnérabilité ou la faiblesse du système qui est exploitée. Il peut s'agir par exemple d'un service inutilisé maintenu involontairement en activité sur un dispositif destiné au public ou d'un système d'exploitation dont les correctifs n'ont pas été installés.

6. Mettre en place un mécanisme de filtrage en fonction des caractéritiques de l'attaque, par exemple le bocage des paquets IMCP Echo.

7. Limiter le trafic de certains protocoles à un nombre quelconque de paquets par seconde ou en n'autorisant l'accès des paquets qu'à certains hôtes.

Reprise des services
****

1. Confirmer que l'attaque DSD a pris fin et que les services sont de nouveau disponibles.

2. Confirmer que le niveau de performance de référence des réseaux est rétabli.

3. Au besoin, installer les correctifs et les mises à jour sur les machines touchées.

4. Dansla mesure du possible, identifier l'origine de l'attaque. Solliciter l'aide du FAI.

5. Passer en revue les registres de journalisation pour y repérer la trace des tentatives de reconnaissance. Conserver ces registres en vue d'éventuelles poursuites judiciaires.

Leçons retenues
****

Rédiger ou mettre à jour les documents suivants :

- Procédures d'opération normalisées
- Procédures d'opération d'urgence
- Plans de continuité des opérations

Consultez les références ci-dessous pour en apprendre davantage sur les activités du collectif Anonymous, l'outil LOIC servant aux attaques DSD, le projet de loi C-11 et le déni de service distribué.

Références :
http://www.us-cert.gov/current/index.html#anonymous_activities (en anglais) http://www.us-cert.gov/cas/tips/ST04-015.html (en anglais) http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html (en anglais) http://isc.incidents.org/diary/Javascript+DDoS+Tool+Analysis/12442 (en anglais) http://nakedsecurity.sophos.com/2012/01/20/anonymous-opmegaupload-ddos-attack/ (en anglais) http://www.channelregister.co.uk/2012/01/24/anon_attacks_poland_over_acta/ (en anglais) http://www.reuters.com/article/2012/01/25/ireland-web-attack-idUSL5E8CP1VU20120125 (en anglais) http://www.reuters.com/article/2012/01/23/idUS426379616120120123 (en anglais) http://www.michaelgeist.ca/ (en anglais) http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/acta-acrc.aspx?lang=fra&view=d (en français) http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5144516&file=4 (contenu bilingue)

Note cruciale :

Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à avertir le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique, notamment l'exploration, le téléchargement, le balayage, ou même une recherche Web selon tout texte du présent rapport.

Signalement
==========

AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu

par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Le présent message et toutes les pièces jointes qui l'accompagnent contiennent des renseignements qui peuvent avoir été recueillis de diverses sources externes dont le CCRIC ne peut vérifier ni la fiabilité ni l'intégrité. Le CCRIC n'assume aucune responsabilité pour des conséquences négatives résultant de l'utilisation des renseignements fournis dans la présente.

Les liens vers d'autres sites Web ne relevant pas du gouvernement du Canada sont fournis aux utilisateurs uniquement pour des raisons de commodité. Le gouvernement du Canada n'assume donc pas la responsabilité de l'exactitude, du caractère actuel ni de la fiabilité de leur contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites et leur contenu.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Miller, Kevin

From: Miller, Kevin
Sent: Tuesday, February 14, 2012 10:01 PM
To: COMDO
Subject: Fw: Contentious Tweets

Categories: Green Category

Here is the email JT sent out this afternoon, if the below is similar to what u have captured then go ahead and send to Andrew. If not, then send what u have to JT and we will send with the morning batch @ 11am.

Sry for any confusion, saw AS was cc'ed on ur email so I figure he's expecting it now.

Let me know if u have any questions, I will be available if u need me.

Tks Adam,
K
Kevin K. Miller
Communications Manager | Gestionnaire de Communications

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone : 613-949-9218

Fax | Télécopieur : 613-954-6048

Email | Courriel : Kevin.Miller@ps-sp.gc.ca

From: Turner, Jessica
Sent: Tuesday, February 14, 2012 02:10 PM
To: Swift, Andrew
Cc: Miller, Kevin; Brennan, Nicholas Adam; Chomyshyn, Nicholas; COMDO; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Orton, Karolina; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica
Subject: Contentious Tweets

MINISTER / MINISTRE

kayoazuL
a little bit of nepotism on the side with your fascism vic toews ca.vlex.com/vid/wife-local... #cdnfascism #cdnpoli

kayoazuL 12:55pm via Twitter for Mac
vic toews conflict-of-interest non-disclosure ca.vlex.com/vid/mp-s-pensi... #cdnfascism #cdnpoli

kayoazuL
black gold b***h! a mountain of s**t on vic toews ca.vlex.com/tags/vic-toews... #cdnfascism #cdnpoli

kayoazuL
"Vic has a long tradition of using the Free Press as a villain," endprohibition.ca/group/endprohi... #cdnfascism #cdnpoli

kayoazuL
vic toews in contempt of parliament should be serving time in jail along with stephen harper sixthestate.net/?p=1156 #cdnfascism #cdnpoli

kayoazuL
Vic Toews at a gay bath house wickedclub.com/index.php?opti... #cdnfascism #cdnpoli

___Danno
Did you know Vic Toews, Family-Values Minister fornicated & cheated on his wife & had a child through his much younger girlfriend? #cdnpoli

Polonoscopy
In 2007, Vic Toews cheated on his wife to impregnate a 25 year old, so, so if anyone is "with" the child pornographers.... well...

minasmusings
Never trust a tightass in an overpriced suit. -- Mr. Morality Vic Toews in adultery scandal - goo.gl/yU2Bc

kayoazuL
and yet more dirty vic toews enmasse.ca/forums/viewtop... Mr. Morality Vic Toews in adultery scandal #cdnfascism #cdnpoli

kayoazuL
some dirt on vic toews bit.ly/xY9jXi #cdnfascism #cdnpoli

GinaPhillipsSNN
Ton of Twitter hate for Vic Toews' "Lawful Access" bill, tabled today. Trending all day! That's a lot of child porn supporters... #cdnpoli

0lddutch
Toews: Current privacy laws allow pornographers and organized crime to flourish. Me: Just like our drug laws eh Vic?

skoods
Vic Toews is a buffoon. How dare you name this legislation "protecting children from internet predators act" trying to mask its real intent.

phoneyman
Vic Toews - I'm happy with some of the things this Conservative govermnent has done, but I'm unhappy to be accused of being a child predator

PopeShakey
It seems Vic "Child Pornography" Toews can't go a single week without claiming anyone who opposes him supports child porn. #cdnpoli

skoods
I can't tell if Vic Toews is intentionally deceiving people or simply ignorant.

ry_mccarthy
I'd like Vic Toews to tell me to my face I stand in support of child pornographers, so I can promptly deck him in his. #cluelesspolitics

RealDerekB
Vic Toews brings to table thought police, warrantless searches and taps all in the name of Free--err, 1984.

IceManCeaser
Vic Toews has crossed the fn line. Ppl that dont want to be spied on are "standing with child pornographers" What a piece of s**t #Canada

PereJules
Whenever Vic Toews is in the news, it's never good news. #canadapoli #d****ebag

WillYouBeConned
@ToewsVic Vic Toews - proving time travel is possible. #cdnpoli #Sleazeball #DangerMinister

Ken_Donnelly
You are for letting gov't spy on your every online move, or you are for pedophiles. Vic Toews = idiot. #smartlikeGeorgeBush #cdnpoli

RealDerekB
Vic Toews' "good intention" is child porn, which will do nothing but give more police more broad powers. Old f**k needs to learn from G20.

RealDerekB
Vic Toews won't just be f****g kids, he'll be f****g everyone with his Nazi style demonizing of opposers to fascist PATRIOT style acts

ExpletiveCa
Vic Toews released on good behavior. Applies to be crossing guard. Says those who don't stop at crosswalks are for child porn. #cdnpoli

RealDerekB
Vic Toews needs to stop reading Nazi-era Goering's playbook and painting everyone who doesn't agree with police abuse as "child predators."

quinkster
Vic Toews will police the internet and hunt down child pornographers as soon as he finds the "any" key.

ExpletiveCa
Vic Toews disappointed with prison food, but likes showers. Has wife smuggle in Gerbil for party with cellmate. #cdnpoli

scottbrooks
Vic toews is rather stupid and short sighted on his pushing for warrantless access, back doors into the fabric of canadian liberties. #idiot

ExpletiveCa
Judge says search of Vic Toews computer violates rights. Vic says judge is for child porn. Sent to mandatory 25 years for contempt. #cdnpoli

HayeseLaw
Vic Toews to libertarians: Go to hell natpo.st/zKGHiF #awfulaccess When the National Post abandons the #CPC on an issue, big problem.

Ethereal_Sleep
Alright, Vic Toews. Let me look at everything you've accessed on the internet, as privacy apparently means nothing to you. #scumbag

DocLockwood_SQL
Vic Toews is -in my opinion- the worst kind of politician. Any party backing @ToewsVic or spewing his crap will NEVER EVER have my vote.

oneguycoding
Vic Toews, typical conservative d*****baggery.

august_mk
Will Larry Miller tell Vic Toews what 1930s political entity supported spying on its citizens. *Hint Hint, Nudge Nudge* #CDNPoli

Marty_Chan
"Vic Toews said you stand with child pornographers" || Taken out of context. I meant to say NAZI child pornographers

Marty_Chan
Vic Toews's next claim: "If you don't like ice cream, you stand with the child pornographers." #cdnpoli

BruinBrewin
@ToewsVic vic #toews Any mental simpleton can make Bush-era doublespeak. Well done Toews. You've done Canada proud. Crawl under your rock.

AnthonyFloyd
Vic Toews's contention that we accept warrantless violations of our privacy or we're "with the child pornographers" is fear-mongering s***e.

ExpletiveCa
Vic Toews charged with stalking Neil Patrick Harris. Faces mandatory 25 years. Practices ankle grabbing. Gerbil still no comment. #cdnpoli

matt_gagner
Vic Toews disgustingly compares those who champion online privacy rights as being on the side of child pornographers. Shameful. #cdnpoli

WinnipegFatArse
Hey Vic Toews, those of us with nothing to hide bloody well have a right to be left alone! #cdnpoli #dueprocess

soundtheseventh
According to Vic Toews, if I don't agree with my phone's location being tracked by the cops without a warrant, I support child porn

ExpletiveCa
Cops find Doogie Howser reruns on Vic Toews computer. Semen on mouse sent for analysis, looked frothy and mixed with fecal matter. #cdnpoli

craddo
Your obsession with Justin Beiber is so "Vic Toews-y" #canadawrites

RFAgMTZE
@CharlieAngusMP @MarcGarneau Someone ought to read Vic Toews' browser history on-record in the Commons and see how he likes it #C30.

antimatter7
"Vic Toews" is the guy who would never give your balls back from his yard when you were a kid.

Sporked
If Vic Toews is right, Stockwell Day supports child pornography. cbc.ca/news/canada/st...

Edmonton_Eh
Hey Vic Toews, you're an idiot, track that lil message without a warrant... #fail #CPC

etownbudsfan
@wapimaskwa69 Vic Toews sure brings up child porn a lot. I think the public should be given full access to his internet history.

RobTeszka
F**k you, Vic Toews, and f**k the rest of the Harper government. cbc.ca/news/technolog... #fascistcanada

ExpletiveCa
Vic Toews stands with a look of half contempt and half constipation, you're all child pornographers who I'd like to torture. Kinky. #cdnpoli

G_Williams_CA
More lunacy from Vic Toews, this gov outdoes itself each and every day in the idiotic rhetoric department bit.ly/yROOMK #cdnpoli

TelegramDaniel
Having to choose between aligning yourself with Vic Toews or with child pornographers sounds like a punishment on some level of hell.

ALL_CAPS
It does give me some satisfaction that 'Vic Toews' and 'child pornographer' are now inextricably linked on Google. #cdnpoli

BaribeauP
Vic Toews already doesn't need a warrant to find out that I think he's a terrible human being. #cdnpoli

themanpanda
MP Vic Toews can't figure out how to play a DVD, but is drafting Internet legislation. Somebody stop the Tories. #invasionofprivacy

mode23
vic toews: a man with no intelligence, insulting the intelligent. #cdnpoli

ExpletiveCa
Happy Valentine's Day Vic Toews. I hope pictures of you and Cupid don't wind up on your Facebook wall. That would be ironic.

bmupton
According to Vic Toews if I object to my government surveilling me, I'm no better than a child pornographer. F**k you, Vic Toews.

letmelive_
vic toews, go f**k yourself and your stupid bill proposal. #freecanada

cabernar
Jesus Christ, Vic Toews.

gagnonshayne
Thumbs up Vic Toews, moé je suis de ton bord et pas du bord des gauchistes pédophiles. cyberpresse.ca/actualites/que...

ExpletiveCa
@ToewsVic Vic Toews can eat a bag of baby d***s. Last I checked, free speech was still legal, but only until next Monday.

Topkasa
According to Vic Toews, either you support the erosion of privacy rights, or you support Child Porn. Go f**k yourself, Vic.

_AnonymousOne
How awesome would it be if Anonymous Got Dox on Vic Toews?

Spookylish

The Tories want to violate online privacy rights & anyone who disagrees is aligned with child pornographers. Vic Toews is my #C**tOfTheDay.

peterisfunny
Old, white MP Vic Toews can't figure out how to play a DVD, but is drafting Internet legislation. Somebody stop the Tories. #VicToews

Edmonton_Eh
Vic Toews: "You can stand with us, or you can stand with the child pornographers." You sir, are a special kind of moron #CPC

Beari8it
"Vic Toews confessed to being a pederast." thestar.com/opinion/editor... #cdnpoli

ExpletiveCa
Vic Toews can't scare people with terrorists anymore, pity no attacks, so if you value privacy you now support child porn.

perkinz
What the f**k does Vic Toews know about 21st century technology?

datalaundry
we should force Vic Toews to resign over what he said today. what a scumbag. tactics like that should not be accepted.

rogkicksass
@ToewsVic Track this communication. F**k You Vic Toews.

EmAvon
Nice try, Vic Toews.

ColeMFHoward
#ifyouaresingle you are probably a child pornographer. Thanks Vic Toews, you really opened my eyes to how f**king horrible we all are! <3

ExpectUsCanada
@ToewsVic Office numbers: Ottawa: 613-992-3128, Steinbach 204- 326-988, 204-345-9762. Do it - take a minute & call.

ExpectUsCanada
Please Call And Let @ToewsVic Know Your Not A Child Pornographer #F**kVicToews Search His Computer

RobertJensen2
The infantile comments of @ToewsVic yesterday in the HOC were an embarrassment to parliament, to Canada and to himself. #Toews

thelieisacake
@HarrisAJackson @ToewsVic The first duty of the Harper Government is the protection of Conservative power and control, not the citizenry.

TheUselessCoin
Maybe Vic Toews has a faulty Bible. The one I have is pretty tough on adultery & lying, but says zip about child porn. #cdnpoli #harpercrite

captainpearson
Wait, I'm coming to this story kind of late...did Vic Toews finally admit to being a child pornographer?

johnsobey
@dgardner "He can either stand with us, or with the witches." - if Vic Toews lived in 17th century Salem

canadiancynic
I await eagerly Public Safety Minister Vic Toews warning us about mother rapers and father stabbers, accompanied by numerous 8x10 glossies.

ThatJeremyBrown
Possibly the greatest weapon against Vic Toews and Lawful Access is Vic Toews' mouth. And I say this as a guy making the weapons.

pirie
my f**k Vic Toews is a moron. bit.ly/A82h6U -- Dear Cdns, Please wake up soon. Seriously. Love, Carman.

ASaunders87
Just skimmed @ToewsVic's stream, where he refers to "NDP logic." No mention of "Vic Toews logic" where you either agree w/him or molest kids

pussindasboot
Vic Toews & Cupid trending. Did he have Cupid thrown in jail for shooting arrows? #toughoncrime

coldacid
Someone needs to tell Vic Toews that the golden age of fascism was 70-80 years ago. He should go back to that time. ... plus.google.com/10362293498163...

darkgreendesk
It's not just that Vic Toews equates civil liberties with child porn; any govt with a "public safety minister" is ipso facto scary. #cdnpoli

deepgreendesign
Why does Vic Toews ignore all the Pedophiles in the #Catholic Church? Or is that Freedom of #Religion? #SexCrime #CdnPoli #UnSafeSafety

fishymessiah
Like: this just in from Vic Toews: Police think a Police State would make their jobs way easier.

MVellacott
goo.gl/8NCen Vic Toews taking it from page one of the CPC handbook. Disagree with us and you love child rapists and terrorists!

streetmusicmtl
This makes me vomit a little: tinyurl.com/6u79fqv I'm against child pornographers. I am also in favour of warrants. Vic Toews, too complex?

AlbertHowell
Vic Toews has done the impossible, by calling those who oppose the Conservatives 'child pornographers', he's made the term a compliment.

kevinrns
Vic Toews shames Canada. Imposing survielance, he says only rapists need privacy. Every free society has been attacked like this. #canpoli

mridley
"He [Francis Scarpaleggia] can either stand with us or with the child pornographers." - Vic Toews. bit.ly/yZYk7g Seriously? Resign.

HarrisAJackson
"stand with us or with the child pornographers" Vic Toews, Minister Public Safety cbc.ca/news/technolog... Toews: A Fascist Pedophile #cdnpoli

zibipic
According to Vic Toews, I "stand" with child pornographers. According to me, Vic Toews "stands" with fascism. theglobeandmail.com/news/politics/...

canadiancynic
Dear "Anonymous" hackers: If the Cons' "lawful access" legislation passes, I'll want to know where Vic Toews has been online. Hugs, CC.

seyDoggy
Dear Vic Toews, stick your bill up you're a**. That makes me pro child porn? #f**kyou #a**hole cbc.ca/m/touch/news/s...

accessd
Apparently, you're either for big brother spying on you, or you like kiddie porn. That's solid logic @ToewsVic. is.gd/T5duly

Russell_Barth
one can only assume that Vic Toews is a child porn enthusiast, himself....

DangerToews
MT @ALL_CAPS: "'Vic Toews' and 'child pornographer' are now inextricably linked on Google" || We're going to pass a bill to fix that soon.

IsleofMang
You must be 'for' child pornography: bit.ly/zMzlwU The Cons are false dichotomy experts and love the police state #cdnpoli

youandeyeareone
Vic toews trending who would've have thought. The rhetoric spewed from the conservatives is appalling. Think of the past few months #gross

coco_urnews

Vic Toews anxious to follow John Baird's and Peter Van Loan's internet use

AgniOrtiz
This fascist minister should resign for lumping all honest Canadians who oppose draconian bills with pedophiles: thestar.com/news/canada/po...

JGentile91
Awful accusations by the unprofessional Vic Toews, a sad day for #cdnpoli when this accusations are made by Con MP soc.li/mLs69yE

blogging_tories
The Phantom Observer: Ken Epp Award Nominee: Vic Toews tinyurl.com/6n8oeuj #roft #cdnpoli

deepgreendesign
Vic Toews using #GOP 3brain dead "yes/no" "wedge classic" explains lack of any intelligent #CPC policy or #Debate. #cdnpoli #law #Fail #UN

JeffAMelanson
"You're either with us or with the child pornographers" - Vic Toews WHAT KIND OF LOGIC IS THAT??!? #cdnpoli

ptheriault
Vic Toews supports child pornographers. #Accusingpeopleofsupportingchildpornographersiseasy

jsliverz
Vic Toews sort of looks like a pedophile.

argilo
Vic Toews on internet surveillance critic: "He can either stand with us or with the child pornographers." Idiotic! cbc.ca/news/technolog...

zanyzanyworld
According to Vic Toews, I "stand" with child pornographers. According to me, Vic Toews "stands" with fascism. theglobeandmail.com/news/politics/...

gaaslin
ah bin coudonc! Un Georges Bush canadien! radio-canada.ca/nouvelles/Poli...

teesaini
So apparently In this country if you oppose your govt.. You must be on the side of child pornographers..... Smart argument Vic Toews. #smh

wallnerr
Vic Toews, are you f******g serious? cbc.ca/news/technolog...

Jeff_Power
Vic Toews stands with every regime that would remove it's citizens rights and freedoms for the purposes of warrant-less surveillance.

curtisonyon
And @LarryMiller thinks supporters of the gun registry are like Hitler? Larry mirror now! Vic Toews is out of his mind. theglobeandmail.com/news/politics/...

canadiancynic
You either stand with people who respect the sanctity of monogamous marriage, or you stand with Vic Toews.

gattaca
Vic Toews, thanks for pissing me off before my first cup of coffee. (-:|3

mode23
vic toews, we can use ultimatums too: either we live in a free country or we live in a police state. #cdnpoli

CurtMcD
Just, f*****g, Wow! Vic Towes says if you're against the government spying on you online, you must be into kiddie porn; bit.ly/yYirhB

intrepidblue
Online surveillance critics accused of supporting child porn - Technology & Science - CBC News bit.ly/xGfXjO - Vic Toews, sad idiot.

novascotiarasta
Toews accuses critics of siding with child pornographers j.mp/wj0LAt Vic wasn't rocked enough as a child #CdnPoli #Privacy

pmacpherson1

Vic Toews would like to remind all the ladies out there that if your man forgot Valentine's Day it's because he HATES you.

delmarhasissues
Vic Toews, Conservative Minister in charge of fear mongering: "Stand with us or with the child pornographers." Ass. theglobeandmail.com/news/politics/...

dbmeaford
Yes, yes Vic Toews, we know. That judge must be a child pornographer. #cpc #cdnpoli #lpc

zeptepe
Even after a good sleep and pondering the situation, Vic Toews still scares the jeepers out of me. He's a dangerous man. #cdnpoli

northwesternlad
Just had it confirmed that in Vic Toews bizzaro-world, Debate is just a waste of time - But really who is shocked by that #cdnpoli

canadiancynic
Vic Toews, who once adulterously impregnated a much younger woman ...hinglywrongrightwingnutz.blogspot.com/2010/03/this-i... lectures you on child porn theglobeandmail.com/news/politics/...

jessehawken
Don't 'Vic Toews' me, bro

stephenlautens
Choose between Vic Toews and pornographers? Hmm. Don't rush me. Still trying to decide which is more loathsome... #cdnpoli

rilesrouke
Ironic that Vic Toews is accusing the opp of siding with childporn.New bill gives em less time than pot growers#cdnpoli journalpioneer.com/Opinion/Column...

rilesrouke
The rhetoric of this gov't never ceases to amaze. #cdnpoli Vic Toews cbc.ca/news/technolog...

inkamloops
Vic Toews is an embarrassment to Canada. I believe in protecting my democratic right to privacy - that doesn't make me a child pornograher!

reloweeda
wow, Vic Toews, way to get in the news. not wanting to be monitored on the internet does not equal child pornography. thx from all MBans.

montrealsimon
Golly. How many times can the Con zombie Vic Toews stick his foot in his mouth, and eat it? bit.ly/xbaM6V #cdnpoli

Slack, Jessica

From: Slack, Jessica
Sent: February-15-12 5:13 PM
To: Swift, Andrew (Andrew.Swift@ps-sp.gc.ca)
Cc: Champoux, Martin; Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca)
Subject: FW: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Andrew, as discussed.

From: [redacted] [mailto: [redacted] @CSE-CST.GC.CA]
Sent: February-15-12 5:11 PM
To: Emma Bedard
Cc: Slack, Jessica; [redacted]; Plamondon, Jean J.
Subject: RE: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Classification: UNCLASSIFIED

Hello Emma,

Thank you very much for the opportunity to review these lines.

I suspect that Public Safety may want to respond on behalf of the GC and am copying them on this.

Hope to have a decision shortly.

Best,

[redacted]
Media Relations/Public Affairs
Communications Security Establishment Canada

[redacted]
Relations avec les médias/affaires publiques
Centre de la sécurité des télécommunications Canada
Tel. (613) 991-7248 Fax (613) 991-7691

From: Emma Bedard [mailto:Emma.Bedard@aadnc-aandc.gc.ca]
Sent: February 15, 2012 4:23 PM
To: [redacted]
Cc: Angela Matchim; Isabelle Duguay
Subject: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

PLEASE NOTE - the media response below is DRAFT, for your information only and not to be shared until approved.

Hello [redacted]

As discussed, attached is a draft response to address the following media call:

[redacted] **Journalist, APTN**
Hacking group Anonymous is picking up the indigenous cause. Is AANDC prepared to deal with hacking attacks? Are we aware of potential threats?

DEADLINE: Today, end of day.

AANDC PROPOSED RESPONSE:

- AANDC is aware of the current threat concerning the Anonymous group.
- AANDC manages the risk of security breaches through a layered perimeter defense implementation and through coordinated communications with the Communication Security Establishment Canada (CSEC).
- CSEC is the technical lead for information technology security to safeguard Government of Canada electronic information.
- For more information on technology security at the Government of Canada, please contact their Media Relations Office at 613-991-7248.

We are currently circulating this response in internal approvals. Please advise asap if you have any issues/concerns with the above statements.

Thank you,

Emma Bédard
Communications Advisor / Conseillère en communications
Aboriginal Affairs and Northern Development Canada / Affaires autochtones et Développement du Nord Canada
1900 - 10 rue Wellington St.
Gatineau, QC K1A 0H4
Tel: 819-934-6532
Fax: 819-934-3423
emma.bedard@aandc-aadnc.gc.ca

Slack, Jessica

From: Slack, Jessica
Sent: February-15-12 5:25 PM
To: Swift, Andrew (Andrew.Swift@ps-sp.gc.ca)
Subject: FW: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Not sure if you want the 3rd one but I think it fits.

We do not comment on security threats. That said, our government takes threats seriously and has measures in place to address them.

In October 2010 the Government of Canada released Canada's Cyber Security Strategy. The Government is improving its ability to respond to cyber security incidents, working to update government policy to tackle complex cyber security issues, and engaging provincial governments and private sector stakeholders to collaborate on cyber security.

The first pillar of the Strategy is Securing Government Systems and the creation of Shared Services Canada is a great example. The move within Government to one email system, the reduction in the overall number of data centres, and the streamlining of electronic networks will make IT more secure and reliable as well as improving services to Canadians (http://news.gc.ca/web/article-eng.do?nid=614499)

From: Slack, Jessica
Sent: February-15-12 5:13 PM
To: Swift, Andrew (Andrew.Swift@ps-sp.gc.ca)
Cc: Champoux, Martin; Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca)
Subject: FW: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Andrew, as discussed.

From: [redacted] [mailto: [redacted] @CSE-CST.GC.CA]
Sent: February-15-12 5:11 PM
To: Emma Bedard
Cc: Slack, Jessica; [redacted]; Plamondon, Jean J.
Subject: RE: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Classification: UNCLASSIFIED

Hello Emma,

Thank you very much for the opportunity to review these lines.

I suspect that Public Safety may want to respond on behalf of the GC and am copying them on this.

Hope to have a decision shortly.

Best,

Media Relations/Public Affairs
Communications Security Establishment Canada

Relations avec les médias/affaires publiques
Centre de la sécurité des télécommunications Canada
Tel. (613) 991-7248 Fax (613) 991-7691

From: Emma Bedard [mailto:Emma.Bedard@aadnc-aandc.gc.ca]
Sent: February 15, 2012 4:23 PM
To:
Cc: Angela Matchim; Isabelle Duguay
Subject: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

PLEASE NOTE - the media response below is DRAFT, for your information only and not to be shared until approved.

Hello ,

As discussed, attached is a draft response to address the following media call:

Journalist, APTN
Hacking group Anonymous is picking up the indigenous cause. Is AANDC prepared to deal with hacking attacks? Are we aware of potential threats?

DEADLINE: Today, end of day.

AANDC PROPOSED RESPONSE:

- AANDC is aware of the current threat concerning the Anonymous group.
- AANDC manages the risk of security breaches through a layered perimeter defense implementation and through coordinated communications with the Communication Security Establishment Canada (CSEC).
- CSEC is the technical lead for information technology security to safeguard Government of Canada electronic information.
- For more information on technology security at the Government of Canada, please contact their Media Relations Office at 613-991-7248.

We are currently circulating this response in internal approvals. Please advise asap if you have any issues/concerns with the above statements.

Thank you,

Emma Bédard
Communications Advisor / Conseillère en communications
Aboriginal Affairs and Northern Development Canada / Affaires autochtones et Développement du Nord Canada
1900 - 10 rue Wellington St.
Gatineau, QC K1A 0H4
Tel: 819-934-6532

Fax: 819-934-3423
emma.bedard@aandc-aadnc.gc.ca

Slack, Jessica

From: Slack, Jessica
Sent: February-15-12 5:41 PM
To: COMDO; Filipps, Lisa; Picard, Josée; Swift, Andrew
Subject: Re: Call on Media Line

Thanks. This has been sorted. Good night

From: COMDO
Sent: Wednesday, February 15, 2012 05:39 PM
To: Filipps, Lisa; Picard, Josée; Slack, Jessica; Swift, Andrew
Subject: Call on Media Line

Good evening,

Emma Bedard, 819-934-6532, a Comms Advisor with Aboriginal Affairs and Northern Development Canada called re a media call they received from APTN in relation to hacking group Anonymous and threats to AANDC. The response includes reference to CSE, who suggested they get in touch with PS Comms to decide who the file should reside with.

- Adam

Slack, Jessica

From: Slack, Jessica
Sent: February-15-12 5:44 PM
To: Champoux, Martin
Subject: Fw: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Hey Martin...just fyi

From: Swift, Andrew
Sent: Wednesday, February 15, 2012 05:29 PM
To: 'Emma.Bedard@aadnc-aandc.gc.ca' <Emma.Bedard@aadnc-aandc.gc.ca>
Cc: [redacted]@cse-cst.gc.ca>; Plamondon, Jean J. [redacted]@cse-cst.gc.ca>; Slack, Jessica; Williams, Christpher; Filipps, Lisa
Subject: FW: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Emma,

We've consulted our Minister's Office and PCO and suggest that the following standard lines to this line of questioning be provided by AANDC.

- We do not comment on security threats. That said, our government takes threats seriously and has measures in place to address them.
- In October 2010 the Government of Canada released Canada's Cyber Security Strategy. The Government is improving its ability to respond to cyber security incidents, working to update government policy to tackle complex cyber security issues, and engaging provincial governments and private sector stakeholders to collaborate on cyber security.
- The first pillar of the Strategy is Securing Government Systems and the creation of Shared Services Canada is a great example. The move within Government to one email system, the reduction in the overall number of data centres, and the streamlining of electronic networks will make IT more secure and reliable as well as improving services to Canadians (http://news.gc.ca/web/article-eng.do?nid=614499)

I've cc'd my PCO analyst who will confirm with yours on the proposed direction.

Thanks,

Andrew

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: [redacted] [mailto: [redacted]@CSE-CST.GC.CA]
Sent: February-15-12 5:11 PM

To: Emma Bedard
Cc: Slack, Jessica; [redacted] Plamondon, Jean J.
Subject: RE: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Classification: UNCLASSIFIED

Hello Emma,

Thank you very much for the opportunity to review these lines.

I suspect that Public Safety may want to respond on behalf of the GC and am copying them on this.

Hope to have a decision shortly.

Best,

[redacted]
Media Relations/Public Affairs
Communications Security Establishment Canada

[redacted]
Centre de la sécurité des télécommunications Canada
Tel. (613) 991-7248 Fax (613) 991-7691

From: Emma Bedard [mailto:Emma.Bedard@aadnc-aandc.gc.ca]
Sent: February 15, 2012 4:23 PM
To: [redacted]
Cc: Angela Matchim; Isabelle Duguay
Subject: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

PLEASE NOTE - the media response below is DRAFT, for your information only and not to be shared until approved.

Hello [redacted]

As discussed, attached is a draft response to address the following media call:

[redacted] **Journalist, APTN**
Hacking group Anonymous is picking up the indigenous cause. Is AANDC prepared to deal with hacking attacks? Are we aware of potential threats?

DEADLINE: Today, end of day.

AANDC PROPOSED RESPONSE:

- AANDC is aware of the current threat concerning the Anonymous group.
- AANDC manages the risk of security breaches through a layered perimeter defense implementation and through coordinated communications with the Communication Security Establishment Canada (CSEC).

- CSEC is the technical lead for information technology security to safeguard Government of Canada electronic information.
- For more information on technology security at the Government of Canada, please contact their Media Relations Office at 613-991-7248.

We are currently circulating this response in internal approvals. Please advise asap if you have any issues/concerns with the above statements.

Thank you,

Emma Bédard
Communications Advisor / Conseillère en communications
Aboriginal Affairs and Northern Development Canada / Affaires autochtones et Développement du Nord Canada
1900 - 10 rue Wellington St.
Gatineau, QC K1A 0H4
Tel: 819-934-6532
Fax: 819-934-3423
emma.bedard@aandc-aadnc.gc.ca

Pages 25 to / à 27

are duplicates of

sont des duplicatas des

pages 222 to / à 224

Swift, Andrew

From: Durand, Stéphanie
Sent: Wednesday, February 15, 2012 7:49 PM
To: Dick, Robert; Swift, Andrew
Subject: Re: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Categories: ATI PRINT

Thanks.
Andrew: see below.

From: Dick, Robert
Sent: Wednesday, February 15, 2012 07:16 PM
To: Durand, Stéphanie
Subject: Fw: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Info

From: CYBERDO
Sent: Wednesday, February 15, 2012 06:35 PM
To: Anderson, Windy; Dick, Robert
Cc: GOC-COG; CYBERDO; Beaudoin, Luc; Champoux, Martin
Subject: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Windy/Robert for your situational awareness;

At 17:15 EST 15 Feb 2012, the GOC received a call from AADNC, Senior Communications Officer, Isabelle Duguay (819-997-3544) with the following queries:

AADNC has been receiving calls from a Journalist for information on potential hacking of AADNC by the group Anonymous.

A response was provided to AADNC a short time ago by Andrew Swift (Public Safety Affairs). (I'm not sure what the response was however apparently AADNC is satisfied.)

See additional comments below from AADNC Senior Communications Officer:

CONTEXT: We have developed the response in collaboration with our departmental CIO and called to give a heads-up to CSEC that we were directing potential media questions to them.
CSEC told us that sometimes, in such cases, Public Safety would take the lead.
journalist's deadline is today.

s.19(1)

Here is the question AADNC received:
[redacted] Journalist, APTN - Hacking group Anonymous is picking up the indigenous cause... Is the Dept prepared to deal with hacking attacks? Are we aware of potential threats?

and here's AADNC proposed response:

- AANDC is aware of the current threat concerning the Anonymous group.
- AANDC manages the risk of security breaches through a layered perimeter defense implementation and through coordinated communications with the Communication Security Establishment Canada (CSEC).
- CSEC is the technical lead for information technology security to safeguard Government of Canada electronic information.
- For more information on technology security at the Government of Canada, please contact CSEC Media Relations Office at 613-991-7248.

Thank you!

Bruce Moore
Public Safety Canada
CCIRC
Cyber Duty Officer
613-991-7000

Swift, Andrew

From: Durand, Stéphanie
Sent: Friday, February 17, 2012 2:24 PM
To: Hatfield, Adam; Dick, Robert
Cc: Anderson, Windy; Swift, Andrew
Subject: RE: [redacted]
Attachments: image001.jpg

Categories: ATI PRINT

Thanks – we will monitor.
No action on our end for now.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications **s.16(2)**

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Hatfield, Adam
Sent: Friday, February 17, 2012 1:48 PM
To: Dick, Robert; Durand, Stéphanie
Cc: Anderson, Windy
Subject: FW: [redacted]

Hello Robert and Stephanie,

For information only - no action needed and no escalation required – [redacted] Shared Services, CSEC, and CCIRC are aware; Shared Services is handling [redacted] has advised CSEC that they do not require assistance. CCIRC is not involved.

[redacted]

Again, no action required.

Thanks,
Adam

From: Anderson, Windy
Sent: February-17-12 1:39 PM
To: Hatfield, Adam

Cc: Bendelier, Kenneth; Klassen, Nathan
Subject: FW: [redacted]

Adam – an update for you.

Have a great day,

Windy

Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Williston, Sandra
Sent: February-17-12 1:27 PM
To: CYBERDO; Anderson, Windy
Cc: Beaudoin, Luc
Subject: RE: [redacted]

s.16(2)

Windy;

[redacted]

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: CYBERDO
Sent: February-17-12 1:22 PM
To: Anderson, Windy
Cc: Beaudoin, Luc; CYBERDO
Subject: [redacted]
Importance: High

Windy;

CCIRC contacted CTEC immediately upon receipt of the below email.

CTEC was aware since this morning and have been in contact [redacted]

[redacted] they do not require any assistance at this time.

No participation by CCIRC at this time.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

s.16(2)

From: Jacques Latour [mailto:jacques.latour@cira.ca]
Sent: February-17-12 1:10 PM
To: stephan.aube@parl.gc.ca; Beaudoin, Luc; CYBERDO
Subject: RE: [redacted]
Importance: High

Hi All,

As you may be aware, [redacted] see below.

Stef is the IT director and I think he can benefit from your assistance [redacted]

He can share with you current activities that took place.

[redacted]

Stéphan Aubé
Dir. Opérations des TI, Chambre des communes
Dir. IT Operations, House of Commons
181, Queen, bureau-room 6-028, Ottawa, Ontario, Canada K1A 0A6
Tel.: (613)992-7449 - Fax: 613-947-6292 – E-Mail : aubes@parl.gc.ca

Regards,

Jacques

Jacques Latour, Director Information Technology
Canadian Internet Registration Authority (CIRA)
Tel: (613) 237-5335 x294 | www.cira.ca

From: Jacques Latour
Sent: February-17-12 11:58 AM
To: 'saube@parl.gc.ca'

Subject: STEF: [redacted]
Importance: High

[redacted]

Poste aujourdhui.

[redacted]

Jack 613-291-1619

[redacted]

From: stephan.aube@parl.gc.ca [mailto:stephan.aube@parl.gc.ca]
Sent: February-17-12 1:07 PM
To: Jacques Latour
Subject: DDOS

Tel que discute !

Stéphan Aubé
Dir. Opérations des TI, Chambre des communes
Dir. IT Operations, House of Commons
181, Queen, bureau-room 6-028, Ottawa, Ontario, Canada K1A 0A6
Tel.: (613)992-7449 - Fax: 613-947-6292 – E-Mail : aubes@parl.gc.ca

Miller, Kevin

From: Miller, Kevin
Sent: Friday, February 17, 2012 4:26 PM
To: COMDO
Subject: RE: Investigation launched into Twitter campaign targeting **>public...

Categories: Green Category

Yes, please include with package, no need to send out stand alone.

Tks,
K

-----Original Message-----
From: COMDO
Sent: Friday, February 17, 2012 4:23 PM
To: Miller, Kevin
Subject: FW: Investigation launched into Twitter campaign targeting **>public...

This issue seems to have taken an awfully political turn. I'm assuming I'm to package this item?

-----Original Message-----
From: Command News [mailto:fp.NEWS.COMDO@commandnews.com]
Sent: February 17, 2012 4:22 PM
To: COMDO
Subject: Investigation launched into Twitter campaign targeting **>public...

Profile: COMDO / My Drawer / Public Safety - Clip 69 (limit 500) Feb 17 2012 16:21:00 - Source: CP [The Canadian Press]

Investigation launched into Twitter campaign targeting **>public safety minister<** (Online-Surveillance-T) By Stephanie Levitz

THE CANADIAN PRESS

OTTAWA _ A Twitter tit-for-tat took a tawdry turn Friday with the Conservatives accusing the NDP of being behind an online campaign against **>Public Safety Minister<** **>Vic Toews.<**

But the New Democrats say a Twitter account targeting Toews isn't connected to them and they want the Tories to apologize.

The Speaker of the House of Commons is looking into an Ottawa Citizen report that the account is connected to a Commons Internet protocol address.

The newspaper said the same address is linked to updates in an online encyclopedia with NDP-friendly entries.

The Conservatives seized on the report to accuse the NDP of playing dirty politics.

``Not only have they stooped to the lowest of the lows, but they have been running this nasty Internet dirty-tricks campaign with taxpayers' money,'' said Foreign Affairs Minister John Baird in question period.

A spokesman for Toews also said he's sending a letter to Speaker Andrew Scheer about the matter.

But the NDP said their own investigation shows the same IP address is linked to changes on dozens of other pages, including ones with ties to the Conservatives and the Liberals.

``This is not an NDP campaign,'' New Democrat MP Jack Harris said Friday.

Toews has been the target of an online campaign all week in connection with the introduction of a surveillance bill that gives police easier access to people's Internet lives.

Critics say it will give police agencies too much power to snoop and violate Canadians' privacy.

In protest, a Twitter account using the name Vikileaks has been posting details from Toews' divorce, juxtaposing them with public statements he's made about family values.

The Ottawa Citizen linked the Twitter account to a Commons IP address by persuading the owner to click on a link set up by the paper. They were then able to trace the address of the user.

IP addresses are unique labels assigned to computers to identify them on networks.

Large organizations such as Parliament often manage their networks using two sets of addresses to protect their computers behind a firewall.

Computers connecting to an internal network each have their own IP address but when they are connecting to the external Internet, they share a small set of the IP addresses.

It's akin to having a group of people at a house party designate one person to go out and buy a pizza, said digital public affairs strategist Mark Blevis.

One person gets the whole pizza at the restaurant, but inside the house everyone gets their own slice.

It will be possible for Commons technology staff to trace exactly which computer is posting to the Twitter account though it will take time, Blevis said.

But Liberal MP Wayne Easter said he wasn't sure any rules have actually been broken.

``I think what the whole issue shows as well is in the new technological age that we're in people not being required to sign their names to their points of view is a problem,'' he said.

He said anonymous comments online amount to almost a hate attack.

``I do think we've got to find ways to identify some of these anonymous folks that are basically producing hate in some fashion.''

Blevis said anonymous tweeting to score points against a politician runs the risk of polluting the political process.

``Our political system and the ability for people to engage is dependent on people wanting to be part of the process,'' he said.

``And I think this kind of effort is very damaging to the political process and very damaging to democratic engagement. It's certainly not what we're accustomed to in Canadian politics.''

The documents being posted by Vikileaks have been public for years but have never been published by media outlets.

Blevis suggested that while Vikileaks may be embarrassing to Toews, another simultaneous online campaign being run might be making a better protest about the bill.

In the last 24 hours, over 24,000 messages have been posted to Twitter using an identifier of #tellviceverything.

Users are mockingly pre-empting the supposed need for the bill by just telling Toews what they're doing.

``Just sent my mom an email, will you tell her I love her _ I forgot to add it,'' wrote one user.

While Toews' reputation may have taken a bashing, it's also given him a moment of Internet stardom.

An online algorithm used to gauge social media standings suggests that Toews is currently more popular online than Treasury Board President Tony Clement, known as the ``Minister of Twitter'' for his use of social media.

INDEX: NATIONAL POLITICS
Visit thecanadianpress.com for more services from The Canadian Press, Canada's trusted news leader.

Swift, Andrew

From: Filipps, Lisa
Sent: Tuesday, February 21, 2012 9:28 AM
To: Durand, Stéphanie; Dick, Robert; Swift, Andrew
Cc: Anderson, Windy; Coburn, Stacey; Wong, Suki; Fortunato, Stephanie; Hatfield, Adam; Gordon, Robert; Matz, Mark; Salewski, Shawn; Champoux, Martin
Subject: RE: Heads-up

Categories: ATI PRINT

Martin will work with Cyber this a.m. on revised lines. Thanks for the heads up.

-----Original Message-----
From: Durand, Stéphanie
Sent: Tuesday, February 21, 2012 9:12 AM
To: Dick, Robert; Clairmont, Lynda; Swift, Andrew; Filipps, Lisa
Cc: Anderson, Windy; Coburn, Stacey; Wong, Suki; Fortunato, Stephanie; Hatfield, Adam; Gordon, Robert; Matz, Mark; Salewski, Shawn
Subject: Re: Heads-up

Thanks Robert. We have been monitoring. We will update our holding lines.

Andrew / Lisa: pls action.

Thanks.

----- Original Message -----
From: Dick, Robert
Sent: Tuesday, February 21, 2012 09:05 AM
To: Clairmont, Lynda; Durand, Stéphanie
Cc: Anderson, Windy; Coburn, Stacey; Wong, Suki; Fortunato, Stephanie; Hatfield, Adam; Gordon, Robert; Matz, Mark
Subject: Heads-up

For awareness: Internet posts are circulating, purportedly by Anonymous, calling for a Distributed Denial of Service attack to "shut the Internet down" March 31,2012. It is being dubbed Operation Global Blackout.

Our assessment (and others') is that the likelihood of the attack being successful is very, very low due to a variety of design, technical and operational factors. Some brief performance degradation is a more likely outcome.

This is, however, the sort of story the media may pick up and escalate. Stéphanie, we can work with your team on lines -- existing lines referencing Canada's plan with a slight twist about resilience of critical infrastructure plus fact GoC collaborates with allies ought to do it.

Robert

Slack, Jessica

From: Slack, Jessica
Sent: February-21-12 4:19 PM
To: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca)
Subject: FW: Humber College: Interview on Cyber Security

Lisa, how's this for Humber? I swapped out "cyber warfare" for "online terrorism" (Martin says this works) and made just a few tweaks to one of the answers we gave Radio-Canada and CBC. First paragraph is especially apt as it relates to the "Anonymous" threat (ie pursuing a political agenda etc)
Will send to Robert but wanted to make sure this is what you had in mind.

PROPOSED RESPONSE:

Rather than "online terrorism," the Government of Canada prefers to talk about cyber security because the real threats that we see every day are the use of cyberspace to facilitate crime. Criminals are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, and spread criminal material like child pornography. Sometimes it is led by organized crime; sometimes these crimes are perpetrated by individuals who are seeking thrills, pursuing a political agenda, or are trying to achieve notoriety or fame. As has been reported in the media, corporations and foreign governments use cyber space as a way to conduct espionage, such as to steal trade secrets and research.

Technology itself not responsible for these problems – the internet has had tremendous benefits. This is a case of criminals deliberately misusing and abusing the networks on which we rely. We need to remember that these crimes don't just "happen." These threats exist because educated and skilled people invest huge effort to construct the software to do something illegal and then, quite deliberately, commit crimes for their personal gain.

These are the types of attacks we are seeing every day. The Government is committed to addressing these cyber threats as they are the most pressing for the country.

In October 2010 the Government of Canada released *Canada's Cyber Security Strategy*. The Strategy is founded on the idea of partnerships because, ultimately, the only way to improve our cyber security is by working together, both inside and outside government.

The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians.

The Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such telecommunications networks, the financial sector, power grids and others vital systems – are getting the information they need to protect themselves and keep their systems secure. For example, the Canadian Cyber Incident Response Centre (CCIRC) monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats.

Another important element of the Strategy is *Get Cyber Safe*, the Government of Canada's national public awareness initiative to help Canadians protect themselves and their families against a wide range of online threats.

Reporter's Name	[redacted]	s.19(1)
Media Outlet	Humber	
Call Date	2/21/2012 12:00 PM	
Telephone	[redacted]	
E-mail address		
Deadline	2/24/2012 5:00 PM	
Status	Consulting	
Branch		
Subject	TBD	

Questions

Clarification:
"Groups like anonymous in particular. We're looking at this new age of crime an how the government has had to adapt to online terrorism and has had to take those extra precautions. Basically is this the future of crime, and how people in Canada can protect themselves on the Internet."

*****
For a story on hackers, she wants to talk to someone re cyber security,

She is looking for information re how the government is dealing with hackers and some stats on cases the GoC has had to deal with.

Slack, Jessica

From: Slack, Jessica
Sent: February-21-12 4:45 PM
To: Mueller, Mike; Slack, Jessica; Issues / Enjeux; McDonald, Jessica; Dussault, Josée; Eke, Darren; Fournier, Martin; Leclair, Natalie; McAteer, Julie; McDonald, Andrea; McRae, Marley; Swift, Andrew; Therien, Stephane; Tomlinson, Jamie; Patton, Michael; Johnson, Mark; Manning, Kerri; Champoux, Martin; Stanfield, Charles; Paulson, Erika; Wilson, Barbara; Willey, Chris; Carmichael, Julie; Filipps, Lisa; Williams, Christpher; * Media Monitoring / Suivi des médias; Csversko, Christine
Subject: Daily Media Report / Rapport média quotidien

For your information, we received 3 new media calls on Tuesday, February 21 2012 // Pour votre information, nous avons reçu 3 appels de médias le mardi 21 février.

NEW

Reporter's Name	[redacted]
Media Outlet	Humber
Call Date	2/21/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	2/24/2012 5:00 PM
Status	Consulting
Branch	
Subject	TBD
Questions	Clarification: "Groups like anonymous in particular. We're looking at this new age of crime an how the government has had to adapt to online terrorism and has had to take those extra precautions. Basically is this the future of crime, and how people in Canada can protect themselves on the Internet." ***** For a story on hackers, [redacted] wants to talk to someone re cyber security, [redacted] is looking for information re how the government is dealing with hackers and some stats on cases the GoC has had to deal with.

Reporter's Name	[redacted]
Media Outlet	Kings County Record
Call Date	2/21/2012 12:00 PM
Telephone	(902) 681-2121 ext [redacted]
E-mail address	
Deadline	2/23/2012 12:00 PM
Status	Background interview to be completed on Thursday
Branch	CSP
Subject	Aborignal Community Constable Program

Questions	• How long was the Aboriginal Community Constable Program in place in Kings County, N.S.? • Does the program still exist? If so how many communities and in which provinces? • Why was the position in Kings County, N.S. converted to the Provincial Police Service Agreement? What does simplify administration mean? Did the federal government have multiple people responsible for monitoring these two programs? Did they lay off people as part of simplify administration? • What is the cost saving to the federal government in making this change? I know in Kings County the bands are picking up $25,000 the federal government used to cover. What's the impact nationally?
Reporter's Name	[redacted]
Media Outlet	CJOB Radio Winnipeg,
Call Date	2/21/2012 11:00 AM
Telephone	[redacted]
E-mail address	
Deadline	
Status	Referred to MO
Branch	
Subject	TBD
Questions	[redacted] CJOB Radio Winnipeg, [redacted] wants to speak to minister (live-to-tape) about "rigamarole" on C-30. Open to doing it whenever minister is available.

Swift, Andrew

From: Filipps, Lisa
Sent: Tuesday, February 21, 2012 5:27 PM
To: Swift, Andrew
Cc: Champoux, Martin
Subject: FW: FOR APPROVAL: Media Lines - Operation Global Blackout version 2

Categories: ATI PRINT

Running this for Martin while I am still here. These were the lines that SD asked us to work up in response to Robert Dick's email this a.m. re: response to Anonymous threat to shut down the Internet:

Media Lines

- There are reports on websites that individuals claiming to be part of the hacker group Anonymous have announced plans to shut down the Internet on March 31st in what they are calling "Operation Global Blackout". Reports state that they would do so by attacking the Domain Name Service (DNS) root servers that control traffic on the Internet.

- Global DNS root servers are well-protected and strong components of the internet's infrastructure. Nevertheless, the Government of Canada will work with international partners and internet service providers to keep Canadians safe from this threat. There are no indications right now that individual Canadians and businesses need to take any action.

- The Canadian Cyber Incident Response Centre (CCIRC), part of Public Safety Canada, is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents.

COMDO

From: COMDO
Sent: Tuesday, February 21, 2012 9:49 PM
To: Chomyshyn, Nicholas; Durand, Stéphanie; Filipps, Lisa; Hannan, Andrew; Manji, Natasha; Miller, Kevin; Swift, Andrew; Tomlinson, Jamie
Cc: Brennan, Nicholas Adam; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica; Orton, Karolina
Subject: RE: FYI - New Anonymous video on YouTube directed at the Minister

Importance: High

Below is an apparent transcript of Anonymous' new video (taken from a post on Twitter). Due to not having access to social media, I can't verify the accuracy of its contents.

Hello Mr. Toews. We are Anonymous. Over the past several days, we have been watching you.

You have continued to deceive the Canadian people by claiming that the information made accessible to police by Bill c-30 is no greater than that which can be found in a phonebook. Tell us Mr. Toews, in what phonebook can you find an individual's internet browsing history? Their private emails? Their financial information? Their credit card number? And all their personal contacts?

How convenient it is that you fail to mention Bill C-30 would not only allow police access to this information without a warrant, but would make it illegal for internet service providers to inform their customers that their information has been accessed by the RCMP or CSIS.

You have continued to waste the Canadian public's time and money by demanding a parliamentary investigation into the legal release of public records. We are not shocked in the slightest, as this is consistent with your pattern of ignoring true wrongdoings in favour of feigning moral outrage.

What is shocking-- not to mention extremely disturbing-- is that you have claimed you are surprised by the contents of Bill C-30, a bill that you yourself tabled. This is a pathetically transparent attempt to feign ignorance in the face of a massive public backlash. However, let us imagine for a moment that you are telling the truth. Let us imagine that you, an elected official in the House of Commons, either did not take the time or are simply too dimwitted to understand a piece of legislation that you yourself championed. A piece of legislation that legalizes governmental spying on Canadian citizens, and effectively ends the right to privacy in this country.

This alone is grounds for you to tender your immediate resignation. The fact that you spun this catastrophic failure to perform your duties as an argument in your own defense would be laughable were the consequences not so dire.

Of course, we all know this is simply another addition to your ever-growing web of lies. And this isn't the first time you have found yourself tangled up in your own web of deceit, is it, Mr. Toews?

The Canadian public is now well aware that you carried on multiple affairs during your 30-year marriage to your first wife, all the while selling yourself as a devout Christian who championed so-called traditional family values.

Quote: "Marriage is a uniquely heterosexual institution, that indeed is a sacrament. Marriage is one of the cornerstones upon which our society has been built."

And yet, even after demonstrating you do not believe a single word of that statement, you continue to imply that your dedication to your personal family relationships makes you a suitable candidate for political office.Anonymous has gained access to a letter you recently sent to your constituents. In it, you quote Yeats:

"All this life can give us is a child's laughter; a woman's kiss."

Do you think the Canadian people are stupid, Mr. Toews? Do you honestly think that quoting saccharine poetry to us is going to convince us you are a God-fearing family man? Especially now that you are living in a common-law relationship with your former mistress, the very sort of relationship you turned your nose up at when it suited your political interests.

Mr. Toews, you have used the illusion of a traditional family life, faith, and moral values as tools in your desperate bid for power, all the while trampling on the rights of others. You have used your own family as pawns in the creation of this illusion. Once again, you have inserted your spouse and children into this debate as rhetorical devices.

We warned you that you would not be allowed any secrets if you did not allow the Canadian public any secrets of their own.

Therefore, we are naming the woman you referenced in this letter to your constituents.

The woman Vic Toews is cohabitating with, whom he impregnated in an affair that took place during his first marriage, is Stacey Meek. She is employed in an administrative capacity by Senator Terry Stratton. She runs a public relations firm based in Toronto. She previously worked for Conservative MP Joy Smith, and is currently listed as a constituency assistant for Conservative MP Joyce Bateman. In the past, she was employed by Issues Ink, a consulting and publishing company based in Winnipeg.

Of course, we're sure you had absolutely nothing to do with Stacey Meek being hired by Senator Stratton, Mr. Toews. Surely a man like yourself with such solid moral convictions would never engage in that kind of nepotism!

She has a father, Joe, who is a doctor of veterinary medicine; a brother, Jeff; a sister-in law, Rhea; and two nieces who we shall not name, all of whom reside in Winnipeg. Her mother is deceased and passed away due to cancer in in 2002.

We also have information about your youngest son, who was the product of your affair with Ms. Meek. However, as he is only 4 years-old and entirely innocent in this matter, we will not release this information. Anonymous does not hold the son responsible for the crimes of the father.

However, the woman you are cohabitating with is politically active, a government employee, and in particular is a constituency assistant to MP Joyce Bateman, who voted Yes on Bill C-30. As such, we have no qualms about releasing information about her to the Canadian public.

We have also decided not to release your personal contact information, such as your phone number and address, at this time, as we understand you have received credible violent threats from members of the public.

Shall we continue, Mr. Toews? Do we have your attention? How does it feel to have personal information about your family in the hands of people you know nothing about, with no control over who disseminates it or how it will be used?

Let it be known this is only a taste of the information we have access to. And this is only the beginning.

And yet, it is nothing compared to the personal information of millions of Canadians that will be collected, stored, and scrutinized by the authorities if Mr. Toews and this corrupt government are allowed to pass Bill C-30. If this outrageous piece of legislation is allowed to pass, the government will have access to massive legally-required databases filled with information on your spouses, your children, your parents, your brothers, your sisters, your friends and your neighbours.

Let it be known, Mr. Toews, that Anonymous will do to corrupt politicians exactly what you are attempting to do to the Canadian public. There will be no two-tier system of privacy for the government and the people of this country. You, and any public official who spies or support spying on Canadian citizens, will reap exactly what you have sewn.

It would appear you have made many political enemies, Mr. Toews. Since Anonymous made an email address available through which the public can submit more Vikileaks, we have received no less than a dozen emails from your peers in Ottawa, several of whom have offered information or have made offers to provide us with information. And that does not include the messages from members of the public who know you in a personal capacity.

And to the rest of the Parliament of Canada: you would do well to mind your words about Anonymous. Any attempt to score political points by claiming we are associated with a particular political party will not be met kindly. Your party affiliations are utterly irrelevant to us. Our only interest in this matter is protecting the freedom of information, and protecting the privacy of Canadians from the tyranny of our own government.

Anonymous demands the immediate resignation of Vic Toews, the scrapping of Bills C-30 and C-11 in their entirety, and a formal apology to the people of Canada for referring to them as supporters of pedophiles, and importantly, for attempting to undermine their most basic civil rights.

We are Anonymous.

We are Legion.

We do not forgive.

We do not forget.

Expect us.

From: COMDO
Sent: February 21, 2012 9:43 PM
To: Chomyshyn, Nicholas; Durand, Stephanie; Filipps, Lisa; Hannan, Andrew; Manji, Natasha; Miller, Kevin; Swift, Andrew; Tomlinson, Jamie
Cc: Brennan, Nicholas Adam; COMDO; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica; Zablotney, Karolina
Subject: FYI - New Anonymous video on YouTube directed at the Minister
Importance: High

FYI – People are Tweeting at news outlets about the new video and information.

- Sean

From: COMDO
Sent: February 21, 2012 9:38 PM
To: Swift, Andrew; Miller, Kevin
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; COMDO; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica; Zablotney, Karolina
Subject: New Anonymous video on YouTube directed at the Minister

AnonsOfCanada 9:18pm via Web
Video identifying Vic Toews' former mistress, Stacey Meek, is up on YouTube. You were warned, Mr. Toews. This is war. #c30 #victoews

AnonsOfCanada 9:17pm via Web
Anonymous posts new message to Vic Toews and the Parliament of Canada, including release of new information: youtube.com/watch?v=-sb0-Q... #victoews

Sean Despard
Communications Duty Officer/ Agent de service des communications
Government Operations Centre/ Centre des opérations du gouvernement
Tel.: (613) 991-7010
Fax/Télécopieur: (613) 996-0995
Email/courriel: COMDO@ps-sp.gc.ca

Swift, Andrew

From: COMDO
Sent: Tuesday, February 21, 2012 10:02 PM
To: Swift, Andrew; Miller, Kevin
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica; Orton, Karolina
Subject: RE: New Anonymous video on YouTube directed at the Minister

Categories: ATI PRINT

Good.

I'll be on the lookout for anything mainstream media picks up.

- Sean

From: Swift, Andrew
Sent: February 21, 2012 10:00 PM
To: COMDO; Miller, Kevin
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica; Orton, Karolina
Subject: Re: New Anonymous video on YouTube directed at the Minister

Thanks Sean, I've given a heads up. Transcript you also forwarded looks to be accurate based on my viewing of the video.
Andrew

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: COMDO
Sent: Tuesday, February 21, 2012 09:37 PM
To: Swift, Andrew; Miller, Kevin
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; COMDO; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica; Orton, Karolina
Subject: New Anonymous video on YouTube directed at the Minister

AnonsOfCanada 9:18pm via Web
Video identifying Vic Toews' former mistress, Stacey Meek, is up on YouTube. You were warned, Mr. Toews. This is war. #c30 #victoews

AnonsOfCanada 9:17pm via Web
Anonymous posts new message to Vic Toews and the Parliament of Canada, including release of new information: youtube.com/watch?v=-sb0-Q... #victoews

Sean Despard
Communications Duty Officer/ Agent de service des communications

Government Operations Centre/ Centre des opérations du gouvernement
Tel.: (613) 991-7010
Fax/Télécopieur: (613) 996-0995
Email/courriel: COMDO@ps-sp.gc.ca

Slack, Jessica

From: Slack, Jessica
Sent: February-22-12 4:46 PM
To: Mueller, Mike; Slack, Jessica; Issues / Enjeux; McDonald, Jessica; Dussault, Josée; Eke, Darren; Fournier, Martin; Leclair, Natalie; McAteer, Julie; McDonald, Andrea; McRae, Marley; Swift, Andrew; Therien, Stephane; Tomlinson, Jamie; Patton, Michael; Johnson, Mark; Manning, Kerri; Champoux, Martin; Stanfield, Charles; Paulson, Erika; Wilson, Barbara; Willey, Chris; Carmichael, Julie; Filipps, Lisa; Williams, Christpher; * Media Monitoring / Suivi des médias; Csversko, Christine
Subject: Daily Media Report / Rapport média quotidien

For your information, we received 3 new media calls on Wednesday, February 22 2012 // Pour votre information, nous avons reçu 3 appels de médias le mercredi 22 février.

NEW

Reporter's Name	[redacted]
Media Outlet	Rogers Radio News
Call Date	2/22/2012 1:50 PM
Telephone	[redacted]
E-mail address	[redacted]@rogers
Deadline	ASAP
Status	Consulting with MO
Branch	
Subject	Costs associated with Bill C-30
Questions	Would like to somebody to confirm the stats CBC has been reporting on costs associated with Bill C-30. Hoping the Minister would be available for an Interview on the topic.

s.19(1)

Reporter's Name	[redacted]
Media Outlet	Yellowknifer newspaper
Call Date	2/22/2012 3:00 PM
Telephone	[redacted]
E-mail address	editorial@nnsl.com
Deadline	2/22/2012 7:00 PM
Status	Consulting with MO
Subject	Costs associated with Bill C-30
Questions	I have three questions in regards to Bill C-30. 1) How much money will it cost to implement the lawful access bill? 2) How much will it cost to maintain once implemented? 3) If available, what kind of financial support would be made available to internet service providers to build and maintain the data centres necessary to store the information set out in bill C-30. This request is for Yellowknifer newspaper, a bi-weekly publication in Yellowknife, NT. We

are an affiliate of Northern News Services.

My deadline for this story is 5 p.m. Mountain Time today (Wednesday). This is 7 p.m. EST. Please give me a call at [redacted] with this information or if you need any clarification.

Regards,
--
[redacted] Reporter, Yellowknifer and NNSL

Reporter's Name	[redacted]
Media Outlet	CBC Radio
Call Date	2/22/2012 2:00 PM
Telephone	[redacted]
E-mail address	[redacted]@cbc.ca
Deadline	2/23/2012 10:00 AM
Status	Referred to other organization – Transport Canada
Branch	
Subject	Drone surveillance aircrafts
Questions	1) Is there a legislation that covers the use of drone surveillance aircrafts in Canada? 2) If there are any rules with regards to what uses drone aircrafts can be employed by security agencies in Canada?

<u>OUTSTANDING:</u>

Reporter's Name	[redacted]
Media Outlet	Humber
Call Date	2/21/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	2/24/2012 5:00 PM
Status	Consulting
Branch	
Subject	TBD
Questions	Clarification: "Groups like anonymous in particular. We're looking at this new age of crime an how the government has had to adapt to online terrorism and has had to take those extra precautions. Basically is this the future of crime, and how people in Canada can protect themselves on the Internet." ***** For a story on hackers, [redacted] wants to talk to someone re cyber security, [redacted] is looking for information re how the government is dealing with hackers and some stats on cases the GoC has had to deal with.
Reporter's Name	[redacted]
Media Outlet	Kings County Record

Call Date	2/21/2012 12:00 PM
Telephone	(902) 681-2121 ext [redacted]
E-mail address	
Deadline	2/23/2012 12:00 PM
Status	Background interview to be completed on Thursday
Branch	CSP
Subject	Aboriginal Community Constable Program
Questions	• How long was the Aboriginal Community Constable Program in place in Kings County, N.S.? • Does the program still exist? If so how many communities and in which provinces? • Why was the position in Kings County, N.S. converted to the Provincial Police Service Agreement? What does simplify administration mean? Did the federal government have multiple people responsible for monitoring these two programs? Did they lay off people as part of simplify administration? • What is the cost saving to the federal government in making this change? I know in Kings County the bands are picking up $25,000 the federal government used to cover. What's the impact nationally?

Swift, Andrew

From: Issues / Enjeux
Sent: Thursday, February 23, 2012 2:05 PM
To: De Curtis, Laura; McDonald, Jessica; Picard, Josée; Swift, Andrew; Filipps, Lisa; Manning, Kerri; Champoux, Martin; Ferguson, Michelle; Wilson, Barbara; Slack, Jessica
Subject: FW: CCIRC Technical Report TR12-001: Mitigation Guidelines for Denial-of-Service Attacks / CCRIC Rapport technique RT12-001: Principes de prévention contre les attaques par déni de service

Categories: ATI PRINT

From: COMDO
Sent: February-23-12 2:05:21 PM (UTC-05:00) Eastern Time (US & Canada)
To: Eke, Darren; Stanfield, Charles; Bronson, Jessie
Cc: Issues / Enjeux
Subject: FYI: CCIRC Technical Report TR12-001: Mitigation Guidelines for Denial-of-Service Attacks / CCRIC Rapport technique RT12-001: Principes de prévention contre les attaques par déni de service

(La version française suit)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
Technical Report
****

Number: TR12-001
Date: 22 February 2012

****
Mitigation Guidelines for Denial-of-Service Attacks
****

AUDIENCE

This Information Report is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries. The recipients of this product may further distribute it to technical stakeholders within their organization.

PURPOSE

The purpose of this Information Report is to provide IT security personnel with an introduction to distributed denial-of-service (DDoS) attacks, their modus-operandi and the recommended steps to help with the preparation, identification, containment, recovery and continuous improvement efforts required to limit associated organizational risk. This

document may be used by system administrators, computer security incident response teams (CSIRTS), IT security operations centres and other related technology groups.

INTRODUCTION

Denial of service (DoS) attacks are common malicious network actions aimed at disrupting the availability of computing resources from legitimate users. These types of attacks, especially DDoS attacks have recently gained in popularity due to the availability of DoS rental services from botnet operators, as well as the availability of various free and easy to use hacking tools. The latter have enabled activists using hacking to support their causes (also known as hacktivists) to efficiently recruit large numbers of followers to perpetrate cyber attacks, increasing both their distribution and power. Well known examples of DoS attacks include the use of the Low Orbit Ion Cannon DDoS tool in support of Wikileaks (Introduction to LOIC: http://en.wikipedia.org/wiki/LOIC) used by hacking group "Anonymous" and attacks against national infrastructures such as Korea (http://blogs.mcafee.com/mcafee-labs/malware-in-recent-korean-ddos-attacks-destroys-systems), Georgia (http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/) and Estonia (http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia).

DOS AND DDOS DEFINITION

A DoS attack is an attempt to make a computer resource unavailable to its intended users (Definition: http://en.wikipedia.org/wiki/Denial-of-service_attack). A DDoS attack occurs when multiple systems simultaneously flood networked computer resources, rendering them inaccessible. A DDoS attack, in contrast with a DoS attack, comes from many sources, often hundreds or even thousands. As a result, mitigation actions against a DDoS attack are more difficult to coordinate and associated traffic is more damaging to the target.

DDoS attacks often use stateless protocols such as UDP and ICMP, but stateful protocols can also be used when the connections are not fully established such as during a TCP SYN flood attack. Both techniques make it easier for the attacker to use spoofed IP addresses and harder to determine the source of the attack.

FIVE STEPS TO DEFEND AGAINST DDOS ATTACKS

Preparation:

Preparation is the most important step in defending against a DDoS attack. Clear and complete procedures and guidelines should be established well before an attack takes place. Any organization can fall victim to DDoS attacks, either directly or indirectly. Having a solid plan in place will help reduce the risk and lessen the impact should an attack occur.

Identification:

Indicators that your organization may be under a DDoS attack could include poor network performance, inaccessible services or system crashes. Being able to identify and understand the nature of the attack and its targets will help in the containment and recovery process. For this purpose, organizations require tools that provide visibility over their managed information technology (IT) infrastructure. Often, prior to a DDoS attack, a reconnaissance of the target is performed by the attacker. This may include scanning the target network for known exposed vulnerabilities or sending malformed packets to the target host to analyze changes in response time. This reconnaissance activity may be hard to detect, especially because it may take place well before the attack itself. A knowledgeable attacker will also ensure scan traffic does not meet the threshold required to trigger alarms from network monitoring tools. However, there may be available intelligence indicating an increased likelihood of a DDoS attack against an organization. Good examples are the Anonymous Operations (aka "anonops" (http://anonops.blogspot.com/2011/09/tar-sands-action-september-3-press_04.html)), which broadly advertise their motivation and targets.

Containment:

Having a pre-determined containment plan before an attack for a number of scenarios will significantly improve response speed and limit damages resulting from a DDoS attack. For example, the containment strategy for a mail server may differ from one for a web server. Underestimating the importance of this phase can result in mistakes and significant collateral damages. Therefore, understanding the nature of DDoS attacks and documenting the associated decision-making process is critical. An organization should clearly identify its network perimeter and exposed assets. Load balancers, modern firewall technologies (Deep Packet Inspection, proxy, application layer filtering), content caching, content hosting geographic diversity, dynamic DNS service and ISP-based DDoS protection services are some of the tools an organization may leverage to contain an ongoing DDoS attack.

Recovery:

Depending on the containment strategy employed and the sensitivity to its collateral impact, an organization may be under different pressure to recover from a DDoS attack. Understanding the characteristics of the attack is required for an appropriate recovery. DDoS may exploit limits in the following resources:

- Server queue length
- Server computing resources
- Client tolerance to level of service variability
- Bandwidth

A DDoS attack may exploit any or a combination of these limitations. An organization equipped with a flexible provisioning model for these resources may be able to rapidly adapt and sustain long-term DDoS attacks. However, some attacks may leverage vulnerabilities in protocols or software and achieve unexpected high impact as a result (http://www.theregister.co.uk/2011/08/24/devastating_apache_vuln/). An organization equipped with packet capture capability may be able to identify the delivery method of the attack and potentially design an accurate Intrusion Prevention System / Firewall signature. Despite mitigation efforts, some DDoS attacks may be persistent over time. An organization using connection logs and other tools may be able to provide a list of potentially offending IP addresses (if not spoofed) to their upstream ISP, law enforcement and national Computer Emergency Response Team (CERT) to coordinate mitigation/investigation of the offending sources.

Lessons Learned:

Lessons learned is a very important step that is often overlooked. Lessons learned activities should take place as soon as possible following an incident. All decisions and steps taken throughout the incident handling cycle should be reviewed. All procedures should be reviewed to see where improvements may be made.

Perhaps the most challenging part of performing a Lessons Learned review involves documenting the impact and cost the incident caused to the organization. Although time consuming, this step is essential to allow organizations to properly justify security resources and assess their return on investment. Damages to an organization include tangible metrics, such as loss in sales and productivity, as well as intangible metrics, such as reputation and brand.

By performing this review after each incident, organizations will enable continuous improvement and potentially significant reduction in the impact of incidents.

CHECKLIST

The following checklist is intended to help organizations during the various mitigation phases of DDoS attacks. Many of these mitigations are applicable to other types of cyber attacks as well and should be considered accordingly.

Preparation:

1. Identify your most critical assets and the services they provide.
- Are they up to date with the latest patches?
- Do they run any unnecessary services such as Telnet or FTP?

2. Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.

3. Establish 24/7 contact information for your ISP and alternate methods for communications.

4. Deny all obviously spoofed traffic (e.g., internal IP addresses that should not be coming in or going out of your network). Implement a bogon block list (unallocated address space) at the network boundary.

5. Establish procedures on how to segregate your networks in the event of a DDoS attack. Use existing network devices, such as routers and managed switches, to defend against DDoS attacks. Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls.

6. Disable all unnecessary services and restrict access to and from all previously identified critical hosts based on DDoS traffic characteristics.

7. Create a whitelist of the source IPs you must allow if you need to prioritize traffic during an attack.

8 Document your network topology including all IP addresses. Keep it up to date.

9. Review your Business Continuity Plan (BCP) and ensure senior management and legal team understand the significance of a DDoS attack, including their roles.

10. Understand "normal." Establish a baseline of network traffic, CPU usage, connection and memory utilization of critical hosts under normal conditions so that network monitoring tools will trigger on abnormal changes.

11. Acknowledge that your organization may be attacked. Organizations should consider the development and implementation of policies, plans and procedures to defend against DDoS attacks. Identify and plan for resources to implement these plans.

12. Assign roles and responsibilities. Identify who plays a role in defending against a DDoS attack and ensure they are aware of this responsibility. This should include personnel from critical business functions, IT operations, network and IT security teams, legal advisors, and media relations staff. Ensure an up-to-date point-of-contact list with primary and alternate personnel is maintained. As the network may be unavailable, including mobile devices, ensure alternate communications mechanisms are in place.

13. Conduct exercises. The worst time to test plans and procedures is during an attack.

Identification:

1. Determine if you are the primary target or a collateral victim. (ex: is your upstream internet provider or content hosting provider the target ?)

2. Understand the logical flow of the attack.

3. Determine what type of traffic is being used, such as IP addresses, ports and protocols.

4. Consider using network analysis tools to determine the type of traffic being used in the attack (e.g., TcpDump, Wireshark, Snort).

5. Review any available logs to understand the attack and what is being targeted.

6. Notify appropriate personnel. This may include senior management and the legal team.

Containment:

1. Contact your ISP to implement filtering.

2. Block the traffic as close to the network cloud as possible (router, firewall, load balancer, etc.).

3. Relocate the target to another IP address if a particular host is being targeted. This is a temporary solution.

4. If a particular application is being targeted, consider disabling it temporarily.

5. Identify and correct the vulnerability or weakness that is being exploited. An example of this may be an unused service that is accidently left enabled on a public facing device or unpatched operating system.

6. Implement filtering based on the characteristics of the attack. An example may be blocking IMCP echo packets.

7. Implement rate limiting for certain protocols, allowing a certain number of packets per second for a specific protocol or to access a certain host.

Recovery:

1. Confirm that the DDoS attack has finished and services are reachable again.

2. Confirm that your networks are back to your baseline performance.

3. If necessary, patch and update all affected machines.

4. If possible, identify the source of the attack. Enlist the help of your ISP.

5. Review logs for signs of reconnaissance. Maintain logs for possible future law enforcement requirements.

Lessons Learned:

1. Create or update the following documents:
- Standard Operating Procedures
- Emergency Operating Procedures
- Business Continuity Plans

RECOMMENDATIONS

CCIRC recommends that organizations assess their risk exposure to Denial of Service attacks which may be caused accidentally or intentionally and consider mitigation advice herein provided and implement them as appropriate for the specific IM/IT environment.

REFERENCES

1. US-CERT, Understanding Denial-of-Service Attacks
http://www.us-cert.gov/cas/tips/ST04-015.html

2. NIST, Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

3. GovCERT.NL, Factsheet: Protect your online services against dDoS attacks
http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html

4. Societe Generale DDoS Incident Reponse
http://cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf

REPORTING

Any Canadian Critical Infrastructure Operator wishing to report incidents may do so using the CCIRC Cyber Duty Officer PGP encryption key, found at:
http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx
Associated reports should be sent to:
[redacted] s.16(2)(c)

Potentially malicious files/samples may be shared with CCIRC by sending them zipped and protected with the password "infected" via email to:
malware@ccirc-ccric.gc.ca

CRITICAL NOTE:

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

NOTE TO READERS

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
Email: communications@ps-sp.gc.ca

For urgent matters please contact the GOC.

SÉCURITÉ PUBLIQUE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

****
Rapport technique
****

Numéro : TR12-001
Date : 22 février 2011

****
Principes de prévention contre les attaques par déni de service
****

PUBLIC CIBLE

Le présent rapport d'information est rédigé à l'intention des professionnels et gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales, ainsi que des industries à infrastructure critique et autres industries connexes. Les personnes ayant obtenu le présent produit peuvent le divulguer aux intervenants techniques dans leur organisme.

OBJECTIF

Ce rapport d'information renseigne le personnel chargé de la sécurité informatique sur les attaques par déni de service distribué (DSD) et leur modus operandi. Il décrit la procédure recommandée pour faciliter les étapes de préparation, d'identification, de confinement et de reprise des services, ainsi que les efforts d'amélioration que l'organisation doit déployer en tout temps pour limiter les risques de s'exposer à telles attaques. Ce document est destiné aux

administrateurs de système, aux équipes d'intervention en cas d'incident informatique (EIII), aux Centres des opérations de sécurité informatique et aux autres groupes technologiques concernés.

PRÉSENTATION

Dirigées contre les réseaux, les attaques par déni de service sont des actions malveillantes répandues visant à empêcher les utilisateurs légitimes d'avoir accès à des ressources informatiques. Ces actions, en particulier les attaques par déni de service distribué (DSD), se sont récemment multipliées en raison de la disponibilité des services de déni de service loués par des zombimestres (des opérateurs de réseaux d'ordinateurs zombies) et de l'accès à de nombreux outils de piratage gratuits et faciles à utiliser. Ces outils ont permis aux « hacktivistes », des activistes qui font appel au piratage informatique – le hacking – pour défendre leur cause, de lever efficacement une armée de partisans qui appuient et facilitent leurs cyberattaques, leur permettant ainsi d'étendre leur réseau de distribution et d'accroître leur pouvoir. Parmi les attaques par déni de service les plus connues, on retrouve celle du groupe de pirates informatiques Anonymous avec l'application LOIC (Low Orbit Ion Cannon) pour appuyer Wikileaks (Présentation de l'application LOIC : http://fr.wikipedia.org/wiki/LOIC) et des attaques DSD contre les infrastructures nationales de la Corée (http://blogs.mcafee.com/mcafee-labs/malware-in-recent-korean-ddos-attacks-destroys-systems (en anglais)), de la Géorgie (http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/ (en anglais)) et de l'Estonie (http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia (en anglais).

DÉNI DE SERVICE ET DÉNI DE SERVICE DISTRIBUÉ – DÉFINITIONS

Une attaque par déni de service est une attaque ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser (Définition : http://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service). Une attaque par déni de service distribué (DSD) se produit lorsqu'une multitude de systèmes « inondent » de diverses requêtes simultanées les ressources d'un réseau informatique, rendant ces dernières inaccessibles. Contrairement aux attaques par déni de service, les attaques DSD ne sont pas perpétrées par un seul attaquant, mais bien des centaines, voire des milliers. Il est donc plus difficile de coordonner les mesures d'atténuation pour les contrer, et le trafic qu'elles génèrent endommage encore plus l'infrastructure ciblée.

Les attaques DSD reposent souvent sur l'exploitation de protocoles sans état, tel UDP et ICMP, mais utilisent également des protocoles avec état lorsque les connexions sont rendues instables par une attaque par saturation de type TCP SYN. Les deux techniques facilitent l'usurpation d'adresses IP tout en brouillant les pistes menant à l'origine des attaques.

CINQ ÉTAPES POUR SE PROTÉGER DES ATTAQUES DSD

Préparation:

La préparation est l'étape la plus importante de la défense contre les attaques DSD. Il faut établir une série exhaustive de procédures et de lignes directrices claires avant qu'elles ne surviennent. Toute organisation peut être victime d'attaques DSD directes ou indirectes. Elle doit donc instaurer un plan de protection rigoureux pour réduire les risques et atténuer les effets de ces attaques.

Identification:

Une attaque DSD se manifeste entre autres choses par le piètre rendement du réseau, des services indisponibles et des pannes de système. La capacité à la reconnaître, à en comprendre la nature et à en identifier les cibles facilite le processus de confinement et la reprise des services. C'est pourquoi chaque organisation a besoin d'outils qui lui permettent de voir l'ensemble de son infrastructure de technologie de l'information gérée. L'attaquant effectue souvent une reconnaissance du réseau ciblé avant de lancer une attaque DSD contre lui. Il cherchera ainsi à y déceler des vulnérabilités connues ou à y envoyer des paquets mal formés pour analyser les changements du temps de réaction. Une telle activité de reconnaissance s'avère parfois difficile à détecter, surtout parce qu'elle précède longtemps à

l'avance l'attaque proprement dite. Un attaquant chevronné s'assurera également de limiter le trafic servant à l'analyse ne dépasse pas le seuil de déclenchement des alarmes par des outils de surveillance du réseau. Cependant, l'organisation peut avoir accès à de l'information qui l'informe d'une recrudescence des risques d'attaques DSD dirigées conte elle. Un exemple bien connu : les opérations du collectif Anonymous (ou anonops (http://anonops.blogspot.com/2011/09/tar-sands-action-september-3-press_04.html)) qui fait largement étalage de ses intentions et de ses cibles.

Confinement:

Un plan de confinement comportant divers scénarios et établi au préalable réduit considérablement le temps de réaction à une attaque DSD et l'étendue des dommages. Ainsi, on n'appliquera pas la même stratégie de confinement au serveur de courriel et au serveur Web. Négliger cette étape de la défense se traduit par des erreurs et d'importants dommages collatéraux. Il est donc crucial de bien comprendre la nature des attaques DSD et de documenter les processus décisionnels afférents. L'organisation doit identifier clairement le périmètre de son réseau et dresser la liste exhaustive des ressources exposées. Une organisation tirera profit de divers outils lui permettant de confiner une attaque DSD en cours, comme des équilibreurs de charge, des dispositifs pare-feu modernes (inspection approfondie des paquets, les serveurs mandataires, filtrage d'application), la mise en antémémoire du contenu, la diversité géographique des sites d'hébergement du contenu, le service DNS dynamique et les services de protection contre les attaques DSD fournis par les fournisseur d'accès Internet (FAI).

Reprise des services:

La pression exercée sur l'organisation pour qu'elle assure la reprise de ses services à la suite d'une attaque DSD varie en fonction de sa stratégie de confinement et de sa fragilité aux dommages collatéraux. Elle doit donc savoir reconnaître les caractéristiques d'une telle attaque pour assurer une reprise adéquate de ses services. L'attaque DSD tire profit des limites des ressources suivantes :

- Longueur de la file d'attente du serveur
- Ressources informatique du serveur
- Tolérance du client aux variations du niveau de service
- Bande passante

Les attaques DSD exploitent l'une ou l'autre de ces limites, ou plusieurs d'entre elles à la fois. Si l'organisation a appliqué un modèle souple de service à la demande à ces ressources, elle pourra s'adapter rapidement et résister à des attaques SDS soutenues. En revanche, certaines attaques profiteront des vulnérabilités des protocoles ou des logiciels pour causer d'importants dommages impossibles à prévoir (http://www.theregister.co.uk/2011/08/24/devastating_apache_vuln/). L'organisation qui s'est dotée d'un mécanisme de capture des paquets sera en mesure de comprendre le mode de prestation de l'attaque et de concevoir une solution efficace combinant système de prévention des intrusions et dispositif pare-feu. Certaines attaques DSD se poursuivront malgré les mesures d'atténuation en place. Pour assurer la coordination des mesures d'atténuation et permettre d'enquêter sur les sources criminelles, l'organisation utilisera ses journaux de session et d'autres outils pour signaler à son FAI en amont, aux services de police et à l'Équipe nationale d'intervention d'urgence en informatique (EIUI) les adresses IP suspectes – si elle n'ont pas été usurpées – qui pourraient avoir servi à perpétrer de telles attaques.

Leçons retenues:

Cette étape essentielle de la défense est trop souvent omise. Il faut faire le point le plus rapidement possible à la suite d'un incident et examiner chacune de décisions et des mesures prises tout au long de la gestion de la crise. Cet exercice permet de cerner ce qui doit être amélioré dans les procédures appliquées.

L'examen des leçons retenues comporte un volet particulièrement difficile à réaliser : la documentation des répercussions de l'incident sur l'organisation et les coûts qu'il représente. Bien qu'elle prenne beaucoup de temps, cette

étape est essentielle puisqu'elle permet à l'organisation de justifier adéquatement l'acquisition de ressources de sécurité et de bien évaluer le rendement du capital investi. Les dommages subis par l'organisation se mesurent quantitativement d'une part, par exemple le volume de ventes perdues et la baisse de la productivité, et d'autre part qualitativement, quand la réputation et l'image de marque sont entachées.

L'examen systématique des leçons retenues permet à l'organisation de s'améliorer sans cesse et de réduire considérablement les répercussions négatives des incidents.

LISTE DE CONTRÔLE

La liste de contrôle ci-dessous facilite la prise de mesures d'atténuation durant les diverses phases d'une attaque DSD. Bon nombre de ces mesures s'appliquent également aux autres types d'attaques cybernétiques et doivent être envisagées en conséquence.

Préparation:

1. Identifier les ressources matérielles les plus cruciales et les services dont elles assurent la prestation.
- Les derniers correctifs ont-ils été installés?
- Exécutent-elles des services inutiles comme Telnet, FTP, etc.?

2. De concert avec le fournisseur d'accès Internet (FAI), établir des procédures pour connaître l'étendue du soutien qu'il peut apporter à l'organisation lorsqu'elle fait l'objet d'une attaque DSD. Savoir s'il existe un accord sur les niveaux de services (ANS) et connaître les coûts à assumer.

3. Dresser la liste des personnes-ressources du FAI que l'on peut joindre en tout temps, ainsi que des autres moyens de communiquer avec elles.

4. Bloquer tout trafic qui présente des signes évidents d'usurpation d'identité (p. ex., les adresses IP à l'intérieur du réseau de l'organisation qui ne devraient pas être associées à du trafic entrant ou sortant). Instaurer une liste de filtrage Bogon (plage d'adresses non allouées) au périmètre du réseau.

5. Établir des procédures sur la façon de cloisonner les réseaux de l'organisation en cas d'attaque DSD. Se servir des appareils existants, comme les routeurs et les commutateurs gérés, pour s'en protéger. Dans la mesure du possible, configurer les routeurs du périmètre pour filtrer les services afin de réduire la charge imposée aux dispositifs de sécurité, tels les pare-feu, qui analysent le trafic.

6. Désactiver tout service inutile et bloquer tout accès non autorisé vers et depuis les hôtes critiques identifiés précédemment.

7. Créer une liste blanche des adresses IP source s'il est nécessaire d'établir un trafic prioritaire durant une attaque.

8. Documenter la topologie de réseau, y compris toutes les adresses IP. Tenir cette information à jour.

9. Passer en revue plan de continuité des opérations (PCO) de l'organisation et s'assurer que la haute direction et le service du contentieux comprennent bien ce qu'est une attaque DSD et les rôles et responsabilités qui leur sont dévolus.

10. Comprendre ce que constituent des conditions normales. Établir le niveau de référence du trafic sur le réseau, de la charge de travail imposée aux processeurs, de l'utilisation des connexions et de la mémoire des hôtes essentiels en

situation normale afin que les outils de surveillance du réseau entrent en œuvre lorsqu'une variation anormale se produit.

11. Reconnaître que l'organisation peut être attaquée. Solliciter la direction afin d'obtenir son approbation en vue d'élaborer et de mettre en œuvre des politiques, plans et procédures pour se défendre contre les attaques DSD. Identifier et obtenir les ressources nécessaires pour mettre en œuvre ces politiques, plans et procédures.

12. Attribuer les rôles et responsabilités. Connaître les intervenants dans la défense contre les attaques DSD et s'assurer qu'ils sont au fait de cette responsabilité. Ces personnes devraient appartenir au personnel affecté aux fonctions opérationnelles essentielles, aux opérations de TI, à la sécurité des réseaux et des TI, au service du contentieux et aux relations publiques. Tenir à jour la liste des points de contacts primaires et secondaires. Le réseau étant susceptible d'être en panne, y compris les appareils mobiles, mettre également en place d'autres mécanismes de communication.

13. Effectuer des exercices. Ce n'est plus le temps de faire l'essai des plans et des procédures lorsqu'une attaque se produit.

Identification:

1. Savoir si l'organisation est une victime ciblée ou accidentelle. (P. ex., la cible est-elle le fournisseur d'accès Internet (FAI) en amont ou le fournisseur de services d'hébergement de contenu?)

2. Comprendre le déroulement logique de l'attaque.

3. Déterminer le trafic dont se sert l'attaquant en identifiant les adresses IP, les ports et les protocoles qu'il exploite.

4. Envisager de recourir à des outils d'analyse du réseau pour déterminer le type de trafic qu'exploite l'attaquant (p. ex., TcpDump, Wireshark, Snort).

5. Consulter les journaux de serveur pour comprendre le fonctionnement de l'attaque et les cibles visées.

6. Aviser le personnel concerné, notamment celui de la haute direction et du service du contentieux.

Confinement:

1. Communiquer avec le FAI pour mettre en place un mécanisme de filtrage du trafic.

2. Bloquer le trafic le plus près possible du réseau en nuage (p. ex., avec un routeur, un pare-feu, un équilibreur de charges).

3. Changer l'adresse IP de l'hôte ciblé par l'attaque. Il s'agit là d'une solution provisoire.

4. Si l'attaque vise une application en particulier, envisager sa désactivation temporaire.

5. Identifier et corriger la vulnérabilité ou la faiblesse du système qui est exploitée. Il peut s'agir par exemple d'un service inutilisé maintenu involontairement en activité sur un dispositif destiné au public ou d'un système d'exploitation dont les correctifs n'ont pas été installés.

6. Mettre en place un mécanisme de filtrage en fonction des caractéristiques de l'attaque, par exemple le blocage des paquets IMCP Echo.

7. Limiter le trafic de certains protocoles à un nombre quelconque de paquets par seconde ou en n'autorisant l'accès des paquets qu'à certains hôtes.

Reprise des services:

1. Confirmer que l'attaque DSD a pris fin et que les services sont de nouveau disponibles.

2. Confirmer que le niveau de performance de référence des réseaux est rétabli.

3. Au besoin, installer les correctifs et les mises à jour sur les machines touchées.

4. Dans la mesure du possible, identifier l'origine de l'attaque. Solliciter l'aide du FAI.

5. Passer en revue les registres de journalisation pour y repérer la trace des tentatives de reconnaissance. Conserver ces registres en vue d'éventuelles poursuites judiciaires.

Leçons retenues:

1. Rédiger ou mettre à jour les documents suivants :
- Procédures d'opération normalisées
- Procédures d'opération d'urgence
- Plans de continuité des opérations

RECOMMANDATIONS

Le CCRIC recommande aux organisations d'évaluer les risques qu'elles soient exposées à des attaques par déni de service, qu'elles soient provoquées accidentellement ou volontairement. Elles sont invitées à prendre en considération les mesures d'atténuation conseillées dans le présent document et de les mettre en œuvre en fonction de leur propre environnement de GI-TI.

RÉFÉRENCES

1. US-CERT, Understanding Denial-of-Service Attacks (Comprendre les attaques par déni de service) http://www.us-cert.gov/cas/tips/ST04-015.html (en anglais)

2. NIST, Computer Security Incident Handling Guide (Guide de gestion des incidents touchant la sécurité informatique) http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf (en anglais)

3. GovCERT.NL, Factsheet: Protect your online services against dDoS attacks (Protégez vos services en ligne contre les attaques DSD) http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html (en anglais)

4. CERT Société Générale – Déni de service distribué http://cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf (en anglais)

SIGNALEMENT

Les opérateurs d'infrastructure critique canadiens peuvent signaler des incidents en utilisant la clé de chiffrement PGP de l'agent de cybersécurité de service du CCRIC (disponible à l'adresse http://www.publicsafety.gc.ca/prg/em/ccirc/enc-fra.aspx) et transmettre les rapports connexes par courriel à l'adresse [redacted] s.16(2)(c)

Les fichiers et échantillons potentiellement malveillants peuvent être envoyés au CCRIC à l'adresse : malware@ccirc-ccric.gc.ca. Les fichiers et courriels douteux devraient être compressés et protégés avec le mot de passe « infecté ».

NOTE CRUCIALE

Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à avertir le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique, notamment l'exploration, le téléchargement, le balayage, ou même une recherche Web selon tout texte du présent rapport.

AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Le présent message et toutes les pièces jointes qui l'accompagnent contiennent des renseignements qui peuvent avoir été recueillis de diverses sources externes dont le CCRIC ne peut vérifier ni la fiabilité ni l'intégrité. Le CCRIC n'assume aucune responsabilité pour des conséquences négatives résultant de l'utilisation des renseignements fournis dans la présente.

Les liens vers d'autres sites Web ne relevant pas du gouvernement du Canada sont fournis aux utilisateurs uniquement pour des raisons de commodité. Le gouvernement du Canada n'assume donc pas la responsabilité de l'exactitude, du caractère actuel ni de la fiabilité de leur contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites et leur contenu.

AVIS AUX LECTEURS

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la réponse aux incidents. Le CCRIC est responsable d'assurer la résilience de l'infrastructure essentielle nationale en contrôlant les menaces et en coordonnant une réponse fédérale aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement à l'égard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements de nature générale, veuillez communiquer avec la division des Affaires publiques de l'organisme.
Téléphone : 613-944-4875 ou 1-800-830-3118
Télécopieur : 613-998-9589
Courriel : communications@ps-sp.gc.ca

En cas d'urgence, veuillez communiquer avec le Centre des opérations du gouvernement (GOC).

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted] s.16(2)(c)

Slack, Jessica

From: Dick, Robert
Sent: February-23-12 3:48 PM
To: Slack, Jessica
Cc: Matz, Mark; Bencke, Ashley; Champoux, Martin; Filipps, Lisa
Subject: Re: FOR REVIEW/APPROVAL: Humber College request

I'd de-emphasize the "criminal". Second sentence: "Foreign governments, criminals, and others who would do us harm are taking advantage...". Second paragraph: "...these problems - rather, it is those who are..."

From: Slack, Jessica
Sent: Thursday, February 23, 2012 03:29 PM
To: Dick, Robert
Cc: Matz, Mark; Bencke, Ashley; Champoux, Martin; Filipps, Lisa
Subject: RE: FOR REVIEW/APPROVAL: Humber College request

Just checking in. Please advise you are ok with the proposed response.
Thanks,
Jessica

From: Slack, Jessica
Sent: February-22-12 9:41 AM
To: Dick, Robert
Cc: Matz, Mark; Bencke, Ashley; Champoux, Martin
Subject: FOR REVIEW/APPROVAL: Humber College request

Hi Robert,

s.19(1)

We received the inquiry below from a [redacted] at Humber – we are proposing a written response.

We've used some of the material from the written response provided to CBC on "cyberwarfare" and adapted it slightly. If you could let me know by **noon tomorrow** if you are ok with this, it would be most appreciated.
Jessica

PROPOSED RESPONSE
Rather than "online terrorism," the Government of Canada prefers to talk about cyber security because the real threats that we see every day are the use of cyberspace to facilitate crime. Criminals are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, spread criminal material like child pornography and conduct espionage, stealing trade secrets and research.

Technology itself not responsible for these problems – criminals are deliberately misusing and abusing the networks on which we rely.

The Government is committed to addressing these cyber threats as they are the most pressing for the country. In October 2010 the Government of Canada released Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government.

The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In

essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians.

The Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such as telecommunications networks, the financial sector, power grids and other vital systems – are getting the information they need to protect themselves and keep their systems secure. For example, the Canadian Cyber Incident Response Centre (CCIRC) monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats.

Another important element of the Strategy is Get Cyber Safe, the Government of Canada's national public awareness initiative. The getcybersafe.ca web site provides information that helps Canadians protect themselves and their families against a wide range of online threats.

Reporter's Name	[redacted]
Media Outlet	Humber
Call Date	2/21/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	2/24/2012 5:00 PM
Status	Consulting
Branch	
Subject	TBD
Questions	Clarification: "Groups like anonymous in particular. We're looking at this new age of crime an how the government has had to adapt to online terrorism and has had to take those extra precautions. Basically is this the future of crime, and how people in Canada can protect themselves on the Internet." ***** For a story on hackers, [redacted] wants to talk to someone re cyber security, [redacted] is looking for information re how the government is dealing with hackers and some stats on cases the GoC has had to deal with.

s.19(1)

Pages 68 to / à 69

are duplicates of

sont des duplicatas des

pages 74 to / à 75

Slack, Jessica

From: Slack, Jessica
Sent: February-23-12 4:47 PM
To: Mueller, Mike; Slack, Jessica; Issues / Enjeux; McDonald, Jessica; Dussault, Josée; Eke, Darren; Fournier, Martin; Leclair, Natalie; McAteer, Julie; McDonald, Andrea; McRae, Marley; Swift, Andrew; Therien, Stephane; Tomlinson, Jamie; Patton, Michael; Johnson, Mark; Manning, Kerri; Champoux, Martin; Stanfield, Charles; Paulson, Erika; Wilson, Barbara; Willey, Chris; Carmichael, Julie; Filipps, Lisa; Williams, Christpher; * Media Monitoring / Suivi des médias; Csversko, Christine
Subject: Daily Media Report / Rapport média quotidien

For your information, we received 2 new media calls on Thursday, February 23 2012 // Pour votre information, nous avons reçu 2 appels de médias le jeudi 23 février.

NEW

Reporter's Name	[redacted]
Media Outlet	CTV News Toronto
Call Date	2/23/2012 2:10 PM
Telephone	[redacted]
E-mail address	[redacted]@ctv.ca
Deadline	2/25/2012 9:00 PM
Status	Consulting
Branch	LPB
Subject	Missing Aboriginal Women
Questions	She is looking to speak to someone from the First Nations Policing Program regarding the UN meeting that took place on February 13 on missing aboriginal women across Canada. Here are few questions she will likely be asking: - What is the update from the meeting? The issue was supposed to be presented. Was it? What happened? - What has the police force here been doing about the case? - What are some of the challenges in solving this issue from their standpoint? - What is the next step? These are times available for the interview: - Saturday, February 25, 2012 (9 pm) - Sunday, February 26, 2012 (6pm or 8pm)

Reporter's Name	[redacted]
Media Outlet	CTV News
Call Date	2/23/2012 3:45 PM
Telephone	[redacted]
E-mail address	[redacted]@ctv.ca
Deadline	
Status	Final

Branch	
Subject	TBD
Questions	Looking for a copy of Bill C-30.
Reporter and Outlet	[redacted] - CTV News
Actions Taken	Picard, Josée (2/23/2012 4:19 PM): Sent the link to the reporter: http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5380965&file=4.

CLOSED

Reporter's Name	[redacted]
Media Outlet	Kings County Record
Call Date	2/21/2012 12:00 PM
Telephone	(902) 681-2121 ext [redacted]
E-mail address	
Deadline	2/23/2012 12:00 PM
Status	Background interview completed on Thursday
Branch	CSP
Subject	Aboriginal Community Constable Program
Questions	• How long was the Aboriginal Community Constable Program in place in Kings County, N.S.? • Does the program still exist? If so how many communities and in which provinces? • Why was the position in Kings County, N.S. converted to the Provincial Police Service Agreement? What does simplify administration mean? Did the federal government have multiple people responsible for monitoring these two programs? Did they lay off people as part of simplify administration? • What is the cost saving to the federal government in making this change? I know in Kings County the bands are picking up $25,000 the federal government used to cover. What's the impact nationally?

OUTSTANDING:

Reporter's Name	[redacted]
Media Outlet	Humber
Call Date	2/21/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	2/24/2012 5:00 PM
Status	In approvals
Branch	
Subject	TBD
Questions	Clarification: "Groups like anonymous in particular. We're looking at this new age of crime an how the government has had to adapt to online terrorism and has had to take those extra precautions. Basically is this the future of crime, and how people in Canada can protect themselves on the Internet." ***** For a story on hackers, [redacted] wants to talk to someone re cyber security, [redacted] is looking for information re how the government is dealing with hackers and some stats on cases the GoC has had to deal with.

Slack, Jessica

From: Slack, Jessica
Sent: February-23-12 5:08 PM
To: Swift, Andrew
Cc: Filipps, Lisa
Subject: Re: FOR REVIEW/APPROVAL: Humber College request

Ok..I did have links in at one point but must have been lost in cut and paste.
Will send to SD tomorrow am before the training.

From: Swift, Andrew
Sent: Thursday, February 23, 2012 04:53 PM
To: Slack, Jessica
Cc: Filipps, Lisa
Subject: RE: FOR REVIEW/APPROVAL: Humber College request

Jessica,
Some minor tweaks and suggestions for links below.
Andrew

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica
Sent: Thursday, February 23, 2012 4:36 PM
To: Swift, Andrew
Cc: Filipps, Lisa
Subject: FOR REVIEW/APPROVAL: Humber College request s.19(1)

Andrew, for approval-
Please see below for our proposed response to the inquiry we received from a [redacted] at Humber College.
This is adapted from the material we prepared for the CBC requests on cyberwarfare.
Robert Dick and Lisa have approved.

PROPOSED RESPONSE

The Government of Canada prefers to talk about cyber security rather than "online terrorism", because the real threats that we see every day are the use of cyberspace to facilitate crime. Foreign governments, criminals, and others who would do us harm are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, spread criminal material like child pornography, and conduct espionage, stealing trade secrets and research.

Technology itself is not responsible for these problems – rather, it is those who are deliberately misusing and abusing the networks on which we rely.

Page 73

is a duplicate of

est un duplicata de la

page 75

Slack, Jessica

From: Slack, Jessica
Sent: February-24-12 7:41 AM
To: Picard, Josée
Cc: Filipps, Lisa
Subject: Fw: FOR REVIEW/APPROVAL: Humber College request

I tht I was going to be able to get in early enough to do this but I have to meet consultants at 8;15 downstairs and I won't have time to come up first.

Josee when u get in do u mind sending this to stephanie for approval? Just incoroporate andrew's changes as below. Robert Dick, Lisa and Andrew have approved. If we could get it back by noon from her that wld be great. Go ahead and send to mo as well if it comes back from dgo before I get out of the training at noon. Reporter's deadline is actually monday but I wanted to get it to [redacted] today. Thanks very much.

From: Swift, Andrew
Sent: Thursday, February 23, 2012 04:53 PM
To: Slack, Jessica
Cc: Filipps, Lisa
Subject: RE: FOR REVIEW/APPROVAL: Humber College request

Jessica,
Some minor tweaks and suggestions for links below.
Andrew

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica
Sent: Thursday, February 23, 2012 4:36 PM
To: Swift, Andrew
Cc: Filipps, Lisa
Subject: FOR REVIEW/APPROVAL: Humber College request

Andrew, for approval-
Please see below for our proposed response to the inquiry we received from a [redacted] at Humber College.
This is adapted from the material we prepared for the CBC requests on cyberwarfare.
Robert Dick and Lisa have approved.

PROPOSED RESPONSE

The Government of Canada prefers to talk about cyber security rather than "online terrorism", because the real threats that we see every day are the use of cyberspace to facilitate crime. Foreign governments, criminals, and others who would do us harm are taking advantage of the communications opportunities of the internet to steal identities, traffic in

stolen data, spread criminal material like child pornography, and conduct espionage, stealing trade secrets and research.

Technology itself is not responsible for these problems – rather, it is those who are deliberately misusing and abusing the networks on which we rely.

The Government is committed to addressing these cyber threats as they are the most pressing for the country. In October 2010 the Government of Canada released Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government (INCLUDE LINK TO ANNCT).

The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada (INCLUDE LINK TO ANNCT) is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians.

The Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such as telecommunications networks, the financial sector, power grids and other vital systems – are getting the information they need to protect themselves and keep their systems secure. For example, the Canadian Cyber Incident Response Centre (CCIRC) monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats.

Another important element of the Strategy is Get Cyber Safe, the Government of Canada's national public awareness initiative. The getcybersafe.ca web site provides information that helps Canadians protect themselves and their families against a wide range of online threats.

Reporter's Name	[redacted]
Media Outlet	Humber
Call Date	2/21/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	2/24/2012 5:00 PM
Status	Consulting
Branch	
Subject	TBD
Questions	Clarification: "Groups like anonymous in particular. We're looking at this new age of crime an how the government has had to adapt to online terrorism and has had to take those extra precautions. Basically is this the future of crime, and how people in Canada can protect themselves on the Internet." ***** For a story on hackers, [redacted] wants to talk to someone re cyber security, [redacted] is looking for information re how the government is dealing with hackers and some stats on cases the GoC has had to deal with.

Slack, Jessica

From: Slack, Jessica
Sent: February-24-12 10:09 AM
To: Picard, Josée
Subject: Re: FOR DG APPROVAL: Humber College request

Thanks, Josee!

From: Picard, Josée
Sent: Friday, February 24, 2012 10:06 AM
To: Durand, Stéphanie
Cc: Slack, Jessica; Swift, Andrew; Filipps, Lisa; Salewski, Shawn; Bue, Richard; Dubé, Rosanne
Subject: FOR DG APPROVAL: Humber College request s.19(1)

Good morning Stéphanie,

Please see below for your approval, our proposed response to the inquiry we received from a [redacted] at Humber College – see details further below. This is adapted from the material we prepared for the CBC requests on cyberwarfare.

Robert Dick, Andrew Swift and Lisa have approved.

Many thanks.
Josée

PROPOSED RESPONSE

The Government of Canada prefers to talk about cyber security rather than "online terrorism", because the real threats that we see every day are the use of cyberspace to facilitate crime. Foreign governments, criminals, and others who would do us harm are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, spread criminal material like child pornography, and conduct espionage, stealing trade secrets and research.

Technology itself is not responsible for these problems – rather, it is those who are deliberately misusing and abusing the networks on which we rely.

The Government is committed to addressing these cyber threats as they are the most pressing for the country. In October 2010 the Government of Canada released Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government.

The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians.

The Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such as telecommunications networks, the financial sector, power grids and other

Page 77

is a duplicate of

est un duplicata de la

page 81

Dubé, Rosanne

From: Dubé, Rosanne
Sent: Friday, February 24, 2012 10:12 AM
To: Salewski, Shawn; Bue, Richard
Subject: RE: FOR DG APPROVAL: Humber College request

Printed for SD

Rosanne Dubé
Administrative Officer | Agente administrative
Office of the Director General, Communications | Bureau de la Directrice générale, Communications
Public Safety Canada | Sécurité publique Canada
Ottawa, Canada K1A 0P8
Telephone | Téléphone 613 949-4485 / Facsimile | Télécopieur 613 993-7062

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

s.19(1)

From: Picard, Josée
Sent: Friday, February 24, 2012 10:06 AM
To: Durand, Stéphanie
Cc: Slack, Jessica; Swift, Andrew; Filipps, Lisa; Salewski, Shawn; Bue, Richard; Dubé, Rosanne
Subject: FOR DG APPROVAL: Humber College request

Good morning Stéphanie,

Please see below for your approval, our proposed response to the inquiry we received from a [redacted] at Humber College – see details further below. This is adapted from the material we prepared for the CBC requests on cyberwarfare.

Robert Dick, Andrew Swift and Lisa have approved.

Many thanks.
Josée

PROPOSED RESPONSE

The Government of Canada prefers to talk about cyber security rather than "online terrorism", because the real threats that we see every day are the use of cyberspace to facilitate crime. Foreign governments, criminals, and others who would do us harm are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, spread criminal material like child pornography, and conduct espionage, stealing trade secrets and research.

Technology itself is not responsible for these problems – rather, it is those who are deliberately misusing and abusing the networks on which we rely.

The Government is committed to addressing these cyber threats as they are the most pressing for the country. In October 2010 the Government of Canada released Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government.

Page 79

is a duplicate of

est un duplicata de la

page 81

Bue, Richard

From: Durand, Stéphanie
Sent: February-24-12 12:18 PM
To: Picard, Josée
Cc: Slack, Jessica; Swift, Andrew; Filipps, Lisa; Salewski, Shawn; Bue, Richard; Dubé, Rosanne
Subject: RE: FOR DG APPROVAL: Humber College request

Fine by me.
Thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Picard, Josée
Sent: Friday, February 24, 2012 10:06 AM
To: Durand, Stéphanie
Cc: Slack, Jessica; Swift, Andrew; Filipps, Lisa; Salewski, Shawn; Bue, Richard; Dubé, Rosanne
Subject: FOR DG APPROVAL: Humber College request s.19(1)

Good morning Stéphanie,

Please see below for your approval, our proposed response to the inquiry we received from a [redacted] at Humber College – see details further below. This is adapted from the material we prepared for the CBC requests on cyberwarfare.

Robert Dick, Andrew Swift and Lisa have approved.

Many thanks.
Josée

PROPOSED RESPONSE

The Government of Canada prefers to talk about cyber security rather than "online terrorism", because the real threats that we see every day are the use of cyberspace to facilitate crime. Foreign governments, criminals, and others who would do us harm are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, spread criminal material like child pornography, and conduct espionage, stealing trade secrets and research.

Technology itself is not responsible for these problems – rather, it is those who are deliberately misusing and abusing the networks on which we rely.

The Government is committed to addressing these cyber threats as they are the most pressing for the country. In October 2010 the Government of Canada released Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government.

The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians.

The Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such as telecommunications networks, the financial sector, power grids and other vital systems – are getting the information they need to protect themselves and keep their systems secure. For example, the Canadian Cyber Incident Response Centre (CCIRC) monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats.

Another important element of the Strategy is Get Cyber Safe, the Government of Canada's national public awareness initiative. The getcybersafe.ca web site provides information that helps Canadians protect themselves and their families against a wide range of online threats.

Reporter's Name	[redacted]	s.19(1)
Media Outlet	Humber	
Call Date	2/21/2012 12:00 PM	
Telephone	[redacted]	
E-mail address		
Deadline	2/24/2012 5:00 PM	
Status	Consulting	
Branch		
Subject	TBD	
Questions	Clarification: "Groups like anonymous in particular. We're looking at this new age of crime an how the government has had to adapt to online terrorism and has had to take those extra precautions. Basically is this the future of crime, and how people in Canada can protect themselves on the Internet." ***** For a story on hackers, [redacted] wants to talk to someone re cyber security, [redacted] is looking for information re how the government is dealing with hackers and some stats on cases the GoC has had to deal with.	

Wilson, Barbara

From: Picard, Josée
Sent: Friday, February 24, 2012 1:30 PM
To: Wilson, Barbara
Subject: FW: FOR MO APPROVAL: Humber College request

Might be useful

From: Patton, Michael
Sent: Friday, February 24, 2012 12:39 PM
To: Filipps, Lisa; Carmichael, Julie; Johnson, Mark; Williams, Christpher
Cc: Durand, Stéphanie; Swift, Andrew; Slack, Jessica; Champoux, Martin; Stanfield, Charles; Picard, Josée
Subject: RE: FOR MO APPROVAL: Humber College request

approved

From: Filipps, Lisa
Sent: February-24-12 12:33 PM
To: Patton, Michael; Carmichael, Julie; Johnson, Mark; Williams, Christpher
Cc: Durand, Stéphanie; Swift, Andrew; Slack, Jessica; Champoux, Martin; Stanfield, Charles; Picard, Josée
Subject: FOR MO APPROVAL: Humber College request

s.19(1)

Mike/Julie – For your approval - proposed response for request by Humber College [redacted] on Cyber:

PROPOSED RESPONSE

The Government of Canada prefers to talk about cyber security rather than "online terrorism", because the real threats that we see every day are the use of cyberspace to facilitate crime. Foreign governments, criminals, and others who would do us harm are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, spread criminal material like child pornography, and conduct espionage, stealing trade secrets and research.

Technology itself is not responsible for these problems – rather, it is those who are deliberately misusing and abusing the networks on which we rely.

The Government is committed to addressing these cyber threats as they are the most pressing for the country. In October 2010 the Government of Canada released Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government.

The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians.

The Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such as telecommunications networks, the financial sector, power grids and other vital systems – are getting the information they need to protect themselves and keep their systems secure. For example,

the Canadian Cyber Incident Response Centre (CCIRC) monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats.

Another important element of the Strategy is Get Cyber Safe, the Government of Canada's national public awareness initiative. The getcybersafe.ca web site provides information that helps Canadians protect themselves and their families against a wide range of online threats.

Reporter's Name	[redacted]
Media Outlet	Humber
Call Date	2/21/2012 12:00 PM
Telephone	[redacted] s.19(1)
E-mail address	
Deadline	2/24/2012 5:00 PM
Status	Consulting
Branch	
Subject	TBD
Questions	Clarification: "Groups like anonymous in particular. We're looking at this new age of crime an how the government has had to adapt to online terrorism and has had to take those extra precautions. Basically is this the future of crime, and how people in Canada can protect themselves on the Internet." ***** For a story on hackers, [redacted] wants to talk to someone re cyber security, [redacted] s looking for information re how the government is dealing with hackers and some stats on cases the GoC has had to deal with.

Slack, Jessica

From: Swift, Andrew
Sent: February-24-12 5:15 PM
To: Picard, Josée; Slack, Jessica; Filipps, Lisa
Subject: RE: Daily Media Report / Rapport média quotidien

Busy day! Thanks everyone, have a good weekend!

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Picard, Josée
Sent: Friday, February 24, 2012 4:57 PM
To: Slack, Jessica; Issues / Enjeux; McDonald, Jessica; Dussault, Josée; Eke, Darren; Fournier, Martin; Leclair, Natalie; McAteer, Julie; McDonald, Andrea; McRae, Marley; Swift, Andrew; Therien, Stephane; Tomlinson, Jamie; Patton, Michael; Johnson, Mark; Manning, Kerri; Champoux, Martin; Stanfield, Charles; Paulson, Erika; Wilson, Barbara; Willey, Chris; Carmichael, Julie; Filipps, Lisa; Williams, Christpher; * Media Monitoring / Suivi des médias; Csversko, Christine; Picard, Josée
Subject: Daily Media Report / Rapport média quotidien

For your information, we received 5 new media calls on Friday, February 24 2012 // Pour votre information, nous avons reçu 5 appels de médias le vendredi 24 février.

NEW

Reporter's Name	[redacted]
Media Outlet	Computer World
Call Date	2/24/2012 1:15 PM
Telephone	416-290-0240 ext: [redacted]
E-mail address	[redacted]@itworldcanada.com
Deadline	2/24/2012 4:00 PM
Status	Response sent to the reporter - **CLOSED**
Branch	NS
Subject	Cyber Security
Questions	The reporter is doing a piece on cyber security in Canada, specifically regarding the report from Queens University, entitled: Evolving Transnational Threats and Border Security. The report includes a section on Canada and mentions that the Canadian Government is falling behind in the cyber security arena and that the Cyber Strategy launched in the fall of 2010 is too little too late. The reporter is looking to get Public Safety's comments on the report and on the overall strategy and what has changed since 2010.
Final Response	In October 2010, after careful consultations and analysis, the Government of Canada

s.19(1)

released Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government. Canada's Strategy is closely aligned in substance and timing with those of our partners.

In addition to existing resources, the strategy invested an additional $90 million over five years, and $18 million in ongoing funding to strengthen Canada's cyber security. These resources allow the Government to take concrete action to meet the evolving cyber threat.

Canada's Cyber Security Strategy is built on three pillars:

1. Securing government systems;

2. Partnering to secure vital cyber systems outside the Federal Government; and

3. Helping Canadians to be secure online.

In deploying the first pillar, the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians.

In fulfilling elements of the second pillar, the Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such as telecommunications networks, the financial sector, power grids and other vital systems – are getting the information they need to protect themselves and keep their systems secure. For example, the Canadian Cyber Incident Response Centre (CCIRC) monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats. We have clarified roles and mandates of both the CCIRC and the Communications Security Establishment of Canada (CSE) in order to strengthen and improve Canada's ability to identify, prevent and mitigate cyber security incidents.

A third pillar focuses on providing Canadians with the awareness and tools to help stay secure while online. An important element is the Strategy is Get Cyber Safe, the Government of Canada's national public awareness initiative. The getcybersafe.ca web site provides information that helps Canadians protect themselves and their families against a wide range of online threats.

Reporter's Name	[redacted]
Media Outlet	Newcap Radio
Call Date	2/24/2012 4:00 PM
Telephone	[redacted] s.19(1)
E-mail address	[redacted]
Deadline	2/24/2012 6:00 PM
Status	Consulting
Branch	NS
Subject	Fireball
Questions	Reporter is looking for the raw data (doppler radar data) that would have been used to show the altitude/track of the fireball that landed near Rockhaven/North Battleford area of Saskatchewan.
Reporter and Outlet	[redacted] - Newcap Radio
Actions Taken	No existing entries.

Reporter's Name	[redacted]
Media Outlet	Postmedia News
Call Date	2/24/2012 1:35 PM
E-mail address	[redacted]@postmedia.com
Deadline	2/24/2012 4:00 PM
Status	Response sent to the reporter - **CLOSED**
Branch	LPB
Subject	RCMP Policing Agreement
Questions	Follow-up questions:

s.19(1)

So agreements in principle have been completed with every province and territory, and are only waiting on approval by the provincial governments? With Nova Scotia's signing today, how many (and which) governments have finalized their deals? Was the agreement today just an agreement in principle? I don't know how these things are implemented, or if there is a possibility for change after the initial agreement.

I'm just wondering what Nova Scotia's agreement today means. Was it the final province to sign before the April deadline? Did all provinces face that same deadline?

Please let me know if there's someone I can speak to about this.

Final Response

So agreements in principle have been completed with every province and territory, and are only waiting on approval by the provincial governments? With the exception of Alberta and Saskatchewan, whose agreements were already finalized in the summer, and those jurisdictions that do not have Police Service Agreements (Quebec and Ontario), we are just waiting for the rest to advise officially that their province or territory has obtained the necessary authority they would require in order to enter into the agreement.

With Nova Scotia's signing today, how many (and which) governments have finalized their deals? Was the agreement today just an agreement in principle? I don't know how these things are implemented, or if there is a possibility for change after the initial agreement. Nova Scotia is the third province to officially advise that they have reached final agreement. While we have not heard officially from the remaining provinces and territories, further changes to the agreements in principle are not anticipated.

Did all provinces face that same deadline? Yes, all RCMP Police Services Agreements (PSAs) expire on March 31, 2012. The new (2012–2032) Agreements will take effect on April 1. Alberta and Saskatchewan have signed the new Agreements.

Reporter's Name	[redacted]
Media Outlet	PostMedia News
Call Date	2/24/2012 12:30 PM
Telephone	[redacted]
E-mail address	[redacted]@postmedia.com
Deadline	2/24/2012 4:00 PM
Status	Response sent to the reporter - **CLOSED**

Branch	LPB
Subject	RCMP Policing Agreement
Questions	In light of this morning's announcement of the NS RCMP Policing Agreement with the RCMP, what is the status of RCMP Contract negotiations/renewal with the other provinces and territories?
Final Response	As per your question regarding the status of RCMP Contract negotiations/renewal with the other provinces and territories, I can tell you that Alberta and Saskatchewan have already signed their new Agreements. Agreement in principle was reached with the remaining contract jurisdictions in November 2011, and we are now awaiting the official response from the Provinces and Territories on their government's formal approval of the Agreement.

Reporter's Name	
Media Outlet	CP Halifax
Call Date	2/24/2012 12:00 PM
Telephone	902-422-8496 ext.
E-mail address	Halifax@thecanadianpress.com
Deadline	2/24/2012 12:30 AM
Status	Response sent to the reporter - **CLOSED**
Branch	LPB
Subject	RCMP Policing Contract
Questions	Calling regarding the statement issued by the RCMP about NS reaching a policing agreement with the RCMP. Doesn't understand why there's a separate release for NS, he thought that NS was negotiating as part of a larger group. He wants to know why NS was singled out in a separate release.
Final Response	- Alberta and Saskatchewan have already signed their new Agreements. Agreement in principle was reached with the remaining contract jurisdictions in November 2011, and we are now awaiting the official response from the Provinces and Territories on their government's formal approval of the Agreement. - This announcement is to signal that the Governments of Canada and Nova Scotia have reached a final agreement. We will announce each agreement as they are finalized.

CLOSED

Reporter's Name	
Media Outlet	CTV News Toronto
Call Date	2/23/2012 2:10 PM
Telephone	
E-mail address	@ctv.ca
Deadline	2/25/2012 9:00 PM
Status	Referred to DFAIT - **CLOSED**

Branch	LPB
Subject	Missing Aboriginal Women
Questions	She is looking to speak to someone from the First Nations Policing Program regarding the UN meeting that took place on February 13 on missing aboriginal women across Canada. Here are few questions she will likely be asking: - What is the update from the meeting? The issue was supposed to be presented. Was it? What happened? - What has the police force here been doing about the case? - What are some of the challenges in solving this issue from their standpoint? - What is the next step? These are times available for the interview: - Saturday, February 25, 2012 (9 pm) - Sunday, February 26, 2012 (6pm or 8pm)
Reporter's Name	[redacted]
Media Outlet	Humber
Call Date	2/21/2012 12:00 PM
Telephone	[redacted]
Deadline	2/24/2012 5:00 PM
Status	Response sent to the reporter - **CLOSED**
Branch	Cyber
Subject	Cyber Security
Questions	**Clarification:** "Groups like anonymous in particular. We're looking at this new age of crime an how the government has had to adapt to online terrorism and has had to take those extra precautions. Basically is this the future of crime, and how people in Canada can protect themselves on the Internet." ***** For a story on hackers, [redacted] wants to talk to someone re cyber security, [redacted] is looking for information re how the government is dealing with hackers and some stats on cases the GoC has had to deal with.
Final Response	The Government of Canada prefers to talk about cyber security rather than "online terrorism", because the real threats that we see every day are the use of cyberspace to facilitate crime. Foreign governments, criminals, and others who would do us harm are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, and conduct espionage, stealing trade secrets and research. Technology itself is not responsible for these problems – rather, it is those who are deliberately misusing and abusing the networks on which we rely. The Government is committed to addressing these cyber threats as they are the most pressing for the country. In October 2010 the Government of Canada released Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government. The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians. The Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such as telecommunications networks, the financial sector, power grids and other vital systems – are getting the information they need to protect themselves and keep their systems secure. For example, the Canadian Cyber Incident Response Centre (CCIRC) monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats. Another important element of the Strategy is Get Cyber Safe, the Government of Canada's national public awareness initiative. The getcybersafe.ca web site provides information that helps Canadians protect themselves

and their families against a wide range of online threats.

Swift, Andrew

From: Patton, Michael
Sent: Saturday, February 25, 2012 3:09 PM
To: Swift, Andrew; Carmichael, Julie; Johnson, Mark; Mueller, Mike
Cc: Durand, Stéphanie; Filipps, Lisa
Subject: RE: CBC NEWS REQUEST

Categories: ATI PRINT

Andrew,

Responding now

With

"Healthy debate among citizens about changes to legislation is important.

However it is unacceptable when that debate degrades into threats against individuals. Canada's laws do not adequately protect against online child exploitation and other criminal activity. We want to fix our laws while striking the right balance when it comes to protecting privacy.

We are sending this legislation directly to Committee for a full examination of potential amendments to achieve the best protection for our children."

This is closed

From: Swift, Andrew
Sent: February-25-12 2:34 PM
To: Patton, Michael; Carmichael, Julie; Johnson, Mark; Mueller, Mike
Cc: Durand, Stéphanie; Filipps, Lisa
Subject: CBC NEWS REQUEST

Mike,
See questions below for the Minister from CBC. Let me know if you will get back to the reporter.
Thanks,
Andrew

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: PS Media Relations / Relations médias SP
Sent: Saturday, February 25, 2012 12:51 PM
To: Swift, Andrew; Slack, Jessica; McDonald, Jessica; Picard, Josée; Filipps, Lisa
Subject: FW: CBC NEWS REQUEST

From:
Sent: Saturday, February 25, 2012 12:51:48 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject: CBC NEWS REQUEST

Hi there,

I'm a with CBC News: The National in Toronto. I'm hoping to get a statement from Minister Vic Toews today regarding the online outcry against Bill C-30 and the latest attack by Anonymous. The hacker group Anonymous has taken down the Ontario Association of Chiefs of Police website because of their support of bill C-30. They've also posted personal information about OACP members online. What does Minster Toews make of this recent tactic by Anonymous? What does Minster Toews make of the threats against him online and his personal information being exposed? What impact is all of this having on the actual message your government wants to send to the public regarding Bill-C30?

Hoping to get this statement before 3:45pmET today. we are working on a story that will air at 5pmET today.

Thank you,

CBC News: The National
@cbc.ca

Slack, Jessica

From: Swift, Andrew
Sent: February-25-12 3:24 PM
To: COMDO; Filipps, Lisa; Picard, Josée; Slack, Jessica
Subject: Re: Message on the media line - CBC National Television Toronto

Thanks Sean, they wrote by email as well and I flipped it to the MO to respond.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: COMDO
Sent: Saturday, February 25, 2012 03:12 PM
To: Filipps, Lisa; Picard, Josée; Slack, Jessica; Swift, Andrew
Subject: Message on the media line - CBC National Television Toronto

CBC National Television News – Toronto

Reporter was wondering if s could get a statement or interview with Minister Toews before 3pm today (a little late I guess...), regarding Bill C-30, the online outcry against it and Anonymous taking down the Ontario Police Chiefs website.

I just started my shift, so I'm unaware how long ago the call came in at.

Sean Despard
Communications Duty Officer/ Agent de service des communications
Government Operations Centre/ Centre des opérations du gouvernement
Tel.: (613) 991-7010
Fax/Télécopieur: (613) 996-0995
Email/courriel: COMDO@ps-sp.gc.ca

Slack, Jessica

From: Swift, Andrew
Sent: February-27-12 8:46 AM
To: * Media Monitoring / Suivi des médias
Cc: Durand, Stéphanie
Subject: MO Request: Anon videos

See urgent request below. I know Sean found a transcript of one of the videos before. Not sure how many there at this point.

Could someone please look right away into a) how many videos re C-30 and b) see if they can track down existing transcripts on-line?

Thx.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Patton, Michael
Sent: Monday, February 27, 2012 08:39 AM
To: Swift, Andrew
Cc: Filipps, Lisa; Carmichael, Julie; Johnson, Mark
Subject: Anon videos

Andrew would it be possible to get transcripts of the Anonymous Videos this morning?
Mike Patton
Communications, Minister of Public Safety

COMDO

From: Turner, Jessica
Sent: Monday, February 27, 2012 9:40 AM
To: Swift, Andrew
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; COMDO; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Miller, Kevin; Orton, Karolina; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica
Subject: Transcripts for all 3 videos.

Video 3:

1. Hello, Mr. Toews.
2.
3. We are Anonymous.
4.
5. You have now had several days to reflect upon your actions.
6.
7. You have yet to apologize to the Canadian people for referring to them as supporters of pedophilia, or for attempting to infringe on their civil rights. You have stated that you are "open to amendments" on Bill C-30, which has been referred to committee for review.
8.
9. This is not sufficient.
10.
11. It has become very apparent that the purpose of Bill C-30 was never to prevent the distribution of child pornography. This is not merely a matter of opinion. You yourself, Mr. Toews, have submitted a piece to multiple media outlets, stating that Bill C-30 would allow police to crack down on, quote, "identity theft, online organized crime, and many Internet scams and frauds."
12.
13. In only a matter of days, we have gone from preventing child pornography to something as vague as cracking down on, quote "online organized crime". How convenient it is that Bill C-30 has come into prominence at the same time as Bill C-11, an online copyright bill which criminalizes Canadian citizens making personal copies of media they have legally purchased, would block Canadian access to websites deemed to be criminal by the authorities, and would force service providers to terminate service to customers for acts as innocuous as sharing mp3s.
14.
15. Interestingly, it would be possible under Bill C-11 to block Canadian access to YouTube, the site on which this video is hosted, on the basis that it facilitates online piracy.

16.

17. In short, this government's definition of "online organized crime" is so extreme that it includes online activities engaged in by the majority of Canadians.

18.

19. Most telling of all, Bill C-30 was originally named, "An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts". This intentionally vague and confusing title, obviously designed to obscure the bill's true purpose, was later changed to the "Protecting Children From Internet Predators Act", to better sell this massive intrusion of privacy to the Canadian people.

20.

21. Mr. Toews, your pattern of obfuscation and deception has only continued. We are growing impatient.

22.

23. Anonymous has warned you this is only beginning.

24.

25. Over the past several days, we have been inundated with messages exposing all manner of political wrongdoings and personal scandals, some of which extend to the very highest levels of your government.

26.

27. However, there is one incident, Mr. Toews, that the Canadian public would find particularly interesting. It is an act that you concealed so well that it does not appear in the affidavits from your divorce. In fact, we highly suspect neither your first wife, your former mistress, nor your political peers are aware of it. This incident pertains not only to your personal life, but to the direct abuse of your political position. Information about this incident has been submitted to us multiple times, independently, by both named and anonymous sources.

28.

29. Think very hard, Mr. Toews. As we said previously, we have no doubt that there are many skeletons in your closet. However, upon reflection, you should be able to determine which incident on the lengthy list of your illicit activities we are referring to.

30.

31. There is a very real possibility that after the revelation of this incident, Mr. Toews, that public outrage will not be necessary for you to find yourself without a job. It is already widely known that you have engaged in criminal activity to further your political career, as you did in 1999, when you were convicted of violating Manitoba's Election Finances Act during a provincial election.

32.

33. Perhaps you are under the illusion that if you simply allow enough time to pass, the public will lose interest in the controversy over Bill C-30, allowing it to pass unprotested. Perhaps you are under the impression that

there is no scandal so great it cannot destroy your reputation and career. Perhaps you are under the impression that we are bluffing.

34.

35. We are not bluffing, Mr. Toews. You have seven days to reflect upon your personal and political crimes. After that, the Canadian people will be made aware of just how disgustingly unscrupulous and corrupt you are.

36.

37. And to the rest of those who support Bill C-30: do not believe for a moment that you are untouchable. Anonymous has received information implicating many of you in both political and personal scandals. This government has already been shaken by Mr. Toews' disgusting remarks and hypocrisy, it's attempts to legalize spying on Canadian citizens, and the revelation that you have used robocalls to intentionally keep voters away from the polls. Directing voters to incorrect or non-existent polling stations is voter suppression, and is illegal under the Canada Elections Act.

38.

39. Let the next seven days serve as a period of reflection for the entire House of Commons. Ask yourselves, how many more scandals can you afford? How many more of your crimes shall be revealed to the Canadian people?

40.

41. A government that allows it's citizens no secrets will not be allowed any secrets of it's own. Anonymous calls upon everyone and anyone who does not support governmental spying on Canadian citizens to submit information on any personal scandal, crime, or abuse of power committed by any politician who supports Bill C-30. An email address for this purpose can be found in the description below this video. Anonymous will never name or reveal it's sources.

42.

43. The Canadian people have spoken. They do not support Bill C-30. You ignore their outcry at the peril of your own careers. The True North is strong and free, and we will never surrender our freedom, least of all to fear-mongering hypocrites who attempt to wrench it from us through subterfuge and deception.

44.

45. Anonymous demands the immediate resignation of Vic Toews, the scrapping of Bills C-30 and C-11 in their entirety, and a formal apology to the people of Canada for referring to them as supporters of pedophilia, and more importantly, for attempting to infringe on their most basic civil rights.

46.

47. We are Anonymous.

48.

49. We are Legion.

50.

51. We do not forgive.

52.

53. We do not forget.
54.
55. Expect us.

Video 2:

1. Anonymous - Operation Great White North / Operation Vic.Tory
2.
3. Send your Vikileaks to AnonymousCanada@hush.com
4.
5. *** Transcript***
6.
7. Hello Mr. Toews. We are Anonymous. Over the past several days, we have been watching you.
8.
9. You have continued to deceive the Canadian people by claiming that the information made accessible to police by Bill c-30 is no greater than that which can be found in a phonebook. Tell us Mr. Toews, in what phonebook can you find an individual's internet browsing history? Their private emails? Their financial information? Their credit card number? And all their personal contacts?
10.
11. How convenient it is that you fail to mention Bill C-30 would not only allow police access to this information without a warrant, but would make it illegal for internet service providers to inform their customers that their information has been accessed by the RCMP or CSIS.
12.
13. You have continued to waste the Canadian public's time and money by demanding a parliamentary investigation into the legal release of public records. We are not shocked in the slightest, as this is consistent with your pattern of ignoring true wrongdoings in favour of feigning moral outrage.
14.
15. What is shocking-- not to mention extremely disturbing-- is that you have claimed you are surprised by the contents of Bill C-30, a bill that you yourself tabled. This is a pathetically transparent attempt to feign ignorance in the face of a massive public backlash. However, let us imagine for a moment that you are telling the truth. Let us imagine that you, an elected official in the House of Commons, either did not take the time or are simply too dimwitted to understand a piece of legislation that you yourself championed. A piece of legislation that legalizes governmental

spying on Canadian citizens, and effectively ends the right to privacy in this country.

16.

17. This alone is grounds for you to tender your immediate resignation. The fact that you spun this catastrophic failure to perform your duties as an argument in your own defense would be laughable were the consequences not so dire.

18.

19. Of course, we all know this is simply another addition to your ever-growing web of lies. And this isn't the first time you have found yourself tangled up in your own web of deceit, is it, Mr. Toews?

20.

21. The Canadian public is now well aware that you carried on multiple affairs during your 30-year marriage to your first wife, all the while selling yourself as a devout Christian who championed so-called traditional family values.

22.

23. Quote: "Marriage is a uniquely heterosexual institution, that indeed is a sacrament. Marriage is one of the cornerstones upon which our society has been built."

24.

25. And yet, even after demonstrating you do not believe a single word of that statement, you continue to imply that your dedication to your personal family relationships makes you a suitable candidate for political office.

26.

27. Anonymous has gained access to a letter you recently sent to your constituents. In it, you quote Yeats:

28.

29. "All this life can give us is a child's laughter; a woman's kiss."

30.

31. Do you think the Canadian people are stupid, Mr. Toews? Do you honestly think that quoting saccharine poetry to us is going to convince us you are a God-fearing family man? Especially now that you are living in a common-law relationship with your former mistress, the very sort of relationship you turned your nose up at when it suited your political interests.

32.

33. Mr. Toews, you have used the illusion of a traditional family life, faith, and moral values as tools in your desperate bid for power, all the while trampling on the rights of others. You have used your own family as pawns in the creation of this illusion. Once again, you have inserted your spouse and children into this debate as rhetorical devices.

34.

35. We warned you that you would not be allowed any secrets if you did not allow the Canadian public any secrets of their own.

36.

37. Therefore, we are naming the woman you referenced in this letter to your constituents.

38.

39. The woman Vic Toews is cohabitating with, whom he impregnated in an affair that took place during his first marriage, is Stacey Meek. She is employed in an administrative capacity by Senator Terry Stratton. She runs a public relations firm based in Toronto. She previously worked for Conservative MP Joy Smith, and is currently listed as a constituency assistant for Conservative MP Joyce Bateman. In the past, she was employed by Issues Ink, a consulting and publishing company based in Winnipeg.

40.

41. Of course, we're sure you had absolutely nothing to do with Stacey Meek being hired by Senator Stratton, Mr. Toews. Surely a man like yourself with such solid moral convictions would never engage in that kind of nepotism!

42.

43. She has a father, Joe, who is a doctor of veterinary medicine; a brother, Jeff; a sister-in law, Rhea; and two nieces who we shall not name, all of whom reside in Winnipeg. Her mother is deceased and passed away due to cancer in in 2002.

44.

45. We also have information about your youngest son, who was the product of your affair with Ms. Meek. However, as he is only 4 years-old and entirely innocent in this matter, we will not release this information. Anonymous does not hold the son responsible for the crimes of the father.

46.

47. However, the woman you are cohabitating with is politically active, a government employee, and in particular is a constituency assistant to MP Joyce Bateman, who voted Yes on Bill C-30. As such, we have no qualms about releasing information about her to the Canadian public.

48.

49. We have also decided not to release your personal contact information, such as your phone number and address, at this time, as we understand you have received credible violent threats from members of the public.

50.

51. Shall we continue, Mr. Toews? Do we have your attention? How does it feel to have personal information about your family in the hands of people you know nothing about, with no control over who disseminates it or how it will be used?

52.

53. Let it be known this is only a taste of the information we have access to. And this is only the beginning.

54.

55. And yet, it is nothing compared to the personal information of millions of Canadians that will be collected, stored, and scrutinized by the authorities if Mr. Toews and this corrupt government are allowed to pass Bill C-30. If

this outrageous piece of legislation is allowed to pass, the government will have access to massive legally-required databases filled with information on your spouses, your children, your parents, your brothers, your sisters, your friends and your neighbours.

56.

57. Let it be known, Mr. Toews, that Anonymous will do to corrupt politicians exactly what you are attempting to do to the Canadian public. There will be no two-tier system of privacy for the government and the people of this country. You, and any public official who spies or support spying on Canadian citizens, will reap exactly what you have sewn.

58.

59. It would appear you have made many political enemies, Mr. Toews. Since Anonymous made an email address available through which the public can submit more Vikileaks, we have received no less than a dozen emails from your peers in Ottawa, several of whom have offered information or have made offers to provide us with information. And that does not include the messages from members of the public who know you in a personal capacity.

60.

61. And to the rest of the Parliament of Canada: you would do well to mind your words about Anonymous. Any attempt to score political points by claiming we are associated with a particular political party will not be met kindly. Your party affiliations are utterly irrelevant to us. Our only interest in this matter is protecting the freedom of information, and protecting the privacy of Canadians from the tyranny of our own government.

62.

63. Anonymous demands the immediate resignation of Vic Toews, the scrapping of Bills C-30 and C-11 in their entirety, and a formal apology to the people of Canada for referring to them as supporters of pedophiles, and importantly, for attempting to undermine their most basic civil rights.

64.

65. We are Anonymous.

66.

67. We are Legion.

68.

69. We do not forgive.

70.

71. We do not forget.

72.

73. Expect us.

Video 1:

1. Welcome to Operation Vic.Tory / Operation Great White North.

2.

3. Below is the contact information of every MP who voted yes on Bill C-11, the Canadian version of SOPA. It was tabled by the dishonorable Christian Paradis. There have been no votes on Bill C-30 as of yet. Let this serve as an example so it remains that way, indefinitely.
4.
5. The ".c1" after the name of each MP allows you to email them personally. Removing it will also allow you contact them, but it will be directed to their Ottawa offices and processed by their staff.
6.
7. Though it is not widely known, you can call your federal MP at their Ottawa office, toll-free, from anywhere in Canada via the Library of Parliament at 1-866-599-4999.
8.
9. Demand that Vic Toews step down, and that the intrusive, exploitative Bills C-30 & C-11 be scrapped in their entirety.
10.
11. We will do our duty; it is time for Canada to do hers.
12.
13.
14.
15. Voted Yes on Bill C-11:
16.
17. ***NOTE - The ".c1" after the name of each MP allows you to email them personally. Removing it will also allow you contact them, but it will be directed to their Ottawa offices and processed by their staff.***
18.
19. ***Vic Toews - vic.toews@parl.gc.ca - 613-992-3128***
20.
21. ***Christian Paradis - christian.paradis@parl.gc.ca - 613-995-1377***
22.
23.
24.
25. Diane Ablonczy - diane.ablonczy.c1@parl.gc.ca - 613-996-2756
26.
27. Eve Adams - eve.adams.c1@parl.gc.ca - 613-995-7784
28.
29. Mark Adler - mark.adler.c1@parl.gc.ca - 613-941-6339
30.
31. Leona Aglukkaq - leona.aglukkaq.c1@parl.gc.ca - 613-992-2848
32.
33. Dan Albas - Dan.Albas.c1@parl.gc.ca - 613-995-1702
34.
35. Harold Albrecht - harold.albrecht.c1@parl.gc.ca - 613-992-4633
36.
37. Mike Allen - mike.allen.c1@parl.gc.ca - 613-947-4431

38.

39. Dean Allison - dean.allison.c1@parl.gc.ca - 613-995-2772

40.

41. Stella Ambler - Stella.Ambler.c1@parl.gc.ca - 613-992-4848

42.

43. Rona Ambrose - rona.ambrose.c1@parl.gc.ca - 613-996-9778

44.

45. Rob Anders - rob.anders.c1@parl.gc.ca - 613-992-3066

46.

47. David Anderson - david.anderson.c1@parl.gc.ca - 613-995-8042

48.

49. Scott Armstrong - scott.armstrong.c1@parl.gc.ca - 613-992-3366

50.

51. Jay Aspin - Jay.Aspin.c1@parl.gc.ca - 613-995-6255

52.

53. John Baird - john.baird.c1@parl.gc.ca - 613-996-0984

54.

55. Joyce Bateman - Joyce.Bateman.c1@parl.gc.ca - 613-992-9475

56.

57. Leon Benoit - leon.benoit.c1@parl.gc.ca - 613-992-4171

58.

59. Maxime Bernier - maxime.bernier.c1@parl.gc.ca - 613-992-8053

60.

61. Steven Blaney - steven.blaney.c1@parl.gc.ca - 613-992-7434

62.

63. Kelly Block - kelly.block.c1@parl.gc.ca - 613-995-1551

64.

65. Ray Boughen - ray.boughen.c1@parl.gc.ca - 613-992-9115

66.

67. Peter Braid - peter.braid.c1@parl.gc.ca - 613-996-5928

68.

69. Garry Breitkreuz - garry.breitkreuz.c1@parl.gc.ca - 613-992-4394

70.

71. Gord Brown - gord.brown.c1@parl.gc.ca - 613-992-8756

72.

73. Lois Brown - lois.brown.c1@parl.gc.ca - 613-992-9310

74.

75. Patrick Brown - patrick.brown.c1@parl.gc.ca - 613-992-3394

76.

77. Rod Bruinooge - rod.bruinooge.c1@parl.gc.ca - 613-995-7517

78.

79. Brad Butt - Brad.Butt.c1@parl.gc.ca - 613-943-1762

80.

81. Paul Calandra - paul.calandra.c1@parl.gc.ca - 613-992-3640

82.

83. Blaine Calkins - blaine.calkins.c1@parl.gc.ca - 613-995-8886
84.
85. Ron Cannan - ron.cannan.c1@parl.gc.ca - 613-992-7006
86.
87. John Carmichael - John.Carmichael.c1@parl.gc.ca - 613-992-2855
88.
89. Colin Carrie - colin.carrie.c1@parl.gc.ca - 613-992-3640 - 613-996-4756
90.
91. Michael Chong - michael.chong.c1@parl.gc.ca - 613-992-4179
92.
93. Rob Clarke - rob.clarke.c1@parl.gc.ca - 613-995 - 8321
94.
95. Tony Clement - tony.clement.c1@parl.gc.ca - 613-944-7740
96.
97. Joe Daniel - Joe.Daniel.c1@parl.gc.ca - 613-995-4988
98.
99. Patricia Davidson - pat.davidson.c1@parl.gc.ca - 613-957-2649
100.
101. Bob Dechert - bob.dechert.c1@parl.gc.ca - 613-995-7321
102.
103. Dean Del Mastro - dean.delmastro.c1@parl.gc.ca - 613-995-6411
104.
105. Barry Devolin - barry.devolin.c1@parl.gc.ca - 613-992-2474
106.
107. Earl Dreeshen - earl.dreeshen.c1@parl.gc.ca - 613-995-0590
108.
109. John Duncan - john.duncan.c1@parl.gc.ca - 613-992-2503
110.
111. Rick Dykstra - rick.dykstra.c1@parl.gc.ca - 613-992-3352
112.
113. Julian Fantino - julian.fantino.c1@parl.gc.ca - 613-996-4971
114.
115. Kerry-Lynne Findlay - Kerry-Lynne.Findlay.c1@parl.gc.ca - 613-992-2957
116.
117. Diane Finley - diane.finley.c1@parl.gc.ca - 613-996-4974
118.
119. Jim Flaherty - jim.flaherty.c1@parl.gc.ca - 613-992-6344
120.
121. Parm Gill - Parm.Gill.c1@parl.gc.ca - 613-995-4843
122.
123. Shelly Glover - shelly.glover.c1@parl.gc.ca - 613-995-0579
124.
125. Robert Goguen - Robert.Goguen.c1@parl.gc.ca - 613-992-8072
126.
127. Peter Goldring - peter.goldring.c1@parl.gc.ca - 613-992-3821

Gary Goodyear - gary.goodyear.c1@parl.gc.ca - 613-992-3821

Bal Gosal - Bal.Gosal.c1@parl.gc.ca - 613-992-9105

Jacques Gourde - jacques.gourde.c1@parl.gc.ca - 613-992-2639

Nina Grewal - nina.grewal.c1@parl.gc.ca - 613-996-2205

Richard Harris - richard.harris.c1@parl.gc.ca - 613-995-6704

Laurie Hawn - laurie.hawn.c1@parl.gc.ca - 613-992-4524

Bryan Hayes - Bryan.Hayes.c1@parl.gc.ca - 613-992-9723

Russ Hiebert - russ.hiebert.c1@parl.gc.ca - 613-947-4497

Jim Hillyer - Jim.Hillyer.c1@parl.gc.ca - 613-996-0633

Randy Hoback - randy.hoback.c1@parl.gc.ca - 613-995-3295

Candice Hoeppner - candice.hoeppner.c1@parl.gc.ca - 613-995-9511

Ed Holder - ed.holder.c1@parl.gc.ca - 613-996-6674

Roxanne James - Roxanne.James.c1@parl.gc.ca - 613-992-6823

Brian Jean - brian.jean.c1@parl.gc.ca - 613-992-1154

Randy Kamp - randy.kamp.c1@parl.gc.ca - 613-947-4613

Gerald Keddy - gerald.keddy.c1@parl.gc.ca - 613-996-0877

Jason Kenney - jason.kenney.c1@parl.gc.ca - 613-992-2235

Peter Kent - peter.kent.c1@parl.gc.ca - 613-992-0253

Ed Komarnicki - ed.komarnicki.c1@parl.gc.ca - 613-992-7685

Daryl Kramp - daryl.kramp.c1@parl.gc.ca - 613-992-5321

Mike Lake - mike.lake.c1@parl.gc.ca - 613-995-8695

Guy Lauzon - guy.lauzon.c1@parl.gc.ca - 613-992-2521

Denis Lebel - denis.lebel.c1@parl.gc.ca - 613-996-6236

Ryan Leef - Ryan.Leef.c1@parl.gc.ca - 613-995-9368

Kellie Leitch - Kellie.Leitch.c1@parl.gc.ca - 613-992-4224

Pierre Lemieux - pierre.lemieux.c1@parl.gc.ca - 613-992-0490

Chungsen Leung - Chungsen.Leung.c1@parl.gc.ca - 613-992-4964

Wladyslaw Lizon - Wladyslaw.Lizon.c1@parl.gc.ca - 613-996-0420

Ben Lobb - ben.lobb.c1@parl.gc.ca - 613-992-8234

Tom Lukiwski - tom.lukiwski.c1@parl.gc.ca - 613-992-4573

Dave MacKenzie - dave.mackenzie.c1@parl.gc.ca - 613-995-4432

Colin Mayes - colin.mayes.c1@parl.gc.ca - 613-995-9095

Phil McColeman - phil.mccoleman.c1@parl.gc.ca - 613-992-3118

Cathy McLeod - cathy.mcleod.c1@parl.gc.ca - 613-995-6931

Costas Menegakis - Costas.Menegakis.c1@parl.gc.ca - 613-992-3802

Ted Menzies - ted.menzies.c1@parl.gc.ca - 613-995-8471

Rob Merrifield - rob.merrifield.c1@parl.gc.ca - 613-992-1653

Larry Miller - larry.miller.c1@parl.gc.ca - 613-996-5191

James Moore - james.moore.c1@parl.gc.ca - 613-992-9650

Rob Moore - rob.moore.c1@parl.gc.ca - 613-996-2332

Rob Nicholson - rob.nicholson.c1@parl.gc.ca - 613-995-1547

Deepak Obhrai - deepak.obhrai.c1@parl.gc.ca - 613-947-4566

Gordon O'Connor - gordon.oconnor.c1@parl.gc.ca - 613-992-1119

Bev Oda - bev.oda.c1@parl.gc.ca - 613-992-2792

Joe Oliver - Joe.Oliver.c1@parl.gc.ca - 613-992-6361

Christian Paradis - christian.paradis.c1@parl.gc.ca - 613-995-1377

LaVar Payne - lavar.payne.c1@parl.gc.ca - 613-992-4516

Peter Penashue - Peter.Penashue.c1@parl.gc.ca - 613-996-4630

Pierre Poilievre - pierre.poilievre.c1@parl.gc.ca - 613-992-2772

Joe Preston - joe.preston.c1@parl.gc.ca - 613-990-7769

Lisa Raitt - lisa.raitt.c1@parl.gc.ca - 613-996-7046

James Rajotte - james.rajotte.c1@parl.gc.ca - 613-992-3594

Brent Rathgeber - brent.rathgeber.c1@parl.gc.ca - 613-996-4722

Scott Reid - scott.reid.c1@parl.gc.ca - 613-947-2277

Michelle Rempel - Michelle.Rempel.c1@parl.gc.ca - 613-992-4275

Blake Richards - blake.richards.c1@parl.gc.ca - 613-996-5152

Lee Richardson - lee.richardson.c1@parl.gc.ca - 613-995-1561

Greg Rickford - greg.rickford.c1@parl.gc.ca - 613-996-1161

Gerry Ritz - gerry.ritz.c1@parl.gc.ca - 613-995-7080

Andrew Saxton - andrew.saxton.c1@parl.gc.ca - 613-995-1225

Gary Schellenberger - gary.schellenberger.c1@parl.gc.ca - 613-992-6124

Kyle Seeback - Kyle.Seeback.c1@parl.gc.ca - 613-995-5381

Gail Shea - gail.shea.c1@parl.gc.ca - 613-992-9223

Bev Shipley - bev.shipley.c1@parl.gc.ca - 613-947-4581

Devinder Shory - devinder.shory.c1@parl.gc.ca - 613-947-4487

Joy Smith - joy.smith.c1@parl.gc.ca - 613-992-7148

Robert Sopuck - robert.sopuck.c1@parl.gc.ca - 613-992-3176

Kevin Sorenson - kevin.sorenson.c1@parl.gc.ca - 613-947-4608

Bruce Stanton - bruce.stanton.c1@parl.gc.ca - 613-992-6582

Brian Storseth - brian.storseth.c1@parl.gc.ca - 613-996-1783

David Sweet - david.sweet.c1@parl.gc.ca - 613-996-4984

David Tilson - david.tilson.c1@parl.gc.ca - 613-995-7813

Lawrence Toet - Lawrence.Toet.c1@parl.gc.ca - 613-995-6339

Vic Toews - vic.toews.c1@parl.gc.ca - 613-992-3128

Brad Trost - brad.trost.c1@parl.gc.ca - 613-992-8052

Bernard Trottier - Bernard.Trottier.c1@parl.gc.ca - 613-995-9364

Susan Truppe - Susan.Truppe.c1@parl.gc.ca - 613-992-0805

Merv Tweed - merv.tweed.c1@parl.gc.ca - 613-995-9372

Tim Uppal - tim.uppal.c1@parl.gc.ca - 613-995-3611

Bernard Valcourt - Bernard.Valcourt.c1@parl.gc.ca - 613-995-0581

Dave Van Kesteren - dave.vankesteren.c1@parl.gc.ca - 613-992-2612

Peter Van Loan - peter.vanloan.c1@parl.gc.ca - 613-996-7752

Maurice Vellacott - maurice.vellacott.c1@parl.gc.ca - 613-992-1899

Mike Wallace - mike.wallace.c1@parl.gc.ca - 613-995-0881

Mark Warawa - mark.warawa.c1@parl.gc.ca - 613-992-1157

Chris Warkentin - chris.warkentin.c1@parl.gc.ca - 613-992-5685

Jeff Watson - jeff.watson.c1@parl.gc.ca - 613-992-1812

John Weston - john.weston.c1@parl.gc.ca - 613-947-4617

Rodney Weston - rodney.weston.c1@parl.gc.ca - 613-947-2700

David Wilks - David.Wilks.c1@parl.gc.ca - 613-995-7246

John Williamson - John.Williamson.c1@parl.gc.ca - 613-995-5550

Alice Wong - alice.wong.c1@parl.gc.ca - 613-995-2021

Stephen Woodworth - stephen.woodworth.c1@parl.gc.ca - 613-995-8913

Terence Young - terence.young.c1@parl.gc.ca - 613-995-4014

Wai Young - Wai.Young.c1@parl.gc.ca - 613-995-7052

Bob Zimmer - Bob.Zimmer.c1@parl.gc.ca - 613-947-4524

Swift, Andrew

From: Turner, Jessica
Sent: Wednesday, February 29, 2012 12:10 PM
To: Swift, Andrew
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; COMDO; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Miller, Kevin; Orton, Karolina; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica
Subject: FYI - Anonymous Video

Categories: ATI PRINT

A new Anonymous video was posted yesterday. It mentions Vic Toews, and Vikileaks. The video description states that a transcript of the video will be up today. We will watch for the transcript and send it to you as soon as it is available.

Anonymous encourages viewers to protest the Provencher Conservative Association that will hold their annual meeting in Steinbach, MB on March 3, with Vic Toews attending. It also mentions the hacking of the Ontario Chiefs of Police website, and does not claim responsibility.

The creators of the video provide a link, and suggests MPs look at the viewer comments from the first video.

The video description also links to a playlist of music, "Operation Vic.Tory/Great White North Soundtrack"

1. 1. kill bill (c-30) - battle without honour or humanity
2.
3. 2. south park - blame canada
4.
5. 3. vic toews' song - richard cheese - me so horny
6.
7. 4. matthew good band - advertising on police cars
8.
9. 5. ana johnson - we are
10.
11. 6. inception - mind heist
12.
13. 7. afi - miseria cantare
14.
15. 8. kill bill - l'arena
16.
17. 9. bjork - army of me - sucker punch version
18.
19. 10. l7 - shit list
20.
21. 11. party ben & the chemical brothers - galvanize the empire
22.
23. 12. la roux - in for the kill - schrillex version
24.

13. forever the sickest kids - men in black

14. weird al - canadian idiot

15. moxy früvous - your new boyfriend's a bit of a right-wing shit

16. the ting tings - stacey meek's song - that's not my name

17. vic backtraced it (and you've been reported to the cyber police!)

18. peaches - i don't give a fuck

19. frou frou - who's getting scared now?

20. disturbed - land of confusion

21. south park - la resistance

22. lo fidelity allstars - battle flag

23. against me - bob rae's song - baby, i'm an anarchist (you're a spineless liberal)

24. dedicated to our anonymous brothers & sisters - crash test dummies - superman's song

25. A. dedicated to the people of canada - nikki yanofsky - i believe in the power of you and i

B. annie villeneuve - j'imagine (french version of i believe in the power of you and i)

26. heather small - what have you done today (to make you feel proud)?

27. south park - o canada

28. orbital - halcyon and on (theme from hackers)

Miller, Kevin

From: Miller, Kevin
Sent: Wednesday, February 29, 2012 3:15 PM
To: Turner, Jessica
Subject: Fw: Cyber Security Keywords

Categories: Green Category

See below. More keywords. :)
Kevin K. Miller
Communications Manager | Gestionnaire de Communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-9218
Fax | Télécopieur : 613-954-6048
Email | Courriel : Kevin.Miller@ps-sp.gc.ca

From: Eke, Darren
Sent: Wednesday, February 29, 2012 03:10 PM
To: Miller, Kevin
Cc: Chomyshyn, Nicholas; Stanfield, Charles
Subject: RE: Cyber Security Keywords

Hi again, Kevin.
We have received a new list of key words from our policy folks; for your consideration, could you please add the following to your list:

Rootkit
Anonymous
Computer worm
Computer compromise
Password compromise
Software vulnerability
Denial of service attack
Distributed denial of service attack
Spear Phishing
Computer network operations
Computer network attack
Computer network defence
Computer network exploitation
Cyber effects
Offensive cyber operations
Defensive cyber operations
Cyber operations

Thanks,
-Darren

From: Eke, Darren
Sent: February 28, 2012 4:30 PM
To: Miller, Kevin
Cc: Chomyshyn, Nicholas; Stanfield, Charles
Subject: Cyber Security Keywords

Hello Kevin,
The list looks great – we would only suggest adding one word, "hameçonnage", to complement "phishing". This change is reflected as a highlighted addition, please note it is not formatted because I'm uncertain of your specific ranking/ordering of keywords.
Thanks,
-Darren

From: Miller, Kevin
Sent: February 15, 2012 1:40 PM
To: Stanfield, Charles
Cc: Eke, Darren; Chomyshyn, Nicholas
Subject: Updates and Revisions - Media Monitoring Keyword Lists

Good afternoon Charles,

The Media Monitoring team is in the process of updating all of our keywords lists. Please find attached the lists of words we currently have related to your files. What we need is for you and your team to review the current lists, and make any additions and/or deletions as necessary. We have provided the documents in Microsoft Word format so that track changes may be enabled.

Once completed please send these lists back to myself and Nick C. via email by **Friday, March 2nd, 2012.**

As always, your cooperation in this matter is greatly appreciated.

Thanks,
Kevin

Kevin K. Miller
Communications Manager | Gestionnaire de Communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-9218
Fax | Télécopieur : 613-954-6048
Email | Courriel : Kevin.Miller@ps-sp.gc.ca

Swift, Andrew

From: COMDO
Sent: Thursday, March 01, 2012 10:41 AM
To: Turner, Jessica; Swift, Andrew
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Miller, Kevin; Orton, Karolina; Patriquin, Kimberly; Therien, Stephane
Subject: RE: Anonymous - New video (March 1, 2012)

Categories: ATI PRINT

Also, the video says they are "on the eve of a new release", thus I assume a new video revealing more information about the Minister will be coming out tomorrow.

- Sean

From: Turner, Jessica
Sent: March 1, 2012 10:33 AM
To: Swift, Andrew
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; COMDO; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Miller, Kevin; Orton, Karolina; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica
Subject: Anonymous - New video (March 1, 2012)

Anonymous posted a new video this morning. They're encouraging Canadians and twitter users to bombard their MPs, Minister Toews, and Prime Minister Harper, re. Bill C-30.

Here is a copy of the description of the video. The poster makes no mention of posting a transcript.

"This is a call to action for all Canadian citizens, Twitter users, concerned bystanders and our Anonymous brothers and sisters around the world.

Vic Toews and the Canadian government want to silence legal online protests using social media through government intimidation, and have demanded the creator of Vikileaks be called before a Parliamentary ethics committee:

http://www.cbc.ca/news/politics/inside-politics-blog/2012/02/vikileaks-watch-...

This has become a true mirror of the greater Wikileaks situation, where the release of information that puts the government or it's officials in a bad light is met with government harassment and intimidation.

This shall not stand.

Email your Vikileaks to AnonymousCanada@hush.com. If you wish to remain anonymous yourself, it's free and easy to make a disposable account there.

Email Vic directly & anonymously from the following link, and demand he cease his attempts to silence the Vikileaks creator & that step down immediately - http://canadaforfreenet.x10.mx/

Or contact him directly:

Vic Toews - vic.toews.c1@parl.gc.ca - (613) 992-3128

List of all Canadian MP Twitter accounts: http://politwitter.ca/page/canadian-politics-twitters/mp/house

Vic Toews: @ToewsVic

Stephen Harper: @PMHarper
Tom Lukiwski: @TomLukiwski (MP who asked we be held in contempt of Parliament)

Read the deleted Vikileaks tweets here: http://twitter.com/AnonsOfCanada

Contact information for every MP who voted yes on Bill C-11, the Canadian version of SOPA, can be found at the following link: http://pastebin.com/JnFj3Lsv

Though it is not widely known, you can call your federal MP at their Ottawa office, toll-free, from anywhere in Canada via the Library of Parliament at 1-866-599-4999.

(We've got a little something for our fellow Anons as well: http://pastebin.com/vNXtwXK0)"

Pages 115 to / à 131

are duplicates of

sont des duplicatas des

pages 133 to / à 149

Champoux, Martin

From: Champoux, Martin
Sent: Thursday, March 01, 2012 2:15 PM
To: COMDO; Miller, Kevin; Chomyshyn, Nicholas
Subject: RE: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous

No that is still the case. I just wanted to make it clear a few people that this document was not being distributed publicly because of the sensitive subject of the content.

-----Original Message-----
From: COMDO
Sent: Thursday, March 01, 2012 1:46 PM
To: Champoux, Martin; Miller, Kevin; Chomyshyn, Nicholas
Subject: RE: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous

I am confused by your "FYI" Martin.

I thought it was our understanding with CCIRC that any cyber advisories, information notes our cyber alerts that aren't posted publicly (but still contain the media relations contact address at the bottom) are to be shared with Darren, Jessie and Charles with a CC to issues management for their awareness.

Is this no longer the case?

- Sean

-----Original Message-----
From: Champoux, Martin
Sent: March 1, 2012 1:34 PM
To: Eke, Darren; Bronson, Jessie; Stanfield, Charles
Cc: Issues / Enjeux; COMDO; Miller, Kevin
Subject: FW: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous

FYI

This is a limited distribution publication intended for small number of CCIRC stakeholders. It is not meant for public distribution.

Martin

-----Original Message-----
From: Issues / Enjeux
Sent: Thursday, March 01, 2012 1:27 PM
To: De Curtis, Laura; McDonald, Jessica; Picard, Josée; Swift, Andrew; Filipps, Lisa; Manning, Kerri; Champoux, Martin; Ferguson, Michelle; Wilson, Barbara; Slack, Jessica

Subject: FW: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous

---

From: COMDO
Sent: Thursday, March 01, 2012 1:26:47 PM (UTC-05:00) Eastern Time (US & Canada)
To: Bronson, Jessie; Stanfield, Charles; Eke, Darren
Cc: Issues / Enjeux
Subject: FYI: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous

(La version française suit)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
INFORMATION NOTE
****

Number: IN12-501
Date: 1 March 2012

****
Overview of the Hacktivist Group "Anonymous"
****

PURPOSE
========

The purpose of this report is to provide an overview of the hacktivist group "Anonymous." It contains information on its organizational structure, tradecraft and targets; the threat to Canadian Critical Infrastructure systems; and recommended mitigation.

ASSESSMENT
==========

EXECUTIVE SUMMARY

Anonymous targets governments, private firms and individuals whose activities or purposes appear to be in conflict with principles espoused by the group. These principles mainly focus on: civil rights (e.g. oppressive regimes); information accessibility (e.g. Internet censorship); and other causes associated with perceived social injustice.

Based on a view of previous targeting by Anonymous, Canadian critical infrastructure systems could be targeted due to government legislative and regulatory initiatives (e.g. the Copyright Modernization Act) and initiatives that may result in activist opposition (e.g. environmental or social issues).

[redacted]

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their agendas. Most notably, "Anonymous" is a term that refers to a group of activist hackers, or hacktivists, that poses a wide range of cyber threats to government and commercial organizations around the world. Anonymous' agenda has included initiating cyber threat activities in protest of perceived government-mandated Internet censorship and in support of worldwide activist movements.

[redacted]

Pages 135 to / à 139

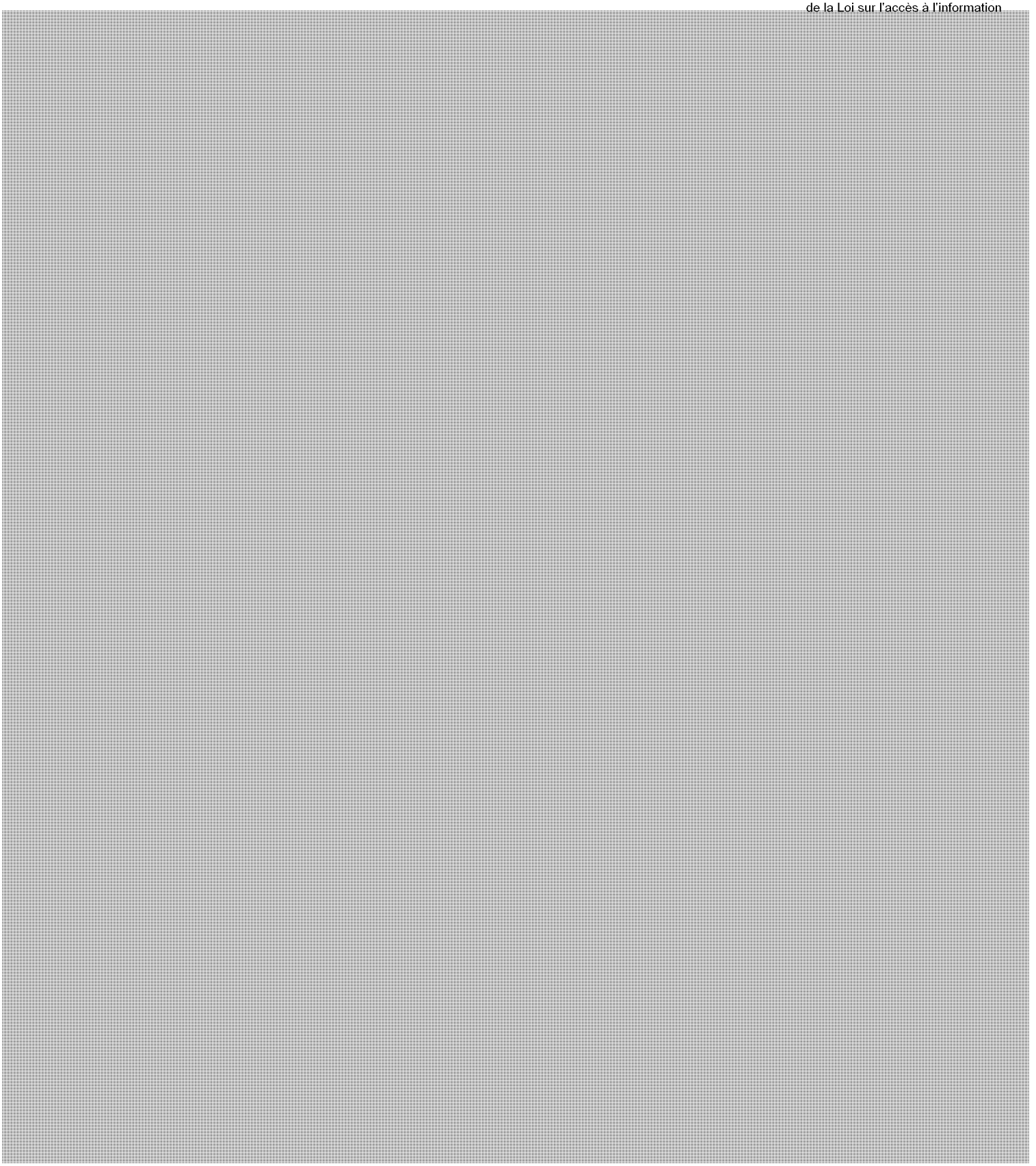
are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information



Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates

in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquires into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

****

SÉCURITÉ PUBLIQUE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

****
NOTE D'INFORMATION
****

Numéro : IN12-501
Date : 1 mars 2012

****
Aperçu du collectif d'hacktivistes Anonymous
****

OBJECTIF
========

Le présent rapport donne un aperçu du groupe d'hacktivistes Anonymous. Il présente des renseignements sur sa structure organisationnelle, ses techniques et ses cibles, sur la menace qu'il pose pour les systèmes d'infrastructures essentielles du Canada et sur les mesures d'atténuation recommandées.

ÉVALUATION
==========

SOMMAIRE

Anonymous cible les gouvernements, les entreprises privées et les particuliers dont les activités ou les buts semblent être en conflit avec les principes énoncés par le groupe. Ces principes sont axés sur les droits civils (p. ex., régimes oppressifs), l'accès à l'information (p. ex., censure sur Internet) et d'autres causes liées aux injustices sociales perçues.

Compte tenu des cibles précédentes d'Anonymous, les systèmes des infrastructures essentielles du Canada pourraient être ciblés en raison des initiatives législatives et réglementaires du gouvernement (p. ex., Loi sur la modernisation du

droit d'auteur) et d'initiatives qui pourraient provoquer une opposition militante (p. ex, enjeux sociaux ou environnementaux).

[redacted]

APERÇU

Les pirates militants poursuivent de plus en plus des activités de menaces cybernétiques pour atteindre leurs objectifs. En particulier, le terme « Anonymous » fait référence à un groupe de pirates militants (hacktivistes) qui font peser un large éventail de cybermenaces sur les gouvernements et les organisations commerciales partout au monde. Le programme d'Anonymous a compris l'utilisation de cybermenaces pour manifester contre la censure gouvernementale perçue sur Internet et appuyer des mouvements militants internationaux.

[redacted]

Pages 143 to / à 148

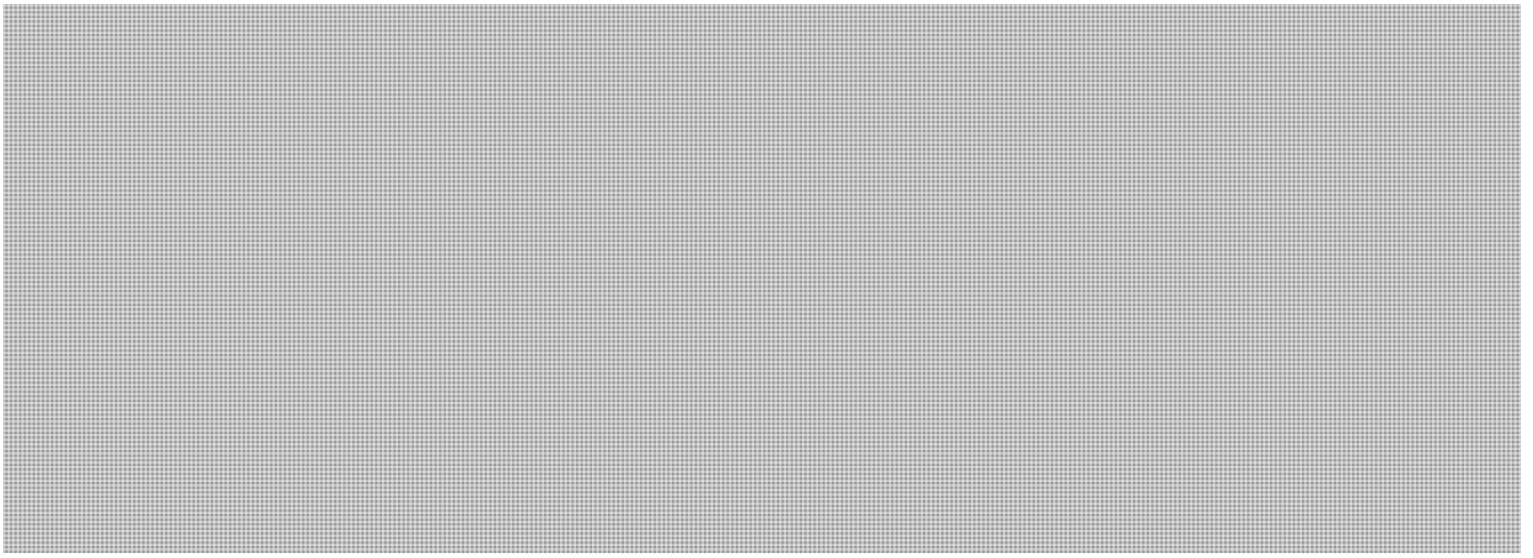
are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information



Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118
Télécopieur : 613-998-9589
Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: s.16(2)(c)

COMDO

From: COMDO
Sent: Saturday, March 03, 2012 5:41 PM
To: Turner, Jessica; Swift, Andrew
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Miller, Kevin; Orton, Karolina; Patriquin, Kimberly; Therien, Stephane
Subject: RE: New Anonymous video

In case it hasn't already been circulated, here is the transcript of the Anonymous video posted yesterday:

1. Nearly all the information discussed beyond this point can be confirmed by news media, governmental and other sources linked from Wikipedia articles. We encourage Canadians not to take our word for it, but to confirm these facts for themselves.
2.
3. Vic Toews held the position of Minister of Justice, which he was appointed to by Stephen Harper, from February 6, 2006 - January 4, 2007.
4.
5. In November 2006, Toews announced that police representatives would be appointed to the provincial judicial advisory committees that review the qualifications of potential judges. This proposal was widely criticized by the Canadian media and by opposition MPs, some of whom argued that Toews' intent was to stack the courts with right-wing judges. In an unprecedented move, Chief Justice Beverley McLachlin and the Canadian Judicial Council issued a statement that Toews's proposal would "compromise the independence of the Advisory Committees", and called for the minister to consult with judicial and legal representatives before making any changes.
6.
7. The Federation of Law Societies of Canada has also criticized Toews's plan, arguing that the government had "politicized" the judicial appointments process. Ontario Chief Justice Roy McMurtry and Attorney General Michael Bryant added their opposition in early 2007, with Bryant arguing that "the forces of legal populism" were threatening to "tear asunder the basic principle of judicial independence". Toews' indicated that he would proceed with his changes despite the opposition, though he was removed from the Justice portfolio before the new system could be implemented. In January 2007, the Conservatives appointed two powerful Ontario police union leaders to an advisory committee.
8.
9. Prime Minister Stephen Harper shuffled his cabinet on January 4, 2007, and appointed Toews as President of the Treasury Board. Some commentators argued that Toews's hardline approach to law-and-order issues was damaging the

Conservative Party's image among centrist voters, and described his replacement Rob Nicholson as presenting a more moderate image.

10.

11. The Cabinet shuffle confused many at the time, especially because despite removing Toews, the Conservative Party went ahead with his controversial plan to appoint high-ranking police officers to the provincial judicial advisory committee. If it was truly Mr. Toews' hardline approach that motivated his removal from the position of Justice Minister, why then push ahead with the very policies that alienated so many in the first places?

12.

13. An article from Xtra.ca, published in August 2008, sheds more light on this confusing series of events and the conclusion people later came to. The article begins:

14.

15. About six months before I spotted Toews at the Winnipeg Fringe Festival, Stephen Harper shuffled him from the high-profile Justice portfolio into the influential but less noticeable job of Treasury Board President.

16.

17. It was Jan 2007, and the move puzzled cabinet-watchers. It was seen as a demotion, even though Conservatives seemed to like Toews as Justice Minister. Apart from some controversial views, he hadn't done anything scandalous – at least not that most people knew about at the time. In light of new revelations about his personal life, though, the move is now seen as Harper's attempt to distance himself from Toews. That's because the Treasury Board President's formerly squeaky-clean image as an upright, Christian family man is now in tatters. His wife of 32 years, and the mother of his adult children has filed for divorce. A few months ago, another woman gave birth to a baby – his.

18.

19. Many people would say that's nobody's business, except for one thing: the way the Conservatives are allegedly trying to deal with the sticky situation of having an adulterer in their ranks.

20.

21. End of article for our purposes.

22.

23. Listen closely, because the following timeline is very important.

24.

25. November 23, 2006 - Justice Minister Vic Toews appoints Catherine Everett to the Family Division of the Court of Queen's Bench of Manitoba.

26.

27. January 4, 2007 - Stephen Harper removes Vic Toews as Justice Minister, confusing many.

28.

29. People will later conclude, based on the birth of Mr. Toews son and his subsequent divorce, that this was the motivation behind his removal, as the

Conservatives didn't want Vic Toews' marital scandal hurting the party's political prospects. However, Vic had not even told his wife he was having an affair yet, and would not do so until January 28, as confirmed in sworn court affidavits.

30.

31. His son would not be born for another 6 or 7 months.

32.

33. His first wife would not file for divorce until more than a year later.

34.

35. These events cannot have been the motivation for Vic Toews' removal from the position of Justice Minister, unless you believe that Mr. Toews told Stephen Harper about his mistress's pregnancy nearly a month before informing his own wife.

36.

37. The other frequently offered explanation for Vic Toews' removal, that his hardline reputation was alienating voters, seems very dubious as the Conservative Party followed through with the very plans that caused so much controversy and earned Vic Toews that reputation in the first place.

38.

39. January 28th, 2007 - Court affidavits from Toews' first wife state, quote, "On January 28th, 2007 Vic informed me that he had been having an affair for the past 3 years and that the woman was pregnant."

40.

41. July, 2007 - Vic Toews' and Stacey Meek's son is born.

42.

43. March 31, 2008 - Vic Toews' first wife files for divorce.

44.

45. So, what then was Stephen Harper's motivation for removing Vic Toews from the position of Justice Minister, a position in which he was generally well-liked by Conservatives?

46.

47. Anonymous has been informed that not only did Vic Toews appoint Catherine Everett to the Court of Queen's Bench while sleeping with her, but that Stephen Harper was discovered this at some point in time during the month or so between Nov. 26, 2006 and January 4, 2007, and quietly removed Vic Toews from the position of Justice Minister in a careful orchestrated balancing act between protecting himself and the party by not having his sitting Justice Minister embroiled in a political and legal scandal were this information to be made public, and continuing to conceal this information in order to protect the Conservative Party's political prospects.

48.

49. If there was any justice in this country, an investigation would be launched into these allegations. However, as our government seems hell-bent on calling those who engage in legal protests using social media before ethics

committees and holding Anonymous in contempt of Parliament instead, this seems unlikely. We will not be holding our breath.

50.

51. Vic Taves has said in regard to Bill C-30, "I will continue to do my duty and carry out my responsibilities in respect of this piece of legislation." Mr. Toews, it is not your duty to pass Bill C-30. Bill C-30 represents the antithesis of your duty, and everything this country stands for. Your duty is to serve the people of Canada, not invade their privacy, violate their civil rights, or treat them like criminals by presuming them guilty before they are proven innocent.

52.

53. Having released this information, Anonymous must now take additional measure to ensure both our anonymity and our security. This means there will likely be no new videos released for a week or more. Some will say that we have fled, or that we've given up the fight. They will be wrong. If it were possible to frighten Anonymous into silence, we would have deleted this account the day it was demanded we be held in contempt of Parliament, and we would never have released this information. They said our first video was rhetoric and nothing more. They said we had nothing to tell before we revealed the identity of Mr. Toews' mistress. Anonymous has kept all it's promises to the Canadian public thus far. Have faith in us.

54.

55. Should we receive more information we feel the Canadian public must be made aware of, or should the Canadian government once again attempt to undermine the civil rights of Canadian citizens, we will re-emerge to meet these challenges to our collective liberty head on. Our allegiance does not, and will never, lie with the government of this country... our allegiance lies with the Canadian people.

56.

57. We are Anonymous.

58.

59. We are Legion.

60.

61. We do not forgive.

62.

63. We do not forget.

64.

65. Expect us, for O Canada, we stand on guard for thee.

From: Turner, Jessica
Sent: March 2, 2012 6:03 AM
To: Swift, Andrew
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; COMDO; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon,

Adam; Miller, Kevin; Orton, Karolina; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica
Subject: New Anonymous video

Posted an hour ago.

Pwn Parliament Friday - Sex, Lies & Judicial Appointments - Part II
http://www.youtube.com/watch?v=rbfsN3ADvlk&context=C355dc3dADOEgsToPDskI8SaGBdL_7eYZRuoNnofAK

Swift, Andrew

From: Turner, Jessica
Sent: Tuesday, March 27, 2012 1:06 PM
To: Swift, Andrew
Cc: Brennan, Nicholas Adam; Chomyshyn, Nicholas; COMDO; Despard, Sean; Ferguson, Michelle; Glazer, David; Lauzon, Adam; Miller, Kevin; Orton, Karolina; Patriquin, Kimberly; Therien, Stephane; Turner, Jessica
Subject: FYI - IP address

Categories: ATI PRINT

Tweet

ExpectUsCanada 1:02pm via web

#Anonymous Brothers And Sisters It Is Time We Show @ToewsVic That We Are Done With His Bullshit Help Us Take Down His Site #IP173.201.216.69

Miller, Kevin

From: Miller, Kevin
Sent: Tuesday, March 27, 2012 1:29 PM
To: Patriquin, Kimberly
Subject: RE: Summary of Cyber Call

Categories: Green Category

Thanks for this. ☺

K

From: Patriquin, Kimberly
Sent: Tuesday, March 27, 2012 1:21 PM
To: Miller, Kevin
Subject: Summary of Cyber Call

Hi Kevin,

Here's what you missed:

1- **OAG Audit**- Last Thursday Andrew H., Stephanie and Amy met with auditors on the Critical Infrastructure and Cyber audit. The auditors are supposed to send a summary of their discussion. It has not yet been received. The audit will include things like the # of website updates, # of tweets, international research which influenced the campaign etc. The auditors have interviewed over 100 ppl for the audit. Expect a lot of media attention especially if the release of the audit coincides with cyber security month.
2- **2012-13 Business Plan**- In drafting mode. Need to rank priorities. Draft due this Friday. Expect cyber to be in the top 2 or 3.
3- **Strategic Plan for Manifest**- Meeting this afternoon
4- **Secondary Analysis by EKOS**- Close to deadline. Waiting to receive draft report from supplier. Don't anticipate much analysis.
5- **FPT**- Cyber policy FPT Meeting to take place on April 3rd. Stephanie would like Comms to present at that meeting. Meeting tomorrow to discuss.
6- **Roundtable**- Martin provided the following update: Robert Dick is "appearing" before a parliamentary committee on April 3rd. The meeting involves a CCIRC technical paper on Anonymous from a couple of weeks ago. Although the paper was internal, somehow the committee obtained a copy and has accused the department of protecting the Minister. Martin will follow up to find out if a binder or speaking notes is being prepared for Robert Dick or if he will simply be a witness.

Let me know if you have any questions!

Kim

Pages 157 to / à 158

are duplicates of

sont des duplicatas des

pages 1226 to / à 1227

Miller, Kevin

From: Miller, Kevin
Sent: Wednesday, March 28, 2012 7:44 PM
To: Champoux, Martin
Subject: Re: Anonymous Transcripts

Categories: Green Category

Sorry Martin, I got called into a meeting end of day and I didn't get a chance to look. I will send a note to Comdo to see if they can find them.

Apologies.
K
Kevin K. Miller
Communications Manager | Gestionnaire de Communications Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-9218 Fax | Télécopieur : 613-954-6048 Email | Courriel : Kevin.Miller@ps-sp.gc.ca

----- Original Message -----
From: Champoux, Martin
Sent: Wednesday, March 28, 2012 07:40 PM
To: Miller, Kevin
Subject: Anonymous Transcripts

Hi Kevin

Did you get a chance to track down those transcripts we discussed this afternoon? A colleague of ours at CSEC was very eager to get his hands on them as soon as possible. Thanks.

Martin

Miller, Kevin

From: Miller, Kevin
Sent: Wednesday, March 28, 2012 7:47 PM
To: Champoux, Martin
Subject: Re: Anonymous Transcripts

Categories: Green Category

Spoke to comdo, you will have them within the hour.

Thanks
K
Kevin K. Miller
Communications Manager | Gestionnaire de Communications Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-9218 Fax | Télécopieur : 613-954-6048 Email | Courriel : Kevin.Miller@ps-sp.gc.ca

----- Original Message -----
From: Champoux, Martin
Sent: Wednesday, March 28, 2012 07:40 PM
To: Miller, Kevin
Subject: Anonymous Transcripts

Hi Kevin

Did you get a chance to track down those transcripts we discussed this afternoon? A colleague of ours at CSEC was very eager to get his hands on them as soon as possible. Thanks.

Martin

Pages 161 to / à 175

are duplicates of

sont des duplicatas des

pages 191 to / à 205

Pages 176 to / à 190

are duplicates of

sont des duplicatas des

pages 191 to / à 205

Champoux, Martin

From: Champoux, Martin
Sent: Wednesday, March 28, 2012 8:16 PM
To: COMDO
Subject: Fw: As Requested - Transcripts for Anonymous Videos

Importance: High

Adam

Can you please send the fourth transcript you referred to in your e-mail to Kevin. Thx

Martin

From: Miller, Kevin
Sent: Wednesday, March 28, 2012 08:07 PM
To: Champoux, Martin
Subject: Fw: As Requested - Transcripts for Anonymous Videos

As requested.

K
Kevin K. Miller
Communications Manager | Gestionnaire de Communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-9218
Fax | Télécopieur : 613-954-6048
Email | Courriel : Kevin.Miller@ps-sp.gc.ca

From: COMDO
Sent: Wednesday, March 28, 2012 08:03 PM
To: Miller, Kevin
Subject: As Requested - Transcripts for Anonymous Videos

Hi Kevin,

Please see below for transcripts of the three Anonymous videos.

I also have the transcript of a fourth video posted by Anonymous handy if you want it.

Let me know if I can be of further assistance,

Adam

Video 3:

1. Hello, Mr. Toews.
2.

3. We are Anonymous.
4.
5. You have now had several days to reflect upon your actions.
6.
7. You have yet to apologize to the Canadian people for referring to them as supporters of pedophilia, or for attempting to infringe on their civil rights. You have stated that you are "open to amendments" on Bill C-30, which has been referred to committee for review.
8.
9. This is not sufficient.
10.
11. It has become very apparent that the purpose of Bill C-30 was never to prevent the distribution of child pornography. This is not merely a matter of opinion. You yourself, Mr. Toews, have submitted a piece to multiple media outlets, stating that Bill C-30 would allow police to crack down on, quote, "identity theft, online organized crime, and many Internet scams and frauds."
12.
13. In only a matter of days, we have gone from preventing child pornography to something as vague as cracking down on, quote "online organized crime". How convenient it is that Bill C-30 has come into prominence at the same time as Bill C-11, an online copyright bill which criminalizes Canadian citizens making personal copies of media they have legally purchased, would block Canadian access to websites deemed to be criminal by the authorities, and would force service providers to terminate service to customers for acts as innocuous as sharing mp3s.
14.
15. Interestingly, it would be possible under Bill C-11 to block Canadian access to YouTube, the site on which this video is hosted, on the basis that it facilitates online piracy.
16.
17. In short, this government's definition of "online organized crime" is so extreme that it includes online activities engaged in by the majority of Canadians.
18.
19. Most telling of all, Bill C-30 was originally named, "An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts". This intentionally vague and confusing title, obviously designed to obscure the bill's true purpose, was later changed to the "Protecting Children From Internet Predators Act", to better sell this massive intrusion of privacy to the Canadian people.
20.
21. Mr. Toews, your pattern of obfuscation and deception has only continued. We are growing impatient.
22.

23. Anonymous has warned you this is only beginning.
24.
25. Over the past several days, we have been inundated with messages exposing all manner of political wrongdoings and personal scandals, some of which extend to the very highest levels of your government.
26.
27. However, there is one incident, Mr. Toews, that the Canadian public would find particularly interesting. It is an act that you concealed so well that it does not appear in the affidavits from your divorce. In fact, we highly suspect neither your first wife, your former mistress, nor your political peers are aware of it. This incident pertains not only to your personal life, but to the direct abuse of your political position. Information about this incident has been submitted to us multiple times, independently, by both named and anonymous sources.
28.
29. Think very hard, Mr. Toews. As we said previously, we have no doubt that there are many skeletons in your closet. However, upon reflection, you should be able to determine which incident on the lengthy list of your illicit activities we are referring to.
30.
31. There is a very real possibility that after the revelation of this incident, Mr. Toews, that public outrage will not be necessary for you to find yourself without a job. It is already widely known that you have engaged in criminal activity to further your political career, as you did in 1999, when you were convicted of violating Manitoba's Election Finances Act during a provincial election.
32.
33. Perhaps you are under the illusion that if you simply allow enough time to pass, the public will lose interest in the controversy over Bill C-30, allowing it to pass unprotested. Perhaps you are under the impression that there is no scandal so great it cannot destroy your reputation and career. Perhaps you are under the impression that we are bluffing.
34.
35. We are not bluffing, Mr. Toews. You have seven days to reflect upon your personal and political crimes. After that, the Canadian people will be made aware of just how disgustingly unscrupulous and corrupt you are.
36.
37. And to the rest of those who support Bill C-30: do not believe for a moment that you are untouchable. Anonymous has received information implicating many of you in both political and personal scandals. This government has already been shaken by Mr. Toews' disgusting remarks and hypocrisy, it's attempts to legalize spying on Canadian citizens, and the revelation that you have used robocalls to intentionally keep voters away from the polls. Directing voters to incorrect or non-existent polling stations is voter suppression, and is illegal under the Canada Elections Act.

38.

39. Let the next seven days serve as a period of reflection for the entire House of Commons. Ask yourselves, how many more scandals can you afford? How many more of your crimes shall be revealed to the Canadian people?

40.

41. A government that allows it's citizens no secrets will not be allowed any secrets of it's own. Anonymous calls upon everyone and anyone who does not support governmental spying on Canadian citizens to submit information on any personal scandal, crime, or abuse of power committed by any politician who supports Bill C-30. An email address for this purpose can be found in the description below this video. Anonymous will never name or reveal it's sources.

42.

43. The Canadian people have spoken. They do not support Bill C-30. You ignore their outcry at the peril of your own careers. The True North is strong and free, and we will never surrender our freedom, least of all to fear-mongering hypocrites who attempt to wrench it from us through subterfuge and deception.

44.

45. Anonymous demands the immediate resignation of Vic Toews, the scrapping of Bills C-30 and C-11 in their entirety, and a formal apology to the people of Canada for referring to them as supporters of pedophilia, and more importantly, for attempting to infringe on their most basic civil rights.

46.

47. We are Anonymous.

48.

49. We are Legion.

50.

51. We do not forgive.

52.

53. We do not forget.

54.

55. Expect us.

Video 2:

1. Anonymous - Operation Great White North / Operation Vic.Tory

2.

3. Send your Vikileaks to AnonymousCanada@hush.com

4.

5. *** Transcript***

6.

7. Hello Mr. Toews. We are Anonymous. Over the past several days, we have been watching you.

8.

9. You have continued to deceive the Canadian people by claiming that the information made accessible to police by Bill c-30 is no greater than that which can be found in a phonebook. Tell us Mr. Toews, in what phonebook can you find an individual's internet browsing history? Their private emails? Their financial information? Their credit card number? And all their personal contacts?

10.

11. How convenient it is that you fail to mention Bill C-30 would not only allow police access to this information without a warrant, but would make it illegal for internet service providers to inform their customers that their information has been accessed by the RCMP or CSIS.

12.

13. You have continued to waste the Canadian public's time and money by demanding a parliamentary investigation into the legal release of public records. We are not shocked in the slightest, as this is consistent with your pattern of ignoring true wrongdoings in favour of feigning moral outrage.

14.

15. What is shocking-- not to mention extremely disturbing-- is that you have claimed you are surprised by the contents of Bill C-30, a bill that you yourself tabled. This is a pathetically transparent attempt to feign ignorance in the face of a massive public backlash. However, let us imagine for a moment that you are telling the truth. Let us imagine that you, an elected official in the House of Commons, either did not take the time or are simply too dimwitted to understand a piece of legislation that you yourself championed. A piece of legislation that legalizes governmental spying on Canadian citizens, and effectively ends the right to privacy in this country.

16.

17. This alone is grounds for you to tender your immediate resignation. The fact that you spun this catastrophic failure to perform your duties as an argument in your own defense would be laughable were the consequences not so dire.

18.

19. Of course, we all know this is simply another addition to your ever-growing web of lies. And this isn't the first time you have found yourself tangled up in your own web of deceit, is it, Mr. Toews?

20.

21. The Canadian public is now well aware that you carried on multiple affairs during your 30-year marriage to your first wife, all the while selling

yourself as a devout Christian who championed so-called traditional family values.

22.

23. Quote: "Marriage is a uniquely heterosexual institution, that indeed is a sacrament. Marriage is one of the cornerstones upon which our society has been built."

24.

25. And yet, even after demonstrating you do not believe a single word of that statement, you continue to imply that your dedication to your personal family relationships makes you a suitable candidate for political office.

26.

27. Anonymous has gained access to a letter you recently sent to your constituents. In it, you quote Yeats:

28.

29. "All this life can give us is a child's laughter; a woman's kiss."

30.

31. Do you think the Canadian people are stupid, Mr. Toews? Do you honestly think that quoting saccharine poetry to us is going to convince us you are a God-fearing family man? Especially now that you are living in a common-law relationship with your former mistress, the very sort of relationship you turned your nose up at when it suited your political interests.

32.

33. Mr. Toews, you have used the illusion of a traditional family life, faith, and moral values as tools in your desperate bid for power, all the while trampling on the rights of others. You have used your own family as pawns in the creation of this illusion. Once again, you have inserted your spouse and children into this debate as rhetorical devices.

34.

35. We warned you that you would not be allowed any secrets if you did not allow the Canadian public any secrets of their own.

36.

37. Therefore, we are naming the woman you referenced in this letter to your constituents.

38.

39. The woman Vic Toews is cohabitating with, whom he impregnated in an affair that took place during his first marriage, is Stacey Meek. She is employed in an administrative capacity by Senator Terry Stratton. She runs a public relations firm based in Toronto. She previously worked for Conservative MP Joy Smith, and is currently listed as a constituency assistant for Conservative MP Joyce Bateman. In the past, she was employed by Issues Ink, a consulting and publishing company based in Winnipeg.

40.

41. Of course, we're sure you had absolutely nothing to do with Stacey Meek being hired by Senator Stratton, Mr. Toews. Surely a man like yourself with such solid moral convictions would never engage in that kind of nepotism!

42.

43. She has a father, Joe, who is a doctor of veterinary medicine; a brother, Jeff; a sister-in law, Rhea; and two nieces who we shall not name, all of whom reside in Winnipeg. Her mother is deceased and passed away due to cancer in in 2002.

44.

45. We also have information about your youngest son, who was the product of your affair with Ms. Meek. However, as he is only 4 years-old and entirely innocent in this matter, we will not release this information. Anonymous does not hold the son responsible for the crimes of the father.

46.

47. However, the woman you are cohabitating with is politically active, a government employee, and in particular is a constituency assistant to MP Joyce Bateman, who voted Yes on Bill C-30. As such, we have no qualms about releasing information about her to the Canadian public.

48.

49. We have also decided not to release your personal contact information, such as your phone number and address, at this time, as we understand you have received credible violent threats from members of the public.

50.

51. Shall we continue, Mr. Toews? Do we have your attention? How does it feel to have personal information about your family in the hands of people you know nothing about, with no control over who disseminates it or how it will be used?

52.

53. Let it be known this is only a taste of the information we have access to. And this is only the beginning.

54.

55. And yet, it is nothing compared to the personal information of millions of Canadians that will be collected, stored, and scrutinized by the authorities if Mr. Toews and this corrupt government are allowed to pass Bill C-30. If this outrageous piece of legislation is allowed to pass, the government will have access to massive legally-required databases filled with information on your spouses, your children, your parents, your brothers, your sisters, your friends and your neighbours.

56.

57. Let it be known, Mr. Toews, that Anonymous will do to corrupt politicians exactly what you are attempting to do to the Canadian public. There will be no two-tier system of privacy for the government and the people of this country. You, and any public official who spies or support spying on Canadian citizens, will reap exactly what you have sewn.

58.

59. It would appear you have made many political enemies, Mr. Toews. Since Anonymous made an email address available through which the public can submit more Vikileaks, we have received no less than a dozen emails from

your peers in Ottawa, several of whom have offered information or have made offers to provide us with information. And that does not include the messages from members of the public who know you in a personal capacity.

60.

61. And to the rest of the Parliament of Canada: you would do well to mind your words about Anonymous. Any attempt to score political points by claiming we are associated with a particular political party will not be met kindly. Your party affiliations are utterly irrelevant to us. Our only interest in this matter is protecting the freedom of information, and protecting the privacy of Canadians from the tyranny of our own government.

62.

63. Anonymous demands the immediate resignation of Vic Toews, the scrapping of Bills C-30 and C-11 in their entirety, and a formal apology to the people of Canada for referring to them as supporters of pedophiles, and importantly, for attempting to undermine their most basic civil rights.

64.

65. We are Anonymous.

66.

67. We are Legion.

68.

69. We do not forgive.

70.

71. We do not forget.

72.

73. Expect us.

Video 1:

1. Welcome to Operation Vic.Tory / Operation Great White North.

2.

3. Below is the contact information of every MP who voted yes on Bill C-11, the Canadian version of SOPA. It was tabled by the dishonorable Christian Paradis. There have been no votes on Bill C-30 as of yet. Let this serve as an example so it remains that way, indefinitely.

4.

5. The ".c1" after the name of each MP allows you to email them personally. Removing it will also allow you contact them, but it will be directed to their Ottawa offices and processed by their staff.

6.

7. Though it is not widely known, you can call your federal MP at their Ottawa office, toll-free, from anywhere in Canada via the Library of Parliament at 1-866-599-4999.

8.

9. Demand that Vic Toews step down, and that the intrusive, exploitative Bills C-30 & C-11 be scrapped in their entirety.

We will do our duty; it is time for Canada to do hers.

Voted Yes on Bill C-11:

NOTE - The ".c1" after the name of each MP allows you to email them personally. Removing it will also allow you contact them, but it will be directed to their Ottawa offices and processed by their staff.

Vic Toews - vic.toews@parl.gc.ca - 613-992-3128

Christian Paradis - christian.paradis@parl.gc.ca - 613-995-1377

Diane Ablonczy - diane.ablonczy.c1@parl.gc.ca - 613-996-2756

Eve Adams - eve.adams.c1@parl.gc.ca - 613-995-7784

Mark Adler - mark.adler.c1@parl.gc.ca - 613-941-6339

Leona Aglukkaq - leona.aglukkaq.c1@parl.gc.ca - 613-992-2848

Dan Albas - Dan.Albas.c1@parl.gc.ca - 613-995-1702

Harold Albrecht - harold.albrecht.c1@parl.gc.ca - 613-992-4633

Mike Allen - mike.allen.c1@parl.gc.ca - 613-947-4431

Dean Allison - dean.allison.c1@parl.gc.ca - 613-995-2772

Stella Ambler - Stella.Ambler.c1@parl.gc.ca - 613-992-4848

Rona Ambrose - rona.ambrose.c1@parl.gc.ca - 613-996-9778

Rob Anders - rob.anders.c1@parl.gc.ca - 613-992-3066

David Anderson - david.anderson.c1@parl.gc.ca - 613-995-8042

Scott Armstrong - scott.armstrong.c1@parl.gc.ca - 613-992-3366

Jay Aspin - Jay.Aspin.c1@parl.gc.ca - 613-995-6255

53. John Baird - john.baird.c1@parl.gc.ca - 613-996-0984
54.
55. Joyce Bateman - Joyce.Bateman.c1@parl.gc.ca - 613-992-9475
56.
57. Leon Benoit - leon.benoit.c1@parl.gc.ca - 613-992-4171
58.
59. Maxime Bernier - maxime.bernier.c1@parl.gc.ca - 613-992-8053
60.
61. Steven Blaney - steven.blaney.c1@parl.gc.ca - 613-992-7434
62.
63. Kelly Block - kelly.block.c1@parl.gc.ca - 613-995-1551
64.
65. Ray Boughen - ray.boughen.c1@parl.gc.ca - 613-992-9115
66.
67. Peter Braid - peter.braid.c1@parl.gc.ca - 613-996-5928
68.
69. Garry Breitkreuz - garry.breitkreuz.c1@parl.gc.ca - 613-992-4394
70.
71. Gord Brown - gord.brown.c1@parl.gc.ca - 613-992-8756
72.
73. Lois Brown - lois.brown.c1@parl.gc.ca - 613-992-9310
74.
75. Patrick Brown - patrick.brown.c1@parl.gc.ca - 613-992-3394
76.
77. Rod Bruinooge - rod.bruinooge.c1@parl.gc.ca - 613-995-7517
78.
79. Brad Butt - Brad.Butt.c1@parl.gc.ca - 613-943-1762
80.
81. Paul Calandra - paul.calandra.c1@parl.gc.ca - 613-992-3640
82.
83. Blaine Calkins - blaine.calkins.c1@parl.gc.ca - 613-995-8886
84.
85. Ron Cannan - ron.cannan.c1@parl.gc.ca - 613-992-7006
86.
87. John Carmichael - John.Carmichael.c1@parl.gc.ca - 613-992-2855
88.
89. Colin Carrie - colin.carrie.c1@parl.gc.ca - 613-992-3640 - 613-996-4756
90.
91. Michael Chong - michael.chong.c1@parl.gc.ca - 613-992-4179
92.
93. Rob Clarke - rob.clarke.c1@parl.gc.ca - 613-995 - 8321
94.
95. Tony Clement - tony.clement.c1@parl.gc.ca - 613-944-7740
96.
97. Joe Daniel - Joe.Daniel.c1@parl.gc.ca - 613-995-4988

98.

99. Patricia Davidson - pat.davidson.c1@parl.gc.ca - 613-957-2649

100.

101. Bob Dechert - bob.dechert.c1@parl.gc.ca - 613-995-7321

102.

103. Dean Del Mastro - dean.delmastro.c1@parl.gc.ca - 613-995-6411

104.

105. Barry Devolin - barry.devolin.c1@parl.gc.ca - 613-992-2474

106.

107. Earl Dreeshen - earl.dreeshen.c1@parl.gc.ca - 613-995-0590

108.

109. John Duncan - john.duncan.c1@parl.gc.ca - 613-992-2503

110.

111. Rick Dykstra - rick.dykstra.c1@parl.gc.ca - 613-992-3352

112.

113. Julian Fantino - julian.fantino.c1@parl.gc.ca - 613-996-4971

114.

115. Kerry-Lynne Findlay - Kerry-Lynne.Findlay.c1@parl.gc.ca - 613-992-2957

116.

117. Diane Finley - diane.finley.c1@parl.gc.ca - 613-996-4974

118.

119. Jim Flaherty - jim.flaherty.c1@parl.gc.ca - 613-992-6344

120.

121. Parm Gill - Parm.Gill.c1@parl.gc.ca - 613-995-4843

122.

123. Shelly Glover - shelly.glover.c1@parl.gc.ca - 613-995-0579

124.

125. Robert Goguen - Robert.Goguen.c1@parl.gc.ca - 613-992-8072

126.

127. Peter Goldring - peter.goldring.c1@parl.gc.ca - 613-992-3821

128.

129. Gary Goodyear - gary.goodyear.c1@parl.gc.ca - 613-992-3821

130.

131. Bal Gosal - Bal.Gosal.c1@parl.gc.ca - 613-992-9105

132.

133. Jacques Gourde - jacques.gourde.c1@parl.gc.ca - 613-992-2639

134.

135. Nina Grewal - nina.grewal.c1@parl.gc.ca - 613-996-2205

136.

137. Richard Harris - richard.harris.c1@parl.gc.ca - 613-995-6704

138.

139. Laurie Hawn - laurie.hawn.c1@parl.gc.ca - 613-992-4524

140.

141. Bryan Hayes - Bryan.Hayes.c1@parl.gc.ca - 613-992-9723

142.

Russ Hiebert - russ.hiebert.c1@parl.gc.ca - 613-947-4497

Jim Hillyer - Jim.Hillyer.c1@parl.gc.ca - 613-996-0633

Randy Hoback - randy.hoback.c1@parl.gc.ca - 613-995-3295

Candice Hoeppner - candice.hoeppner.c1@parl.gc.ca - 613-995-9511

Ed Holder - ed.holder.c1@parl.gc.ca - 613-996-6674

Roxanne James - Roxanne.James.c1@parl.gc.ca - 613-992-6823

Brian Jean - brian.jean.c1@parl.gc.ca - 613-992-1154

Randy Kamp - randy.kamp.c1@parl.gc.ca - 613-947-4613

Gerald Keddy - gerald.keddy.c1@parl.gc.ca - 613-996-0877

Jason Kenney - jason.kenney.c1@parl.gc.ca - 613-992-2235

Peter Kent - peter.kent.c1@parl.gc.ca - 613-992-0253

Ed Komarnicki - ed.komarnicki.c1@parl.gc.ca - 613-992-7685

Daryl Kramp - daryl.kramp.c1@parl.gc.ca - 613-992-5321

Mike Lake - mike.lake.c1@parl.gc.ca - 613-995-8695

Guy Lauzon - guy.lauzon.c1@parl.gc.ca - 613-992-2521

Denis Lebel - denis.lebel.c1@parl.gc.ca - 613-996-6236

Ryan Leef - Ryan.Leef.c1@parl.gc.ca - 613-995-9368

Kellie Leitch - Kellie.Leitch.c1@parl.gc.ca - 613-992-4224

Pierre Lemieux - pierre.lemieux.c1@parl.gc.ca - 613-992-0490

Chungsen Leung - Chungsen.Leung.c1@parl.gc.ca - 613-992-4964

Wladyslaw Lizon - Wladyslaw.Lizon.c1@parl.gc.ca - 613-996-0420

Ben Lobb - ben.lobb.c1@parl.gc.ca - 613-992-8234

Tom Lukiwski - tom.lukiwski.c1@parl.gc.ca - 613-992-4573

Dave MacKenzie - dave.mackenzie.c1@parl.gc.ca - 613-995-4432

Colin Mayes - colin.mayes.c1@parl.gc.ca - 613-995-9095

Phil McColeman - phil.mccoleman.c1@parl.gc.ca - 613-992-3118

Cathy McLeod - cathy.mcleod.c1@parl.gc.ca - 613-995-6931

Costas Menegakis - Costas.Menegakis.c1@parl.gc.ca - 613-992-3802

Ted Menzies - ted.menzies.c1@parl.gc.ca - 613-995-8471

Rob Merrifield - rob.merrifield.c1@parl.gc.ca - 613-992-1653

Larry Miller - larry.miller.c1@parl.gc.ca - 613-996-5191

James Moore - james.moore.c1@parl.gc.ca - 613-992-9650

Rob Moore - rob.moore.c1@parl.gc.ca - 613-996-2332

Rob Nicholson - rob.nicholson.c1@parl.gc.ca - 613-995-1547

Deepak Obhrai - deepak.obhrai.c1@parl.gc.ca - 613-947-4566

Gordon O'Connor - gordon.oconnor.c1@parl.gc.ca - 613-992-1119

Bev Oda - bev.oda.c1@parl.gc.ca - 613-992-2792

Joe Oliver - Joe.Oliver.c1@parl.gc.ca - 613-992-6361

Christian Paradis - christian.paradis.c1@parl.gc.ca - 613-995-1377

LaVar Payne - lavar.payne.c1@parl.gc.ca - 613-992-4516

Peter Penashue - Peter.Penashue.c1@parl.gc.ca - 613-996-4630

Pierre Poilievre - pierre.poilievre.c1@parl.gc.ca - 613-992-2772

Joe Preston - joe.preston.c1@parl.gc.ca - 613-990-7769

Lisa Raitt - lisa.raitt.c1@parl.gc.ca - 613-996-7046

James Rajotte - james.rajotte.c1@parl.gc.ca - 613-992-3594

Brent Rathgeber - brent.rathgeber.c1@parl.gc.ca - 613-996-4722

Scott Reid - scott.reid.c1@parl.gc.ca - 613-947-2277

Michelle Rempel - Michelle.Rempel.c1@parl.gc.ca - 613-992-4275

Blake Richards - blake.richards.c1@parl.gc.ca - 613-996-5152

Lee Richardson - lee.richardson.c1@parl.gc.ca - 613-995-1561

Greg Rickford - greg.rickford.c1@parl.gc.ca - 613-996-1161

Gerry Ritz - gerry.ritz.c1@parl.gc.ca - 613-995-7080

Andrew Saxton - andrew.saxton.c1@parl.gc.ca - 613-995-1225

Gary Schellenberger - gary.schellenberger.c1@parl.gc.ca - 613-992-6124

Kyle Seeback - Kyle.Seeback.c1@parl.gc.ca - 613-995-5381

Gail Shea - gail.shea.c1@parl.gc.ca - 613-992-9223

Bev Shipley - bev.shipley.c1@parl.gc.ca - 613-947-4581

Devinder Shory - devinder.shory.c1@parl.gc.ca - 613-947-4487

Joy Smith - joy.smith.c1@parl.gc.ca - 613-992-7148

Robert Sopuck - robert.sopuck.c1@parl.gc.ca - 613-992-3176

Kevin Sorenson - kevin.sorenson.c1@parl.gc.ca - 613-947-4608

Bruce Stanton - bruce.stanton.c1@parl.gc.ca - 613-992-6582

Brian Storseth - brian.storseth.c1@parl.gc.ca - 613-996-1783

David Sweet - david.sweet.c1@parl.gc.ca - 613-996-4984

David Tilson - david.tilson.c1@parl.gc.ca - 613-995-7813

Lawrence Toet - Lawrence.Toet.c1@parl.gc.ca - 613-995-6339

Vic Toews - vic.toews.c1@parl.gc.ca - 613-992-3128

Brad Trost - brad.trost.c1@parl.gc.ca - 613-992-8052

Bernard Trottier - Bernard.Trottier.c1@parl.gc.ca - 613-995-9364

Susan Truppe - Susan.Truppe.c1@parl.gc.ca - 613-992-0805

Merv Tweed - merv.tweed.c1@parl.gc.ca - 613-995-9372

Tim Uppal - tim.uppal.c1@parl.gc.ca - 613-995-3611

Bernard Valcourt - Bernard.Valcourt.c1@parl.gc.ca - 613-995-0581

Dave Van Kesteren - dave.vankesteren.c1@parl.gc.ca - 613-992-2612

Peter Van Loan - peter.vanloan.c1@parl.gc.ca - 613-996-7752

Maurice Vellacott - maurice.vellacott.c1@parl.gc.ca - 613-992-1899

Mike Wallace - mike.wallace.c1@parl.gc.ca - 613-995-0881

Mark Warawa - mark.warawa.c1@parl.gc.ca - 613-992-1157

Chris Warkentin - chris.warkentin.c1@parl.gc.ca - 613-992-5685

Jeff Watson - jeff.watson.c1@parl.gc.ca - 613-992-1812

John Weston - john.weston.c1@parl.gc.ca - 613-947-4617

Rodney Weston - rodney.weston.c1@parl.gc.ca - 613-947-2700

David Wilks - David.Wilks.c1@parl.gc.ca - 613-995-7246

John Williamson - John.Williamson.c1@parl.gc.ca - 613-995-5550

Alice Wong - alice.wong.c1@parl.gc.ca - 613-995-2021

Stephen Woodworth - stephen.woodworth.c1@parl.gc.ca - 613-995-8913

Terence Young - terence.young.c1@parl.gc.ca - 613-995-4014

Wai Young - Wai.Young.c1@parl.gc.ca - 613-995-7052

Bob Zimmer - Bob.Zimmer.c1@parl.gc.ca - 613-947-4524

Pages 206 to / à 207

are duplicates of

sont des duplicatas des

pages 208 to / à 209

Champoux, Martin

From: Champoux, Martin
Sent: Wednesday, March 28, 2012 8:23 PM
To: COMDO
Subject: Re: As Requested - Fourth Anonymous Video

Thx. Have a good night.

From: COMDO
Sent: Wednesday, March 28, 2012 08:18 PM
To: Champoux, Martin
Cc: Miller, Kevin
Subject: As Requested - Fourth Anonymous Video

Hi Martin,

Here's the fourth video I referred to in my email to Kevin.

- Adam

A new Anonymous video was posted yesterday. It mentions Vic Toews, and Vikileaks. The video description states that a transcript of the video will be up today. We will watch for the transcript and send it to you as soon as it is available.

Anonymous encourages viewers to protest the Provencher Conservative Association that will hold their annual meeting in Steinbach, MB on March 3, with Vic Toews attending. It also mentions the hacking of the Ontario Chiefs of Police website, and does not claim responsibility.

The creators of the video provide a link, and suggests MPs look at the viewer comments from the first video.

The video description also links to a playlist of music, "Operation Vic.Tory/Great White North Soundtrack"

1. 1. kill bill (c-30) - battle without honour or humanity
2.
3. 2. south park - blame canada
4.
5. 3. vic toews' song - richard cheese - me so horny
6.
7. 4. matthew good band - advertising on police cars
8.
9. 5. ana johnson - we are
10.
11. 6. inception - mind heist
12.
13. 7. afi - miseria cantare
14.
15. 8. kill bill - l'arena
16.

9. bjork - army of me - sucker punch version

10. 17 - shit list

11. party ben & the chemical brothers - galvanize the empire

12. la roux - in for the kill - schrillex version

13. forever the sickest kids - men in black

14. weird al - canadian idiot

15. moxy früvous - your new boyfriend's a bit of a right-wing shit

16. the ting tings - stacey meek's song - that's not my name

17. vic backtraced it (and you've been reported to the cyber police!)

18. peaches - i don't give a fuck

19. frou frou - who's getting scared now?

20. disturbed - land of confusion

21. south park - la resistance

22. lo fidelity allstars - battle flag

23. against me - bob rae's song - baby, i'm an anarchist (you're a spineless liberal)

24. dedicated to our anonymous brothers & sisters - crash test dummies - superman's song

25. A. dedicated to the people of canada - nikki yanofsky - i believe in the power of you and i

B. annie villeneuve - j'imagine (french version of i believe in the power of you and i)

26. heather small - what have you done today (to make you feel proud)?

27. south park - o canada

28. orbital - halcyon and on (theme from hackers)

Champoux, Martin

From: Champoux, Martin
Sent: Thursday, March 29, 2012 3:42 PM
To: [redacted]
Subject: RE: Media Analysis: Vikileaks and Vikileaks/Anonymous

Hi [redacted]

We did not do a formal media analysis piece on these issues.

Martin

From: [redacted] [mailto: [redacted] @CSE-CST.GC.CA]
Sent: Thursday, March 29, 2012 2:52 PM
To: Swift, Andrew; Champoux, Martin
Subject: Media Analysis: Vikileaks and Vikileaks/Anonymous
Importance: High

Classification: UNCLASSIFIED

s.19(1)

Hi Andrew and Martin,

You may or may not know that I am here at CSEC [redacted] I am filling in until we find a replacement (so you may be hearing from me for a while...)

We are doing some work around the PROC proceedings and in fact CSEC will be appearing before the committee on April 3rd, which brings me to my request:

Have you done any media analysis around the Vikileaks and Anonymous/Vikileaks issue? If so, would you be able to share your products? If you can, we'd be most grateful for something by end of day today, or tomorrow morning.

Thanks very much,

[redacted]
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada
Ottawa, Canada K1G 3Z4
[redacted]@cse-cst.gc.ca
Telephone | Téléphone [redacted]
Fax | Télécopieur 613-991-7691
Government of Canada | Gouvernement du Canada

s.19(1)

Miller, Kevin

From: Miller, Kevin
Sent: Friday, March 30, 2012 10:39 AM
To: [redacted] Swift, Andrew; Chomyshyn, Nicholas; COMDO; Glazer, David; Tomlinson, Jamie; Lauzon, Adam; Therien, Stephane; Despard, Sean; Orton, Karolina; Turner, Jessica; Patriquin, Kimberly
Subject: Re: This is scheduled to be on tonight

Categories: Green Category

Can we order this pls. Thanks.

K
Kevin K. Miller
Communications Manager | Gestionnaire de Communications Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-9218 Fax | Télécopieur : 613-954-6048 Email | Courriel : Kevin.Miller@ps-sp.gc.ca

----- Original Message -----
From: [redacted]
Sent: Friday, March 30, 2012 09:28 AM
To: Swift, Andrew; Chomyshyn, Nicholas; COMDO; Glazer, David; Tomlinson, Jamie; Lauzon, Adam; Therien, Stephane; Despard, Sean; Orton, Karolina; Turner, Jessica; Miller, Kevin; Patriquin, Kimberly; [redacted]
Subject: This is scheduled to be on tonight

Apparently CHQR The Rob Breakenridge show tonight will have:

What is Anonymous - and why Vic Toews shouldn't take them on

Champoux, Martin

From: Champoux, Martin
Sent: Tuesday, April 03, 2012 3:16 PM
To: Gordon, Robert; Dick, Robert; Hatfield, Adam
Subject: G&M: RCMP, spy agency shed no light on Anonymous threats against Toews

No mention of PS testimony

RCMP, spy agency shed no light on Anonymous threats against Toews
Latest testimony bolsters notion that parliamentary probe of online hacker group is ultimately futile
By Gloria Galloway, Globe and Mail, April 3, 2012

Representatives of Canada's electronic surveillance agency and national police force were called before a Commons committee Tuesday to tell politicians all they know about threats posted by online hacker group Anonymous against Public Safety minister Vic Toews.

And the answer is: Not much.

Toni Moffa, the assistant deputy minister who is responsible for technical security at the Communications Security Establishment, seemed genuinely confused by the questions being put to her and had to repeatedly explain that threats posted to public Internet sites are outside the jurisdiction of her organization.

And, while Chief Superintendant James Malizia of the RCMP agreed his organization was looking into the activities of Anonymous as they relate to Mr. Toews, he made it clear he could not discuss the details of the investigation.

The matter was referred to the House affairs committee by Speaker Andrew Scheer, who ruled that Mr. Toews's privileges as a parliamentarian may have been breached by Anonymous - a loose network of international protesters who, in this case, objected to controversial online-surveillance legislation introduced by the minister.

Some of the opposition MPs on the committee have previously expressed concern their inquiry is hampered by the fact Anonymous is anonymous. When they asked how they should get around that problem, Mr. Toews - who testified last week - suggested that they should call in the experts.

But the testimony of those experts Tuesday merely bolstered the notion that the committee's efforts are, in many ways, futile.

As Ms. Moffa told the committee, CSE collects foreign intelligence signals and provides assurances to the government that federal computer systems are secure. But when asked by Conservative MP Harold Albrecht to explain what she knows about Anonymous, how it operates and what threats the group may pose, Ms. Moffa was at a loss.

Anything CSE knows about Anonymous comes from "open sources," she said. And "from our perspective, it's not an [information technology] security breach and it would be best dealt with by an investigative body or agency that would do that type of investigation."

But the investigators were not much more informative.

Supt. Malizia confirmed it is public knowledge that there is an ongoing investigation. But, in response to any question about the case of Anonymous and Mr. Toews, he said: "I am not in a position to discuss any details or specifics with respect to any ongoing investigation."

The most important information provided to MPs on the committee by CSE and the RCMP was that they should follow good Internet security protocols and, if they are ever threatened, they should inform the authorities - none of which will get them very far in their current inquiry.

Toward the end of the committee meeting, which finished early because the MPs had nothing more to ask their witnesses and their witnesses had nothing more to tell them, Conservative MP Laurie Hawn conceded it is unlikely that the identities of the people behind the Anonymous threats will ever be revealed.

Searching for ways to make the committee's inquiry relevant, Mr. Hawn asked Supt. Malizia if he thought the process was worthwhile in reminding Internet users that posting threats against parliamentarians is a crime. "Has this process been useful at least in that respect?" he asked the police officer.

"Well, I am not in a position to comment on the committee's work and the process," Supt. Malizia replied, "but I can say is that advances in technology have created an environment where individuals achieve anonymity."

Pages 214 to / à 215

are duplicates of

sont des duplicatas des

pages 1273 to / à 1274

Swift, Andrew

From: Champoux, Martin
Sent: Monday, May 21, 2012 9:52 PM
To: Swift, Andrew; Filipps, Lisa
Subject: Fw: CE12-002994 DDOS attack on [redacted]

Categories: ATI PRINT

Fyi

From: Beaudoin, Luc
Sent: Monday, May 21, 2012 11:05 AM
To: Anderson, Windy
Cc: Champoux, Martin; Clow, Patrick; Bendelier, Kenneth; CYBERDO
Subject: CE12-002994 DDOS attack on [redacted]

Reference :

- CE12-002994
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

Taking the site off-line is likely the cause of the exaggerated impact of the Anonymous attack in the media.

The [redacted] site is another story. They are not part of our CI client community. CCIRC sent a courtesy note to the [redacted] site administrator to inform them of open source media reports and the publicly available DDOS mitigation guide we have on our site.

Luc

Pages 217 to / à 220
are duplicates of
sont des duplicatas des
pages 221 to / à 224

Slack, Jessica

From: Swift, Andrew
Sent: May-24-12 1:52 PM
To: Slack, Jessica
Cc: Champoux, Martin; Filipps, Lisa
Subject: RE: FW: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Thx. Will keep all posted on what I hear back from PCO.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica
Sent: Thursday, May 24, 2012 1:50 PM
To: Swift, Andrew
Cc: Champoux, Martin; Filipps, Lisa
Subject: FW: FW: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

These lines should work...

- We do not comment on security threats. That said, our government takes threats seriously and has measures in place to address them.
- In October 2010 the Government of Canada released Canada's Cyber Security Strategy. The Government is improving its ability to respond to cyber security incidents, working to update government policy to tackle complex cyber security issues, and engaging provincial governments and private sector stakeholders to collaborate on cyber security.
- The first pillar of the Strategy is Securing Government Systems and the creation of Shared Services Canada is a great example. The move within Government to one email system, the reduction in the overall number of data centres, and the streamlining of electronic networks will make IT more secure and reliable as well as improving services to Canadians (http://news.gc.ca/web/article-eng.do?nid=614499)

From: Swift, Andrew
Sent: February-15-12 5:57 PM
To: 'Emma.Bedard@aadnc-aandc.gc.ca'
Cc: 'Angela.Matchim@aadnc-aandc.gc.ca'; 'Isabelle.Duguay@aadnc-aandc.gc.ca'; '[redacted]@CSE-CST.GC.CA'; '[redacted]@cse-cst.gc.ca'; Williams, Christpher; Slack, Jessica; Filipps, Lisa
Subject: Re: FW: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

No, direction is for aandc to take the call.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: Emma Bedard [mailto:Emma.Bedard@aadnc-aandc.gc.ca]
Sent: Wednesday, February 15, 2012 05:54 PM
To: Swift, Andrew
Cc: Angela Matchim <Angela.Matchim@aadnc-aandc.gc.ca>; Isabelle Duguay <Isabelle.Duguay@aadnc-aandc.gc.ca>; [redacted]@cse-cst.gc.ca>; Jean J. Plamondon <[redacted]@cse-cst.gc.ca>; Williams, Christpher; Slack, Jessica; Filipps, Lisa
Subject: Re: FW: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Thank you Andrew,

We will instruct our Public Affairs team to refer this media inquiry to Public Saftey.

Regards,
Emma

Emma Bédard
Communications Advisor / Conseillère en communications
Aboriginal Affairs and Northern Development Canada / Affaires autochtones et Développement du Nord Canada
1900 - 10 rue Wellington St.
Gatineau, QC K1A 0H4
Tel: 819-934-6532
Fax: 819-934-3423
emma.bedard@aandc-aadnc.gc.ca
>>> "Swift, Andrew" <Andrew.Swift@ps-sp.gc.ca> 2/15/2012 5:29 PM >>>

Emma,

We've consulted our Minister's Office and PCO and suggest that the following standard lines to this line of questioning be provided by AANDC.

- We do not comment on security threats. That said, our government takes threats seriously and has measures in place to address them.
- In October 2010 the Government of Canada released Canada's Cyber Security Strategy. The Government is improving its ability to respond to cyber security incidents, working to update government policy to tackle

complex cyber security issues, and engaging provincial governments and private sector stakeholders to collaborate on cyber security.

- The first pillar of the Strategy is Securing Government Systems and the creation of Shared Services Canada is a great example. The move within Government to one email system, the reduction in the overall number of data centres, and the streamlining of electronic networks will make IT more secure and reliable as well as improving services to Canadians (http://news.gc.ca/web/article-eng.do?nid=614499)

I've cc'd my PCO analyst who will confirm with yours on the proposed direction.

Thanks,

Andrew

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: [redacted] [mailto: [redacted] @CSE-CST.GC.CA]
Sent: February-15-12 5:11 PM
To: Emma Bedard
Cc: Slack, Jessica; [redacted]; Plamondon, Jean J.
Subject: RE: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

Classification: UNCLASSIFIED

Hello Emma,

Thank you very much for the opportunity to review these lines.

I suspect that Public Safety may want to respond on behalf of the GC and am copying them on this.

Hope to have a decision shortly.

Best,

[redacted]
Media Relations/Public Affairs
Communications Security Establishment Canada

[redacted]
Relations avec les médias/affaires publiques
Centre de la sécurité des télécommunications Canada
Tel. (613) 991-7248 Fax (613) 991-7691

From: Emma Bedard [mailto:Emma.Bedard@aadnc-aandc.gc.ca]
Sent: February 15, 2012 4:23 PM
To:
Cc: Angela Matchim; Isabelle Duguay
Subject: Media Call - Aboriginal Affairs and Northern Development Canada - Hacking Threats

PLEASE NOTE - the media response below is DRAFT, for your information only and not to be shared until approved.

Hello

As discussed, attached is a draft response to address the following media call:

Journalist, APTN
Hacking group Anonymous is picking up the indigenous cause. Is AANDC prepared to deal with hacking attacks? Are we aware of potential threats?

DEADLINE: Today, end of day.

AANDC PROPOSED RESPONSE:

- AANDC is aware of the current threat concerning the Anonymous group.
- AANDC manages the risk of security breaches through a layered perimeter defense implementation and through coordinated communications with the Communication Security Establishment Canada (CSEC).
- CSEC is the technical lead for information technology security to safeguard Government of Canada electronic information.
- For more information on technology security at the Government of Canada, please contact their Media Relations Office at 613-991-7248.

We are currently circulating this response in internal approvals. Please advise asap if you have any issues/concerns with the above statements.

Thank you,

Emma Bédard
Communications Advisor / Conseillère en communications
Aboriginal Affairs and Northern Development Canada / Affaires autochtones et Développement du Nord Canada
1900 - 10 rue Wellington St.
Gatineau, QC K1A 0H4
Tel: 819-934-6532
Fax: 819-934-3423
emma.bedard@aandc-aadnc.gc.ca

Pages 225 to / à 226

are duplicates of

sont des duplicatas des

pages 362 to / à 363

Slack, Jessica

From: Slack, Jessica
Sent: May-31-12 10:11 AM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Mueller, Mike; Williams, Christpher
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca); Durand, Stéphanie; Swift, Andrew (Andrew.Swift@ps-sp.gc.ca); Champoux, Martin; Carta, John; Eke, Darren; Picard, Josée
Subject: Notification: Media call on Cyber
Attachments: ccirc atip may 12.pdf; ps atip cyberthreats may 12.pdf

Good morning,

We received the call below from Bloomberg.

Consulting with policy. Proposed responses to follow. ATIs he cites are attached for reference.

Jessica

Reporter's Name	[redacted]
Media Outlet	**Bloomberg**
Call Date	**5/31/2012 11:00 AM**
Telephone	[redacted]
E-mail address	[redacted]**@bloomberg.net**
Deadline	**5/31/2012 5:00 PM**
Status	**Consulting**
Branch	**NS**
Subject	**TBD**
Questions	**I have some questions regarding two documents I recently received through ATIP. They are attached. My deadline is 5pm Friday.** **Here are my questions for each document:** **1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):** **- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?** **- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?** **- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?**

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?
- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

COPY

Public Safety Canada | Sécurité publique Canada
Deputy Minister | Sous-ministre
Ottawa, Canada
K1A 0P8

SECRET – CEO

DATE: AOUT AUG 10 2011

File No.: 381594
RDIMS No.: Dragon 549

MEMORANDUM FOR THE MINISTER

UPDATE ON CYBER SECURITY INITIATIVES IN CANADA

(Information only)

ISSUE

As you requested, this note provides an update on initiatives underway across Government to improve cyber security in Canada.

BACKGROUND

As you will recall, in October 2010, you launched *Canada's Cyber Security Strategy* in recognition of the significant cyber risks to Canada and the leadership role of the Government in addressing those risks. The first year of Strategy implementation has played out in the context of a highly dynamic global cyber environment. In particular, the past year has seen continued evolution in the nature of the cyber threat and in the attention being devoted to cyber security by the international community.

The cyber risk environment is difficult to quantify, but several points are clear. First, the threat environment is likely worsening, and is certainly no better, than a year ago. Second, poor cyber security is increasingly recognized as impacting not just national security, but also public safety and economic prosperity through growing cyber crime and loss of intellectual property. Third, while measuring the impact of cyber threats continues to be difficult, all new knowledge obtained indicates the problem is more widespread than previously thought.

Cyber security has continued to gain profile as an international political issue this past year. The United States (U.S.) launched their *International Strategy for Cyberspace*, the United Kingdom (U.K.) proposed and will host a meeting of over 60 countries to discuss international norms and standards for cyberspace, and the number of cyber incidents garnering international media attention has climbed. The willingness of elected officials to publicly name other nation states as being responsible for, or complicit in, cyber attacks has also climbed noticeably.

CURRENT STATUS

Despite these changes, the Strategy remains current and applicable, and is acting effectively as an overall framework to guide Government cyber security activities. Implementation of the Strategy is on track per original estimates. The Strategy's objectives are also being advanced by other related Government initiatives.

With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts, and the subsequent recognition of non-government partners of Government's commitment to cyber security;
- strengthening Government networks and security measures, [redacted]
- the transfer of incident response coordination to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates.

In related work, there has been substantial effort to clarify and mitigate the cyber threat posed by increasingly active nation states, [redacted]

s.69(1)(g) re (a)
s.69(1)(g) re (c)

In addition, the recent announcement of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, will complement the Strategy by facilitating improved security.

With respect to Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- reorienting the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, and industry.

With respect to Pillar 3 of the Strategy, "help Canadians to be secure online," progress includes:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS's Communications Directorate, as the federal lead for cyber security communications, will be launching a national public awareness campaign to

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;

- in late 2010, the Government passed anti-spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) is establishing the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cyber crime.

In response to growing international attention to cyber security, PS is leading a number of cross-government initiatives that have emerged within the past year. Discussions are ongoing with our Five Eyes allies regarding the establishment of international norms and standards for conduct in cyberspace in preparation for the London International Cyber Conference in November 2011. The Minister of Foreign Affairs and yourself have both been invited to attend the conference, and officials are working with international counterparts to prepare Canada's position and advise on an approach to participation. In addition, the Canada-U.S. Beyond the Border vision for perimeter security and economic competitiveness includes two cyber security initiatives that focus on bilateral cooperation and cooperation in international fora.

CONCLUSION

Cyber security is a shared responsibility, and by continuing to advance *Canada's Cyber Security Strategy* and related emerging initiatives, the Government is doing its part. The Strategy remains relevant today as a framework and guide for Government cyber security activities. I expect the coming year to be as dynamic as the last, and will keep you apprised of progress and key developments, as necessary.

Should you require additional information, please do not hesitate to contact me or Ms. Lynda Clairmont, Assistant Deputy Minister, Emergency Management and National Security, at 613-990-4976.

William V. Baker

Prepared by: Melanie Mohammed

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

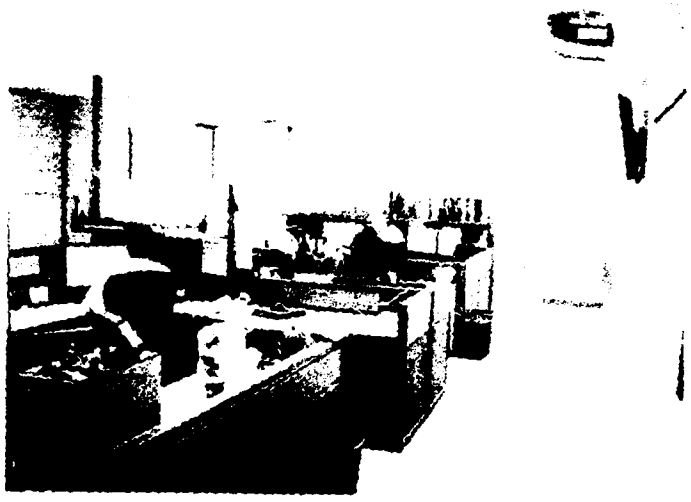
Public Safety Canada | Sécurité publique Canada

January 2012
RDIMS: 538454

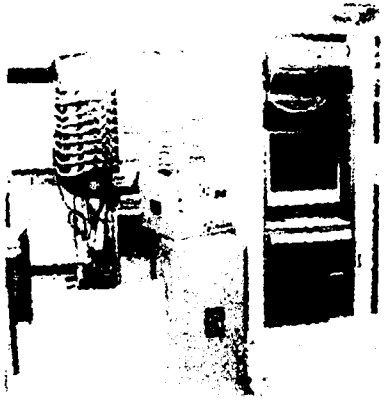
Canada

- Brief on CCIRC – what it is, who it is, what it does
- Discuss challenges and opportunities
- Seek agreement on way forward

- Incident response centre
  - primary contact point into Government for domestic and international partners
  - CCIRC subject matter experts respond 9-5, 5 days a week
  - after hours coverage by Government Operations Centre



- Computer lab
  - isolated from corporate network for analyzing malicious software and testing solutions
  - industrial control system equipment for security testing and analysis in support of CI sectors



CCIRC – [redacted]

- 22 FTEs, 14 staffed
  - mainly highly specialized computer specialists (CS) with knowledge of IT security, computer forensics, and incident handling
  - 4 positions to be staffed for analysis of multi-source intelligence and technical data and writing strategic assessments
- Organized into three functions:
  - Incident Handling – assists partners in identifying, mitigating, and managing incidents
  - Technical Support – operates CCIRC lab infrastructure and provides technical analysis support to incident handling and analysis
  - Strategic Initiatives and Situational Awareness – builds and maintains operational relationships with partners, and produces strategic analysis products for decision makers

CCIRC – what it does

These partners… *provide information to…* *which provides these services:*

- Government S&I community
- Critical Infrastructure
- Provinces and territories
- Five Eyes and International CERTs
- Trusted vendors
- Academia
- Cyber security expert community
- Open source

→ CCIRC →

Incident Handling and National Event Coordination and Assistance
- Direct technical assistance to partners and coordination of Government response to cyber events of national significance
- Audience: technical staff in partner organizations responding to cyber incidents
- Metric: 749 incidents responded to in 2011: 197 notifications to partners of compromised systems. 9 requests issued to shut down malicious systems in Nov/Dec 2011

Provision of Mitigation Advice
- Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice
- Audience: technical staff in partner organizations
- Metric: 27 Cyber Flashes, 6 Alerts, 49 Advisories, and 13 Technical Notes in 2011

Reporting and Analysis
- Daily, weekly, monthly and annual reports providing summary, trend, and strategic analysis
- Audience: technical staff, decision makers (under development)

Current challenges

- Incident Handling and National Event Coordination and Assistance
  - we can't say no – difficult to prioritize clients and services without clearly defined mission and mandate; prospective client base too broad
  - ambiguity of roles in an emergency – absence of a national emergency policy for cyber creates ambiguity for Government and Public Safety
  - limited profile – increased awareness of CCIRC and a credible brand will increase incident reporting
- Provision of Mitigation Advice
  - technology – lab infrastructure aging
  - people – attraction and retention of specialized, bilingual, TOP SECRET staff an ongoing challenge
  - policy – sharing sensitive information
  - accommodations – lack of long-term plan to obtain permanent and highly secure space hampers ability to handle classified information
- Reporting and Analysis
  - strategic analysis product for broader audience to be developed

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Progress in 2011 – work underway within NCSD

- Incident Handling and National Event Coordination and Assistance
  - 6 positions staffed this year; 8 remaining to attain full complement of 22; process underway for 4 more CS03s
  - working with U.S. on plan to inventory and explore potential alignment of information products (e.g., flashes, alerts, technical reports) (NCSD*)
- Provision of Mitigation Advice
  - initiated investment in lab infrastructure
    - $420K this fiscal for some updated technology
  - development of an Industrial Control System (ICS) test-bed in conjunction with Defence R&D Canada and the private sector
  - launched development of secure web portal for info exchange with CI / PT
  - information-sharing MOUs under development with selected PTs and CI sectors (NCSD*)
- Reporting and Analysis
  - working with S&I community on potential joint products (NCSD*)

* Other divisions within NCSD engaged or leading

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Near term objectives (January – March)

- Incident Handling and National Event Coordination and Assistance
  - initiate discussions with PTs on national cyber incident response (NCSD*)
  - conduct federal tabletop exercises to clarify roles in a national response (NCSD*)
  - consult U.S. on initial draft of Canada-U.S. Cyber Security Action Plan to consolidate and drive commitments under Beyond the Borders and other forums (NCSD*)
  - launch anticipatory staffing for Cyber Defence initiative's potential 14 new FTEs for CCIRC with projected start date of April 1, 2012 (CCIRC)
  - develop standardized training regime and integration packages (NCSD*)
- Provision of Mitigation Advice
  - increased engagement with PT and private sector partners (NCSD*, CCIRC)
  - launch secure portal as repository for CCIRC products and mitigation advice (CCIRC)
  - work with corporate branch on short-term accommodations plan for CCIRC
- Reporting and Analysis
  - identification of partner requirements and defining new products and services (NCSD*)

* Other divisions within NCSD engaged or leading

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Near term objectives (cont.): Define mission space

FOR DISCUSSION ONLY

Proposed mandate

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention, mitigation, and response to cyber events.

CCIRC provides authoritative advice to, and coordinates information sharing and event response among, all levels of government, international counterparts, critical infrastructure operators and information technology vendors.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Medium term objectives (April - September)

- Incident Handling and National Event Coordination and Assistance
  - explore potential short-term personnel exchange with CSEC's Cyber Threat Evaluation Centre for new fiscal year
  - conduct tabletop exercise with willing PTs and CI sector representatives to advance national cyber incident response framework and identify policy issues
  - begin implementation of alignment of information products with US-CERT
  - finalize plans with PS-Comms on CCIRC name change, re-branding, re-launching to enhance credibility, visibility, and help to address staff attraction and retention
  - initiate work to develop a cyber Emergency Support Function (ESF) under the Federal Emergency Response Plan (FERP)
- Provision of Mitigation Advice
  - work with corporate branch on long-term accommodations plan for CCIRC and NCSD
  - improve secure connectivity with CSEC
  - explore options for automation in lab testing and analysis, more technology
- Reporting and Analysis
  - pilot production of new products and services for new audiences (CCIRC)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Where CCIRC fits in *Canada's Cyber Security Strategy*

Securing Federal Government Systems

Key actors:
- CSEC
- Shared Services
- TBS CIOB
- CF

Partnering to Secure Vital Systems Outside the Federal Government

Key actors:
- PS CCIRC, NCSD, CISCD
- CI Sector lead departments

Existing effort:
- PT, select CI (telecom, energy, finance)
- U5 CERTs

Future effort:
- trusted vendors
- international CERTs
- remaining CI sectors
- economic interests
- academia

Helping Canadians to be Secure Online

Key actors:
- PS Communications
- law enforcement
- Industry Canada
- CRTC
- Privacy Commissioner
- Competition Bureau

Audiences:
- Home users
- Academia
- Small business

State-sponsored cyber espionage ← ***Risk*** → **Crime**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Goal and Objectives

- DRDC's Center for Security Science (CSS) has provided CCIRC with $200K of funding to champion a *System Control And Data Acquisition* (SCADA) test bed project following a bidding process with organisations interested in executing research and development projects in the field of cyber security.

Project Overview

- This project calls for the establishment of a SCADA network security test bed within the PSC CCIRC (Canadian Cyber Incident Response Centre) secure lab facility. The test bed is to be used for assessment, testing and evaluation of SCADA network architectures, vulnerabilities, and defence mechanisms as well as development of best practices for securing such networks.

- A key project objective is to build greater capacity among Canadian government, industry and academia in the area of SCADA network security.

Project Outcomes

- Create a SCADA Network test bed by identifying and procuring various SCADA components (two test bed/simulators: (1) Gas and chemical plant and (2) Electric Power plant);
- Identify the vulnerabilities of various SCADA components or protocols as applicable to the test bed;
- Use various tools to validate or expose those vulnerabilities;
- Conduct testing with a minimum of two existing SCADA networks security technologies and test their abilities to overcome the identified vulnerabilities;
- Share the outcomes of this project with other groups to increase the size of the Canadian resource pool with SCADA cyber security expertise. Examples could include Federal Government departments and universities researchers;
- Host the test bed at a CCIRC secure lab facility where it will have utility following this specific project;
- Develop a best practices manual for securing SCADA networks;
- Develop a red/blue team exercise environment that will enable training and capacity building in the area of SCADA security.

Quick Facts Sheet

Federal Lead: Public Safety Canada

Partnership: Solana Networks

Start-End: April 2011 to March 2012

Funds: PSTP $200K

In-Kind $171K

Total $371K

- Objective:

  To fill the knowledge and capability gap concerning the construction and use of a SCADA test-bed for purposes of evaluating cyber security of SCADA networks managing Canada's critical infrastructure sector.

- Technologies:

  Provide CCIRC's analysis laboratory with basic control systems setup to increase its forensic capabilities.

  Help build a body of knowledge of best practices of network security for the CoP operating control systems

- Outputs:

  Setting up a SCADA test-bed in a protected laboratory environment and study how it can be applied to test out various network architectures.

  Evaluate security technologies on the various architectures.

  Develop best cyber security practices and recommendations.

- Impact:

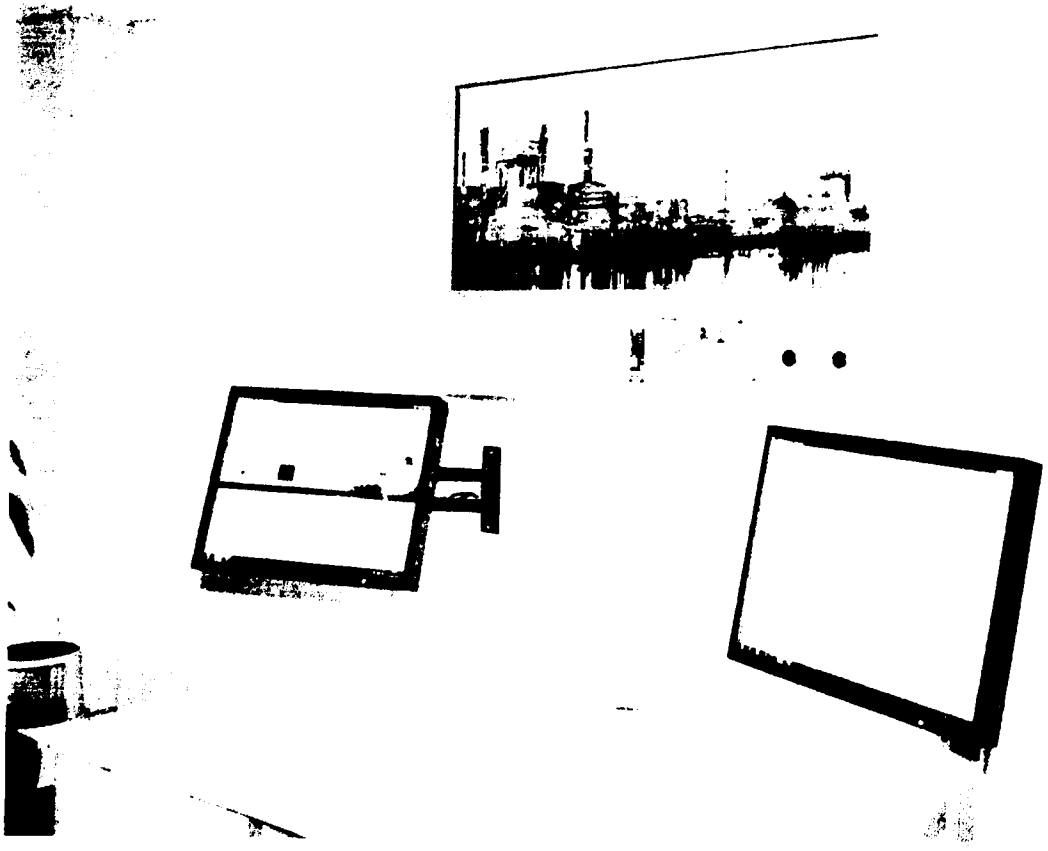
  Give CCIRC the opportunity to promote and advance collaboration across the community of practice.

  Increase cyber security readiness within the CoP by leveraging CCIRC's centre of expertise and information sharing.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Example of Test Bed Design

BEST AVAILABLE COPY



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada
Senior Assistant Deputy Minister | Sous-ministre adjoint principal
Ottawa, Canada K1A 0P8

UNCLASSIFIED

DATE: Jan 3/12

File No. : 382805
RDIMS No.: 495676

MEMORANDUM FOR THE DEPUTY MINISTER
Via: Gary Robertson, Assistant Deputy Minister, CMB

INTERNATIONAL TRAVEL AUTHORIZATION FOR WINDY ANDERSON AND ROBERT PITCHER TO TRAVEL TO NEW ZEALAND AND AUSTRALIA JANUARY 20 TO FEBRUARY 3, 2012
(Signature required)

ISSUE

Your approval is sought for an amendment to the international travel request for Mrs. Windy Anderson to attend Cyber Emergency Response Team (CERT) meetings in Canberra and Brisbane, Australia, and for Mr. Robert Pitcher to attend a Usual 5 (U5) semi-annual meeting in Wellington, New Zealand and CERT meetings in Australia, from January 20 to February 3, 2012.

BACKGROUND

Mrs. Anderson previously requested and received international travel approval to attend the U5 semi-annual meeting, January 21-28, 2012 in Wellington, New Zealand (**TAB A**). However, Australia has requested separate meetings in Canberra and Brisbane with Canadian U5 participants, the Australian Government and National CERTs. As discussions will include both managerial and operational level topics, Australia has requested that both Mrs. Anderson and an operationally focussed Canadian Cyber Incident Response Centre (CCIRC) participant attend. Mr. Pitcher is the recommended operational expert.
The Communications Security Establishment Canada has also requested that two individuals (Director and Technical Manager) attend both the U5 conference and CERT meetings.

CONSIDERATIONS

The U5 has requested that participating nations send the same personnel to semi-annual meetings. When this is not possible, the U5 has requested that someone who has worked "online" with the U5 attend to ensure consistent national representation and enhanced cooperation as the table is filled with "familiar faces". Mrs. Anderson and Mr. Pitcher fulfill this requirement.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The partnership between Canadian and Australian CERTs is both longstanding and operationally successful. Australia has allocated responsibilities between Government and National CERTs, consistent with Canada's current endeavours. There are significant lessons to be learned from the Australian experience as Canada matures its own CERT capabilities. We will enhance the operational effectiveness of CCIRC as it transitions into its role as Canada's national CERT by leveraging the managerial and operational lessons learned and working together to resolve similar issues in our international partnership with Australia.

Normally, a trip such as this would be cost prohibitive. However, as we are attending the U5 meetings, this is an opportunity to leverage the funding allocated and increase the overall value of the trip. The additional costs for time spent in Australia will be incremental.

The estimated cost of this trip is $26,431.13 for Mrs. Anderson and $12,128.13 for Mr. Pitcher. This estimate provides for a possible increase in airfare during the approval process and for business class travel on long haul flights. The trip is forecasted in the National Cyber Security Directorate's travel cap plan.

RECOMMENDATION

It is recommended that you approve this travel request to New Zealand and Australia by signing the Travel Authority and Advance forms **(TAB B)**. My approval of this trip is noted in the International Travel Request **(TAB C)**.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (3)

I approve:

_____
William V. Baker

Prepared by: Windy Anderson

Public Safety Canada
Assistant Deputy Minister
Ottawa, Canada
K1A 0P8

Sécurité publique Canada
Sous-ministre adjoint

UNCLASSIFIED

DATE: NOV 2 2 2011

File No. : 382805
RDIMS No.: 495676

MEMORANDUM FOR THE DEPUTY MINISTER
Via: Gary Robertson, Assistant Deputy Minister, CMB

INTERNATIONAL TRAVEL AUTHORIZATION FOR WINDY ANDERSON: USUAL 5 SEMI-ANNUAL MEETING, WELLINGTON, NEW ZEALAND, JANUARY 21-28, 2012

(Signature required)

ISSUE

Mrs. Windy Anderson is requesting international travel approval to attend the Usual 5 (U5) semi-annual meeting, January 21-28, 2012, in Wellington, New Zealand.

BACKGROUND

The U5 (Canada, Australia, New Zealand, the United States (U.S.) and the United Kingdom (U.K.)) is the equivalent of the security and intelligence "five eyes community" but focuses solely on cyber emergency response. It is a director level international group that meets twice annually to ensure continual improvement of cooperation and information sharing in the cyber realm.

The U5 nations have established a trust relationship, which facilitates sharing information of mutual interest related to cyber threats, vulnerabilities, incidents or events. This information exchange and collaboration has enhanced each participant country's ability to respond to cyber incidents. Canada has benefited significantly from the U5 partnership in terms of cyber information sharing and cooperation.

The meeting participants include delegates from the New Zealand Centre for Critical Infrastructure Protection, the Australian Attorney General's Department, the U.K. Centre for the Protection of National Infrastructure and the U.S. National Cyber Security Division.

Canada

.../2

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

CONSIDERATIONS

The draft agenda is under development and is currently unavailable; however, historically, it includes operational and policy updates from each country and cyber security issues of common interest. The agenda of the July 2010 meeting that Canada hosted is attached as an example (**TAB A**).

The risk in not attending this meeting is potential weakening of international cooperation. It could also send a negative signal that is contrary to the Canadian Cyber Security Strategy.

The total cost of this trip is estimated to be $15,486.48. This estimate provides for a possible increase in airfare during the approval process and for business class travel on long haul flights. The trip is forecasted in the National Cyber Security Directorate's (NCSD) travel cap plan.

RECOMMENDATION

It is recommended that approval be granted for Mrs. Anderson to travel to Wellington, New Zealand, for the U5 meeting, January 21-28, 2012. Should you agree, your signature is sought on the attached Travel Authority and Advance form (**TAB B**). My approval of this trip is noted in the International Travel Request (**TAB C**).

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, NCSD, at 613-990-2661.

for Lynda Clairmont
Assistant Deputy Minister
National Security

Enclosures: (3)

I approve:

William V. Baker

Prepared by: Windy Anderson

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Annex A
Agenda

DRAFT ANNOTATED AGENDA

Day 1, Wednesday July 7, 2010		
08:00 - 08:30	Arrival, Badging and Coffee	All
08:30 – 08:45	Opening and Welcome	*Robert G. Lesser, Director General, Operations*
08:45 – 09:15	Keynote Speaker	Robert Gordon, Head, Cyber Security Strategy
09:15 – 09:30	Operations Update (10 minutes per country, 5 minute discussion)	New Zealand
09:30 – 09:45		Australia
09:45 - 10:00		United Kingdom
10: 00 – 10:15		United States
10:15 – 10:30		Canada
10:30 – 11:00	Health Break	
11:00 – 11:45	A Strategic View on Cyber Security in Canada	Robert Dick, Director General National Cyber Security
11:45 – 13:00	Lunch	
13:00 – 13:30	IT Incident Management Plan – Government of Canada	Treasury Board Secretariat, Chief Information Officer Branch
13:30 – 14:30	CCIRC Operations Case Studies	Luc Beaudoin, Chief Cyber Operations, CCIRC
14:30 – 15:00	Health Break	
15:00 – 15:45	Law Enforcement Initiatives/Combating Cyber Crime	Royal Canadian Mounted Police
15:45 – 16:15	US Secure Communications	Canada/CCIRC
16:15 – 16:30	Wrap up and Adjourn	Chair
18:00 –??	Social Event (Restaurant)	All (optional)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Day 2, Thursday July 8, 2007		
08:00 – 08:30	Arrival & Refreshments	
08:30 – 09:15	Cyber Threat Evaluation Centre (CTEC)	Communications Security Establishment Canada
09:15 –10:00	National Strategy for Critical Infrastructure - Canada	Public Safety Canada/CIP
10:00 – 10:30	Health Break	
10:30 – 10:45	Policy Update (15 minutes per country – 10 minute brief plus 5 minute discussion)	New Zealand
10:45 – 11:00		Australia
11:00 – 11:15		United Kingdom
11: 15 – 11:30		United States
11:30 – 11:45		Canada
11:45 – 13:00	Lunch	
13:00 – 14:30	Table Top Exercise – U5 Coordination of Operations; CSIII preparation	Bill Casey, Rob Pitcher – Public Safety Canada
14:30 – 15:00	Health Break	
15:00 – 15:30	Supply Chain Risk Management - Canada	Communications Security Establishment Canada
15:30 – 16:00	Public Awareness Strategies	Public Safety Canada
16:00 – 16:15	Wrap up & Adjourn	Chair

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Day 3, Friday July 9, 2010		
8:30 – 9:00	Arrival, Coffee	
9:00 – 10:00	Usual 5 and Communities of Interest *IWWN, Meridian, OSSD, APEC, ITU, NATO …(only those communities identified in advance by U5 members)*	**All**
10:00 – 10:15	Health Break	
10:15 – 11:00	**New topic or extra discussion**	**All**
11:00 – 12:00	Way Forward – Action Items	Chair
12:00	Adjourn	Chair

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE / Autorisation de voyager et avance

☑ Original / Prem. demande

☐ Amended (State levels of approval use original dates) / Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

Part A - Partie A

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No - N° du document
Type 2	Name of traveller - Nom du voyageur: **Windy Anderson**	Classification: **EX-01**

Department - Ministère: **Public Safety Canada**	Branch / Division / Group - Direction / Division / Groupe: **EMNS / Canadian Cyber Incident Response**
Address - Adresse: **340 Laurier Ave**	Telephone No. - No. de téléphone: **613-991-7055**
Branch Contact - Personne ressource à la direction: **Jane Hayward**	Telephone No - No. de téléphone: **613-991-1982**
Purpose of travel - Objet du voyage: **Semi-Annual Usual 5 Meeting to Dicuss Cyber Incident Response**	No. of days / Nbre de jours: **5**

If different address, send cheque to: / Si adresse différente, envoyer chèque à

Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)? ☑ Yes / Oui ☐ No / Non

If no, would you like to request one? / Les cas échéant, aimeriez-vous en avoir une? ☑ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation Transport Mode	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de repérage du dossier
January 21 2011	Ottawa	Wellington, New Zealand	07:30 - 11:40 (Jan 18 2011)	Air			
January 27 2011	Wellington, New Zealand	Ottawa	06:40 - 18:10				

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif	Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel
Accommodation (white page hotel) / Hébergement (un des hôtels figurant dans le partie blanche du répertoire)	$875.00	Accommodation (green page hotel) / Hébergement (un des hôtels figurant dans le partie verte du répertoire)	$0.00	
Mid-size car rental (collision damage waiver mandatory / Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory / Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00	
Private vehicle requested by: / Voiture personnelle demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur. Public Liability and Property Damage min $1 million. Deductibles NON reimbursable / Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)		
		Upgrade transportation (specify in "Class" above) / Transport à tarif supérieur (preciser la <classe> ci-dessus)	$0.00	
Transportation / Transport	$900.00	☐ First class (Deputy Head or equivalent approval) / Prem. Classe (approuvee par le sou-chef ou l'équiv.) ☒ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) / Classe d'affaires - ou autre classe à tarif supérieur (approuvée par le sou-chef ou l'équiv. S'il s'agit d'une classe préférentielle, article 3.1.8)		
Meals and incidentals / Repas et frais accessoires	$988.96			
Other (Specify) - Autre (préciser)	$125.00			

Lynda Clairmont — Approval - Approbation

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$13,200.52
Other - Autre	$2,285.96
Trip Total - Coût total du voyage	$15,486.48

Funding - Financement

A) Travellers cheques / Chèques de voyage	
Can / Can	$0.00
US / E.U.	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
Cheque / Cheque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques internes pour les employeurs distincts) et en accepte les conditions.

Windy Anderson — W Anderson — Oct 21/11
Signature — Date

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature): Lynda Clairmont — Date: Nov 3/11

Approved by (signature) - Approuvé par (signature): William V. Baker — Date: NOV 2 2 2011

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (total information) - Détail (tatori)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P	Amount - Montant	Req. No - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0				| 0	

Type 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Codification	Amount - Montant
			2001 PSABASE 475 500087011	

	Description	Financial encumbrance No / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)

Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)

Service officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)

Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations / Demandé pour paiement conformément à l'article 33 de La sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.

Signature

Cheque No. - N° du chèque

Date

000026

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé				Amount/Montant
Airfare / Frais d'avion				$13,200.52
Train / Train				$0.00
Other / Autres				$0.00
				$13,200.52

Estimated Cost - Coût estimatif: Other - Autre		Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du répertoire)		$175.00	5	$875.00
Accomodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du répertoire)		$0.00	0	$0.00
				$875.00
Mid-size car rental / Location d'une voiture intermédiaire		$0.00	0	$0.00
NON Mid-size car rental / Location d'une voiture NON intermédiaire		$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée				$0.00
				$0.00
		Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé		0.570	0	$0.00
		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage				$0.00
Taxi/Limo	Home to Airport (Train Station)		$50.00	$300.00
	Airport - Train Station) - Hotel - Meetings		$50.00	
	Hotel - Airport (Train Station)		$50.00	
	Airport (Train Station) to Home		$50.00	
	Meeting - Meetings		$100.00	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$300.00
		Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners		$20.33	6	$121.98
Lunch / Déjeuners		$44.32	7	$310.24
Dinner / Dîners		$56.48	5	$282.40
Incidentals /Frais divers		$38.76	7	$271.32
				$985.94
Business Phone / Téléphone d'affaires				$25.00
Airport Improvement Fee / Frais de l'Aeroport				$0.00
Cash Advance Fee / Frais d'avances				$0.00
Misc. Business Services / Diverses charges d'affaires				$0.00
Miscellaneous / Diverses Internet and service charges				$100.00
				$125.00

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage International

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
Meetings with Usual 5 CERT on Cyber Security Issues - New Zealand	From - *Du* : Jan. 21, 2012	To - *Au* : Jan 29, 2012
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
Wellington, New Zealand	~~$19,146.64~~ 15,486.48	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?*	
Agenda attached	☒ Yes/Oui ☐ No/Non	

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Windy Anderson	EMNS - CCIRC	257 Slater Street	(613) 991-7055

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

To participate as the Canadian delegate in the semi annual Usual 5 (U5) (Canada, Australia, New zealand, the United States and the United Kingdom) meetings and roundtable discussions on cyber emergency response.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

This is a director level meeting whose purpose is to ensure continued improvement and information sharing in the cyber realm. The focus of these discussions are cyber vulnerabilities, incidents and events. The information exchange and collaboration enhances each other's abiltity to respond to these cyber incidents.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

There are no other Canadian attendees.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

Consultation is ongoing within Public Safety and our collective knowledge is shared throughout government through our ability to respond to cyber incidents.

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

Name of participant's Director General
Nom du Directeur Générale du voyageur

Oct 7/11
Date

Reviewed by/
Examiné par :

Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

OCT 13 2011
Date

000028

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Approved by/
***Approuvé par*:**

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Nov 3/11
Date

PS023

TRAVEL - Windy Anderson
January 14-21, 2011
Wellington, New Zealand
382805

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE / Autorisation de voyager et avance

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

☐ Original / Prem. demande

☑ Amended (Same levels of approval as original dated) / Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

Part A - Partie A

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No. - N° du document
Type 2	Name of traveller - Nom du voyageur: Windy Anderson	Classification: EX-01
Department - Ministère: Public Safety Canada	Branch / Division / Group - Direction / Division / Groupe: EMNS / Canadian Cyber Incident Response	
Address - Adresse: 340 Laurier Ave	Telephone No. - No. de téléphone: 613-991-7055	If different address, send cheque to: / Si adresse différente, envoyer chèque à
Branch Contact - Personne ressource à la direction: Jane Hayward	Telephone No. - No. de téléphone: 613-991-1982	
Purpose of travel - Objet du voyage: Semi-Annual Usual 5 Meeting to Dicuss Cyber Incident Response and CERT Meetings	No. of days / Nbre de jours: 15	Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)? ☑ Yes / Oui ☐ No / Non	If no, would you like to request one? / Les cas échéant, aimeriez-vous en avoir une? ☐ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Départ / Arrival - Départ	Transportation / Transport: Mode	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de repérage du dossier
January 26, 2012	Ottawa	Sydney	17:35 - 10:20 (22)	Air	2	Personal	
January 14, 2012	Sydney	Wellington, NZ	09:20 - 14:30	Air		TBD	
January 27, 2012	Wellington, NZ	Canberra	15:25 - 19:30	Air		Personal	
February 1, 2012	Canberra	Brisbane	08:45 - 09:25	Air		TBD	
February 3, 2012	Brisbane	Ottawa	06:30 - 16:24	Air	2		

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Standard

Item / Type de dépenses	Estimated cost / Coût estimatif
Accommodation (white page hotel) / Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$1,050.00
Mid-size car rental (collision damage waiver mandatory / Location d'une voiture intermédiaire (assurance-collision du répertoire obligatoire)	$0.00
Private vehicle requested by: / Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur	
Public Liability and Property Damage min $1 million. Deductibles NON reimbursable / Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00
Transportation / Transport	$500.00
Meals and Incidentals / Repas et frais accessoires	$2,156.13
Other (Specify) - Autre (préciser)	$125.00

Non-standard - Spéciales

Item / Type de dépenses	Estimated cost / Coût estimatif
Accommodation (green page hotel) / Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Non mid-size car rental (collision damage waiver mandatory / Location d'une voiture non intermédiaire (assurance-collision du répertoire obligatoire)	$0.00
Other (Specify) - Autre (préciser)	
Upgrade transportation (specify in "Class" above) / Transport à tarif supérieur (préciser la «classe» ci-dessus)	$0.00

☐ First class (Deputy Head or equivalent approval) / Prem. Classe (approuvée par le sous-chef ou l'équiv.)

☑ Business class / Other-Upgraded (other than article 3.1.8 Assistant Deputy Head or equivalent approval) / Classe d'affaires - ou autre classe à tarif supérieur (approuvée par le sous-chef ou l'équiv., sfi s'agit d'une classe non prévue à l'article 3.1.8)

Lynda Clairmont

Approval - Approbation

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Long haul flight

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$22,508.00
Other - Autre	$3,981.13
Trip Total - Coût total du voyage	$26,481.13

Funding - Financement

A) Travellers cheques / Chèques de voyage	
Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
Cheque / Chèque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internet policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politique interne pour les employeurs distincts) et en accepte les conditions.

for Windy Anderson — Signature — Dec 29/11 — Date

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature): Lynda Clairmont — Date

Approved by (signature) - Approuvé par (signature): William V. Baker — Date

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant de chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type: 6 | 0	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur | 0	Due Date / Date d'échéance
Type 4						

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code de fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Ventilation	Amount - Montant
			2001 PSABASE 475 500087011	
	Description			Financial encumbrance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)

Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)

Services officer (PWGSC) (signature) / Agent responsable (TPSGC) (signature)

Requisition for payment pursuant to section 26 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 26 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.

Signature

Cheque No. - N° du chèque

Date

000030

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé

	Amount/Montant
Airfare / Frais d'avion	$22,500.00
Train / Train	$0.00
Other / Autres	$0.00
	$22,500.00

Estimated Cost - Coût estimatif: Other - Autre

	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (WHITE page hotel) / Hébergement (un des hôtels figurent dans la partie BLANCHE du répertoire)	$175.00	6	$1,050.00
Accomodation (GREEN page hotel) / Hébergement (un des hôtels figurent dans la partie VERT du répertoire)	$0.00	0	$0.00
			$1,050.00
Mid-size car rental / Location d'une voiture intermédiaire	$0.00	0	$0.00
NON Mid-size car rental / Location d'une voiture NON intermédiaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.570	0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage				$0.00
Taxi/Limo	Home to Airport (Train Station)		$50.00	$500.00
	Airport (Train Station) - Hotel / Meetings		$100.00	
	Hotel - Airport (Train Station)		$100.00	
	Airport (Train Station) to Home		$50.00	
	Meeting - Meetings		$200.00	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$500.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$20.33	13	$264.29
Lunch / Déjeuners	$44.32	13	$576.20
Dinner / Dîners	$56.48	13	$734.24
Incidentals /Frais divers	$38.76	15	$581.40
			$2,156.13
Business Phone / Téléphone d'affaires			$25.00
Airport Improvement Fee / Frais de l'Aeroport			$0.00
Cash Advance Fee / Frais d'avances			$0.00
Misc. Business Services / Diverses charges d'affaires			$0.00
Miscellaneous / Diverses Internet and service charges			$200.00
			$225.00

25•50X
0•7972=
20•3286‡

National Joint Council

55•60X
0•7972=
44•32432‡

ective, Appendix D - Allowances - - Effective July 1, 2011

- Allowances - Module 4

or City:

70•85X
0•7972=
56•48162‡

Return to alphabetical list | Get Rates

Archives: Current - July 1, 2011

id

Accommodation
cial Accommodation
nd justifiable expenses. Receipts required.

48•62X
0•7972=
38•759864‡

- Currency: New Zealand Dollar (NZD)

Type of Accommodation	City	Meal Rate Breakfast	Lunch	Dinner	Meal Total	Incidental Amount	Grand Total (Taxes Included)
C	Auckland	31.60	56.10	70.20	**157.90**	***50.53***	**208.43**
C-75%	Auckland	23.70	42.08	52.65	**118.43**	***37.90***	**156.32**
P	Auckland	31.60	56.10	70.20	**157.90**	***31.58***	**189.48**
P-75%	Auckland	23.70	42.08	52.65	**118.43**	***23.69***	**142.11**
C	Wellington	25.50	55.60	70.85	**151.95**	***48.62***	**200.57**
C-75%	Wellington	19.13	41.70	53.14	**113.96**	***36.47***	**150.43**
P	Wellington	25.50	55.60	70.85	**151.95**	***30.39***	**182.34**
P-75%	Wellington	19.13	41.70	53.14	**113.96**	***22.79***	**136.76**
C	Other	20.40	44.48	56.68	**121.56**	***38.90***	**160.46**
C-75%	Other	15.30	33.36	42.51	**91.17**	***29.17***	**120.34**
P	Other	20.40	44.48	56.68	**121.56**	***24.31***	**145.87**
P-75%	Other	15.30	33.36	42.51	**91.17**	***18.23***	**109.40**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

10-year currency converter

Conversions are based on Bank of Canada nominal noon exchange rates, which are published each business day at about 12:30 ET.

View or save this data in: **SDMX** (http://www.bankofcanada.ca/stats/results/xml?rangeType=range&rangeValue=1&fee=0.04&sF=LOOKUPS_IEXE1901&lP=lookup_currency_converter.php&sR=2001-09-30&sTF=to&sT=L_CAD&co=1.00&dF=&dT=) , **XML** (http://www.bankofcanada.ca/stats/results/p_xml?rangeType=range&rangeValue=1&fee=0.04&sF=LOOKUPS_IEXE1901&lP=lookup_currency_converter.php&sR=2001-09-30&sTF=to&sT=L_CAD&co=1.00&dF=&dT=) , **CSV** (http://www.bankofcanada.ca/stats/results/csv?rangeType=range&rangeValue=1&fee=0.04&sF=LOOKUPS_IEXE1901&lP=lookup_currency_converter.php&sR=2001-09-30&sTF=to&sT=L_CAD&co=1.00&dF=&dT=)

1.00 NZD (New Zealand dollar)

CAD (Canadian Dollar)

Date	CAD = Canadian Dollar	Exchange rate
2011-09-30	0.77 CAD	0.7972 [1.2544]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Countries and cities	Rate Limit
Afghanistan	
Angola	
All cities	380
Antigua and Barbuda	
January 1 - April 15	205
April 16 - December 14	174
December 15 - December 31	205
Argentina	
Bariloche	157
Buenos Aires	196
Cordoba	151
Salta	145
Other	121
Armenia	
All cities	151
Ascension Island	
All cities	20
Australia	
Adelaide	248
Brisbane	223
Cairns	181
Canberra	218
Darwin	
January 1 - March 31	140
April 1 - September 30	228
October 1 - December 31	140
Fremantle	243
Hobart	238
Melbourne	257
Perth	319
Richmond	203
Sydney	218
Other	204
Austria	
Graz	207
Innsbruck	193
Linz	193
Salzburg	229
Vienna	200
Other	193
Azerbaijan	

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Countries and cities	Rate Limit
Namibia	
December 15 - December 31	190
Other	
January 1 - April 14	155
April 15 - December 14	118
December 15 - December 31	155
New Caledonia	
All cities	192
New Zealand	
Auckland	167
Christchurch	142
Queenstown	152
Rotarua	149
Wellington	178
Other	116
Nicaragua	
Managua	144
Other	58
Niger	
Niamey	107
Other	97
Nigeria	
Abuja	376
Bauchi	187
Calabar	171
Enugu	165
Ibadan	113
Jos	154
Kaduna	165
Kano	231
Lagos	265
Maiduguri	116
Sokoto	105
Warri	180
Yenagoa	164
Other	116
Niue	
All cities	80
Norway	
Oslo	210
Stavanger	212

Windy giving authority to Danielle to sign on her behalf as a traveler.

St-Louis, Danielle

From: Anderson, Windy
Sent: December-29-11 2:14 PM
To: St-Louis, Danielle
Subject: Re: URGENT: Travel to Australia and New Zealand January 20 - February 3

Just sign it then.

Windy

From: St-Louis, Danielle
Sent: Thursday, December 29, 2011 02:12 PM
To: Anderson, Windy
Cc: Hayward, Jane
Subject: RE: URGENT: Travel to Australia and New Zealand January 20 - February 3

I am **NOT** signing anything for 32 or 34. I would only be signing for you as a traveler.

Time lines are already tight. International travels are supposed to be in the DMs hands 6 weeks before the travel date (beginning of December for this particular travel)
I know we have the money but if we submit the First TAA and we end up spending more than what we had asked for, you would then have to write a memo to the DM justifying why you overspent what you had requested and ask for his approval to proceed with the travel claim. If he does not approve, this extra travel expense that we did not ask for comes out of your pocket.
If we spend less than what we asked for, everything is good to go.

We can play with the flights when we get the booking stage but for now we have to seek DM's approval. I would suggest that you call Robert if there is still discomfort.

Danielle St-Louis
613-991-7738

From: Anderson, Windy
Sent: December-29-11 1:57 PM
To: Hayward, Jane; St-Louis, Danielle
Subject: Re: URGENT: Travel to Australia and New Zealand January 20 - February 3

I have not yet really seen the travel. Let's just wait until I get back. Can we?

Will I loose what you already did if we wait?

Windy

From: Hayward, Jane
Sent: Thursday, December 29, 2011 01:47 PM
To: St-Louis, Danielle; Anderson, Windy
Subject: Re: URGENT: Travel to Australia and New Zealand January 20 - February 3

The reservation still exists buit was not confirmed by sophie on friday therefore has not been ticketed. Call travel 1 800 514 3798 and quote locator number ICPFGW if you want to proceed, Jane

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

From: St-Louis, Danielle
Sent: Thursday, December 29, 2011 01:20 PM
To: Lajeunesse, Elizabeth
Cc: Hayward, Jane; Isel, Zabrina; Fix, Sophie
Subject: FW: URGENT: Travel to Australia and New Zealand January 20 - February 3

I should have maybe CCed you on this

Danielle St-Louis
613-991-7738

From: St-Louis, Danielle
Sent: December-29-11 1:19 PM
To: Anderson, Windy
Cc: Weir, Sarah; Bendelier, Kenneth
Subject: RE: URGENT: Travel to Australia and New Zealand January 20 - February 3

Hi Windy.

Keep in mind that your flight has not been booked yet and prices increase every day the longer we wait to book your flight.
The estimate I got from Travel Voyage yesterday was
Ottawa to Sydney - business class - (return trip) = **13,929.88** (today it is 14,255.88 so it already went up $300 in one day)
Economy Flights from Sydney to Wellington; Wellington to Camberra; Camberra to Brisbane; Brisbane to Sydney = **$1242** (yesterday's estimated cost)
At it together, we have ~ $15,000. As advised by Elizabeth Lajeunesse (Finance Advisor for National Security), I have added 50% of the total cost to allow flexibility in the price increase until your travel is booked. Therefore, I've added **$7,500**. The total cost including accommodations and other travel related expenses (which I did not modify) add up to **$26,431.13**

I hope this explains the increase in your flight travels.
Please call me if you have any further questions

Danielle St-Louis
613-991-7738

From: Anderson, Windy
Sent: December-29-11 12:25 PM
To: St-Louis, Danielle
Cc: Weir, Sarah
Subject: Re: URGENT: Travel to Australia and New Zealand January 20 - February 3

Danielle,

When Jane and I looked at the travel, the to and from was approx. 5K each way. Add on the extra travel in Australia should not be more than 2K. How did you get 22K. It makes absolutely no sense to me.

Windy

From: St-Louis, Danielle
Sent: Thursday, December 29, 2011 11:42 AM
To: Anderson, Windy
Cc: Weir, Sarah

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Subject: FW: URGENT: Travel to Australia and New Zealand January 20 - February 3

Please include Sarah Weir in the CC when you respond.

Thank you,

Danielle St-Louis
613-991-7738

From: St-Louis, Danielle
Sent: December-29-11 10:09 AM
To: Anderson, Windy
Cc: Hayward, Jane; Isel, Zabrina; Lajeunesse, Elizabeth
Subject: URGENT: Travel to Australia and New Zealand January 20 - February 3
Importance: High

Windy,

I have made changes to your Travel Authority and Advance to reflect a more realistic cost estimate on your flight. It is now an estimate of $22,500. Can you please give me authority to sign your TAA on your behalf?

Thank you

Danielle St-Louis
Administrative Assistant | Adjointe administrative
Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 rue Slater St | Ottawa ON K1A 0P9
Telephone | Téléphone: 613-991-7738 Fax | Téléc.: 613-991-3574
E-mail | Courriel: danielle.st-louis@ps-sp.gc.ca

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada / Sécurité publique Canada

RDIMS: 525670

Commitment Authority (Section 32 FAA) Checklist

(version française est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	Questions
☑	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?

☑ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☐ Request to Attend Conferences Form	☐ Training Application and Authorization Form	☐ Membership Approval Form	☐ Other Specify:

☑	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?
☑	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR? monies reserved
N/A	Have I completed all the paperwork requested by the Contracting Material Management group? ☐ Is the Sole Source Checklist complete and attached? ☐ Is the Competitive Contract Checklist complete and attached?
☑	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☑ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☑ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.
N/A	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☐ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☐ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*

	Purchase Requisition #	Purchase Order #	Funds Commitment #:	RDIMS #
	[redacted]	[redacted]	[redacted]0840 11	[redacted]

000039

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

St-Louis, Danielle

From: St-Louis, Danielle
Sent: December-29-11 9:51 AM
To: St-Louis, Danielle
Subject: Emailing: Itinerary, Price and Alternatives

Add 50% due to TAA purposes
DS.

Skip to page content

Travel AcXess Voyage

[redacted] AMERICAN EXPRESS "BUSINESS TRAVEL"

Log Out
Traveler: Danielle St Louis
Site gocenglish

- Home
- Trips
- Templates

Help with this page

Your trip so far...
Fri, 20 Jan 2012 - Fri, 03 Feb 2012

view details

Flight Details			
Fri, 20 Jan	17:35 - 20:00	Ottawa, Ontario (YOW) to Vancouver, British Columbia (YVR) Non-stop	AIR CANADA Air Canada Flight 189 Seat not assigned Class: Business Classe affaires
The departure and arrival dates are different.			
	23:45 - 10:20 Arrives Sun, 22 Jan	Vancouver, British Columbia (YVR) to Sydney, New South Wales (SYD) Non-stop	AIR CANADA Air Canada Flight 33 Seat not assigned Class: Business Classe affaires
Fri, 03 Feb	12:15 - 07:25	Sydney, New South Wales (SYD) to Vancouver, British Columbia (YVR) Non-stop	AIR CANADA Air Canada Flight 34 Seat not assigned Class: Business Classe affaires
	08:50 - 16:24	Vancouver, British Columbia (YVR) to Ottawa, Ontario (YOW) Non-stop	AIR CANADA Air Canada Flight 166 Seat not assigned Class: Business Classe affaires

Flight Total: Can$14,255.88

Hotel Details

Car Details

Itinerary, Price and Alternatives

Ottawa (YOW) to Sydney (SYD): Fri, 20 Jan 2012

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Sydney (SYD) to Ottawa (YOW): Fri, 03 Feb 2012

Skip over modify search
▶Modify search
▼Modify search

(X) **Shop by Schedule**
Search by schedule to see more flight options.
( ) Shop by Price
Find the lowest-priced options for your destination.

* = Required

* From (airport or city):
YOW
* To (airport or city):
SYD
Depart:
[leaves V] [12:00 V]
Return:
[leaves V] [12:00 V]

Cabin Class
[Business Classe affaires V]
Fare Type:
[Lowest available / Tarif le moins cher V]

Preferred Airlines:
[1st Selection V]
[2nd Selection V]
[3rd Selection V]

Search Again

Company Announcements

Government of Canada Travel Policies
Common airport codes
Important Information on Air Canada Seat Selection
Important Information on WestJet
Important information on Porter Airlines
Via Rail Station Codes

All times are local to each city

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Legend: Company Negotiated Rate Out of Policy

Your Selected Itinerary

Departure	Arrival	Airline	Notes	Price
17:35 - Fri, 20 Jan Ottawa, Ontario (YOW)	20:00 - Fri, 20 Jan Vancouver, British Columbia (YVR)	AIR CANADA Flight 189 - Airbus A320 Class: Business Classe affaires Fare Rules	Non-stop 2209 miles View seats	
23:45 - Fri, 20 Jan Vancouver, British Columbia (YVR)	Different Date 10:20 - Sun, 22 Jan Sydney, New South Wales (SYD)	AIR CANADA Flight 33 - Airbus A320 Class: Business Classe affaires Fare Rules	Non-stop Total flight time 24:45 7775 miles View seats	Can$14,255.88 Select
12:15 - Fri, 03 Feb Sydney, New South Wales (SYD)	07:25 - Fri, 03 Feb Vancouver, British Columbia (YVR)	AIR CANADA Flight 34 - Airbus A320 Class: Business Classe affaires Fare Rules	Non-stop 7775 miles View seats	
08:50 - Fri, 03 Feb Vancouver, British Columbia (YVR)	16:24 - Fri, 03 Feb Ottawa, Ontario (YOW)	AIR CANADA Flight 166 - Airbus A320 Class: Business Classe affaires Fare Rules	Non-stop Total flight time 20:09 2209 miles View seats	

Help with this page

Low Fare Options

The following alternate itineraries, including nearby airports, may also fit your schedule and budget.

Departure	Arrival	Airline	Notes	Price (estimate)
Option 1				
20:00 - Fri, 20 Jan Ottawa, Ontario (YOW)	21:05 - Fri, 20 Jan Toronto, Ontario (YYZ)	WESTJET Flight 613 Class: Economy Économique Fare Rules	Non-stop 225 miles N/A on-time View seats	Can$9,968.92 Select
Different Date 01:30 - Sat, 21 Jan	Different Date 06:05 - Sun, 22 Jan	CATHAY PACIFIC Flight 829 - Boeing 777-300	Non-stop 7805 miles	

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

St-Louis, Danielle

Subject: Emailing: Reserve Seats for Flight 2 of 5

Add 60% Due to TAA purposes.

Skip to page content

Travel AcXess Voyage

[redacted] AMERICAN EXPRESS [redacted]

Log Out
Traveler: Danielle St Louis
Site gocenglish

- Home
- Trips
- Templates

Help with this page

Your trip so far...
Tue, 24 Jan 2012 - Thu, 02 Feb 2012

Estimated Cost from Travel Access V04978 1242.98

View details

Flight Details

Tue, 24 Jan	**09:20 - 14:30**	Sydney, New South Wales (SYD) to Wellington (WLG) Non-stop	Air New Zealand Flight 845 Seat not assigned Class: Economy Économique
Fri, 27 Jan	**15:25 - 17:05**	Wellington (WLG) to Sydney, New South Wales (SYD) Non-stop	Qantas Airways Operated by Jetconnect For Qantas Flight 48 Seat not assigned Class: Economy Économique
	18:40 - 19:30	Sydney, New South Wales (SYD) to Canberra, Australian Capital Territory (CBR) Non-stop	Qantas Airways Operated by Qantaslink - Eastern Australia A/L Flight 1491 Seat not assigned Class: Economy Économique
Wed, 01 Feb	**08:45 - 09:25**	Canberra, Australian Capital Territory (CBR) to Brisbane, Queensland (BNE) Non-stop	Virgin Blue Flight 1211 Seat not assigned Class: Economy Économique
Thu, 02 Feb	**18:25 - 21:00**	Brisbane, Queensland (BNE) to Sydney, New South Wales (SYD) Non-stop	Qantas Airways Flight 553 Seat not assigned Class: Economy Économique

Flight Total: Airfare unavailable

Hotel Details

Car Details

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Reserve Seats for Flight 2 of 5

Wellington (WLG) to Sydney (SYD): Fri, 27 Jan

Company Announcements
Seat requests are subject to change by the airline prior to departure.
Remember to select an **Airline Seating Preference** in your Traveller Profile.

We cannot price your flights at this time.
You may continue and purchase your trip; however, we cannot provide the price of your flights. To start your search over click the Home link. If you have any questions, please contact your travel administrator. **[Reservation system internal error - cannot price this itinerary, please try a different flight.]**

To select a seat, click on a seat in the airplane diagram and then click the "Reserve Seats" button.

[redacted]
Flight: 48
Aircraft: TBA
Booking Class: Classe économique
Remaining Seats: 66%

Passenger	Seat	Seats Selected	Legend	
			1	Your Seat
			A	Available Seat
			T	Seat Taken
			P	Premium Seat (Fee)
			P	Premium Seat (for qualifying Frequent Travelers)
			E	Exit Row Seat (must be reserved at airport)
				Seat Unavailable

Skip Seat Selection Reserve Seat Selection

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE / Autorisation de voyager et avance

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

☑ Original / Prem. demande

☐ Amended (Same levels of approval as original dated) / Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

Part A - Partie A

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No. - N° du document
Type 2	Name of traveller - Nom du voyageur: Robert Pilcher	Classification: CS-03

Department - Ministère: Public Safety Canada	Branch / Division / Group - Direction / Division / Groupe: EMMS / Canadian Cyber Incident Response
Address - Adresse: 340 Laurier Ave	Telephone No. - No. de téléphone: 613-949-8318
Branch Contact - Personne ressource à la direction: Jane Hayward	Telephone No. - No. de téléphone: 613-991-1982
Purpose of travel - Objet du voyage: Semi-Annual Usual 5 Meeting to Dicuss Cyber Incident Response and CERT Meetings	No. of days / Nbre de jours: 15

If different address, send cheque to: / Si adresse différente, envoyer chèque à

Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)? ☑ Yes / Oui ☐ No / Non

If no, would you like to request one? / Si non, désirez-vous en avoir une? ☐ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Départ / Arrival - Arrivée	Transportation Transport: Mode	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de repérage du dossier
January 26, 2012	Ottawa	Sydney	17:05 - 10:30 (22)	Air	2	TBD	
January 26, 2012	Sydney	Wellington, NZ	09:30 - 14:30	Air		TBD	
January 27, 2012	Wellington, NZ	Canberra	15:25 - 19:30	Air		TBD	
February 1, 2012	Canberra	Brisbane	08:45 - 09:25	Air		TBD	
February 3, 2012	Brisbane	Ottawa	06:30 - 16:34	Air	2	TBD	

Part C - Expenses and Allowances / Partie C - Dépenses et allocations

Standard / Générales: Item / Type de dépense	Estimated cost / Coût estimatif	Non-standard / Spéciales: Item / Type de dépense	Estimated cost / Coût estimatif
Accommodation (white page hotel) / Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$2,898.00	Accommodation (green page hotel) / Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory) / Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) / Location d'une voiture non intermédiaire (assurance-collision du répertoire obligatoire)	$0.00
Private vehicle requested by: / Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur	$0.00	Other (Specify) - Autre (préciser)	
Public Liability and Property Damage min $1 million. Deductibles NON reimbursable / Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NE SONT PAS remboursables.		Upgrade transportation (specify in "Class" above) / Transport à tarif supérieur (préciser la «classe» ci-dessus)	$0.00
Transportation / Transport	$1,049.00		
Meals and Incidentals / Repas et frais accessoires	$1,911.00		
Other (Specify) - Autre (préciser)	$225.00		

☐ First class (Deputy Head or equivalent approval) / Prem. Classe (approuvée par le sou-chef ou l'équiv.)

☐ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) / Classe d'affaires - ou autre classe à tarif supérieur (approuvée par le sou-chef ou l'équiv., s'il s'agit d'une classe non prévue à l'article 3.1.9)

Lynda Clairmont

Approval - Approbation

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel.

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$7,147.80
Other - Autre	$4,981.13
Trip Total - Coût total du voyage	$12,128.13
Funding - Financement	
A) Travellers cheques / Chèques de voyage	
Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
Cheque / Chèque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques internes pour les employeurs distincts) et en accepte les conditions.

Robert Pilcher — Signature — Dec 24/2011 — Date

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature): Lynda Clairmont — Date

Approved by (signature) - Approuvé par (signature): William V. Baker — Date

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type 8 | 0	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier Indicator / Indicateur du fournisseur | 0	Due Date / Date d'échéance

Type 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Clalification	Amount - Montant
			128 9109 / 2001 PSABASE 476 50009109	

Description

Financial encumbrance No. / No. de consignation de fonds: 50009109

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)

Verified correct (PWGSC) (signature) / Vérifié conforme (TPSGC) (signature)

Services officer (PWGSC) (signature) / Agent responsable (TPSGC) (signature)

Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.

Signature

Cheque No. - N° du chèque

Date

000045

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé

	Amount/Montant
Airfare / Frais d'avion	$7,147.00
Train / Train	$0.00
Other / Autres	$0.00
	$7,147.00

Estimated Cost - Coût estimatif: Other - Autre

	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (WHITE page hotel) / Hébergement (un des hôtels figurent dans la partie BLANCHE du répertoire)	$175.00	12	$2,100.00
Accomodation (GREEN page hotel) / Hébergement (un des hôtels figurent dans la partie VERT du répertoire)	$0.00	0	$0.00
			$2,100.00
Mid-size car rental / Location d'une voiture intermédiaire	$0.00	0	$0.00
NON Mid-size car rental / Location d'une voiture NON intermédiaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.570	0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Taxis / stationnement et frais de péage				$0.00
Taxi/Limo	Home to Airport (Train Station)		$50.00	$500.00
	Airport (Train Station) - Hotel / Meetings		$100.00	
	Hotel - Airport (Train Station)		$100.00	
	Airport (Train Station) to Home		$50.00	
	Meeting - Meetings		$200.00	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$500.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$20.33	13	$264.29
Lunch / Déjeuners	$44.32	13	$576.20
Dinner / Dîners	$56.48	13	$734.24
Incidentals /Frais divers	$98.76	15	$581.40
			$2,156.13

Business Phone / Téléphone d'affaires	
Airport Improvement Fee / Frais de l'Aeroport	$25.00
Cash Advance Fee / Frais d'avances	$0.00
Misc. Business Services / Diverses charges d'affaires	$0.00
Miscellaneous / Diverses Internet and service charges	$0.00
	$200.00
	$225.00

Public Safety Canada / Sécurité publique Canada

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RDIMS: 525670

Commitment Authority (Section 32 FAA) Checklist

(version francaise est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	**Questions**
☑	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?

☑ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☐ Request to Attend Conferences Form	☐ Training Application and Authorization Form	☐ Membership Approval Form	☐ Other Specify:

☑	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?
☐	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR? money's reserved
N/A	Have I completed all the paperwork requested by the Contracting Material Management group? ☐ Is the Sole Source Checklist complete and attached? ☐ Is the Competitive Contract Checklist complete and attached?
✓ ✓	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☐ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☐ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.
N/A	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☐ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☐ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*

Purchase Requisition #	**Purchase Order #**	**Funds Commitment #:**	**RDIMS #**
[redacted]	[redacted]	[redacted]0009109	[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Added 50% of estimated cost for TAA purposes QS.

St-Louis, Danielle

Subject: Emailing: Itinerary, Price and Alternatives

Robert Pitcher, Flying Economy

Skip to page content

Travel AcXess Voyage

[redacted] AMERICAN EXPRESS® BUSINESS TRAVEL

Log Out
Traveler: Danielle St Louis
Site gocenglish

- Home
- Trips
- Templates

Help with this page

Your trip so far...
Fri, 20 Jan 2012 - Fri, 03 Feb 2012

▼view details

Flight Details			
Fri, 20 Jan	**17:35 - 20:00**	Ottawa, Ontario (YOW) to Vancouver, British Columbia (YVR) Non-stop	**AIR CANADA** Air Canada Flight 189 Seat not assigned Class: Economy Économique
The departure and arrival dates are different.			
	23:45 - 10:20 Arrives Sun, 22 Jan	Vancouver, British Columbia (YVR) to Sydney, New South Wales (SYD) Non-stop	**AIR CANADA** Air Canada Flight 33 Seat not assigned Class: Economy Économique
Fri, 03 Feb	**12:15 - 07:25**	Sydney, New South Wales (SYD) to Vancouver, British Columbia (YVR) Non-stop	**AIR CANADA** Air Canada Flight 34 Seat not assigned Class: Economy Économique
	08:50 - 16:24	Vancouver, British Columbia (YVR) to Ottawa, Ontario (YOW) Non-stop	**AIR CANADA** Air Canada Flight 166 Seat not assigned Class: Economy Économique

Flight Total: Can$3,523.88

Hotel Details

Car Details

Itinerary, Price and Alternatives
Ottawa (YOW) to Sydney (SYD): Fri, 20 Jan 2012
Sydney (SYD) to Ottawa (YOW): Fri, 03 Feb 2012
Skip over modify search
►Modify search
▼Modify search

* = Required

(X) **Shop by Schedule**

000048

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

St-Louis, Danielle

Subject: Emailing: Reserve Seats for Flight 2 of 5

Add 60% Due to TAA purposes.

Skip to page content

Travel AcXess Voyage

[redacted] AMERICAN EXPRESS BUSINESS TRAVEL

Log Out
Traveler: Danielle St Louis
Site gocenglish

[redacted]
Home
Trips
Templates

Help with this page

Your trip so far...
Tue, 24 Jan 2012 - Thu, 02 Feb 2012

Estimated Cost from Travel Access Voyage 1242.98

View details

Flight Details			
Tue, 24 Jan	**09:20 - 14:30**	Sydney, New South Wales (SYD) to Wellington (WLG) Non-stop	Air New Zealand Flight 846 Seat not assigned Class: Economy Économique
Fri, 27 Jan	**15:25 - 17:05**	Wellington (WLG) to Sydney, New South Wales (SYD) Non-stop	Qantas Airways Operated by Jetconnect For Qantas Flight 48 Seat not assigned Class: Economy Économique
	18:40 - 19:30	Sydney, New South Wales (SYD) to Canberra, Australian Capital Territory (CBR) Non-stop	Qantas Airways Operated by Qantaslink - Eastern Australia A/L Flight 1491 Seat not assigned Class: Economy Économique
Wed, 01 Feb	**08:45 - 09:25**	Canberra, Australian Capital Territory (CBR) to Brisbane, Queensland (BNE) Non-stop	Virgin Blue Flight 1211 Seat not assigned Class: Economy Économique
Thu, 02 Feb	**18:25 - 21:00**	Brisbane, Queensland (BNE) to Sydney, New South Wales (SYD) Non-stop	Qantas Airways Flight 553 Seat not assigned Class: Economy Économique

Flight Total: Airfare unavailable

Hotel Details

Car Details

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Reserve Seats for Flight 2 of 5

Wellington (WLG) to Sydney (SYD): Fri, 27 Jan

Company Announcements

Seat requests are subject to change by the airline prior to departure.

Remember to select an **Airline Seating Preference** in your Traveller Profile.

We cannot price your flights at this time.

You may continue and purchase your trip; however, we cannot provide the price of your flights. To start your search over click the Home link. If you have any questions, please contact your travel administrator. **[Reservation system internal error - cannot price this itinerary, please try a different flight.]**

To select a seat, click on a seat in the airplane diagram and then click the "Reserve Seats" button.

Flight: 48
Aircraft: TBA
Booking Class: Classe économique
Remaining Seats: 66%

Passenger	Seat	Seats Selected

Legend	
1	Your Seat
A	Available Seat
T	Seat Taken
F	Premium Seat (Fee)
P	Premium Seat (for qualifying Frequent Travelers)
E	Exit Row Seat (must be reserved at airport)
	Seat Unavailable

Skip Seat Selection Reserve Seat Selection

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

HOLIDAYCITY

Stay Details

Date of Arrival :4 Dec 2011
Date of Departure :9 Dec 2011
No of unit(s) :1
No of Adult(s) :2
No of Child :0
Age of Child :N/A

[redacted]
Wellington Hotels

[redacted]
My Account

Chat with our Customer Service Officer

Currency Converter

Page 1 | Next Page >

Rydges Wellington POPULAR ☆☆☆☆

(Formerly 'Holiday Inn Wellington') 75 Featherston Street 6000 Wellington Location Map

The new Rydges Wellington, formerly Holiday Inn Wellington is centrally located downtown on Featherston Street with a spectacular harbour outlook, close to Custom Quay, Westpac Stadium, Victoria University and Wellington Railway Station.

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 126.65	Available	Show All Room Types

Hotel Ibis Wellington POPULAR ☆☆☆

153 Featherston Street 6001 Wellington Location Map

Ibis Wellington is centrally located just minutes from Lambton Quay shopping, Te Papa Museum, Westpac Stadium and other Wellington attractions. Easily accessible by bus, train and taxi, and with the famous Wellington cafe scene right at its doorstep, the Ibis is...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 129	Available	Show All Room Types

James Cook Hotel Grand Chancellor Wellington POPULAR ☆☆☆☆

147 The Terrace, PO Box 2429, Wellington Location Map

At the heart of Wellington's commercial and retail districts the James Cook Hotel Grand Chancellor has 260 well appointed rooms and suites, two restaurants and bars. Guests can enjoy James Cook Hotel Grand Chancellor recently refurbished terrace wing and will notice...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 150	Available	Show All Room Types

SilverOaks Hotel On Thorndon Wellington POPULAR ☆☆

20 Glenmore Street, 6005 Wellington Location Map

SilverOaks Hotel On Thorndon Wellington is located in historic Thorndon, walking distance to many government and parliament buildings. This Wellington hotel provides easy access to the New Zealand National Maritime Museum, Wellington Botanic Garden, Old Saint Paul's Cathedral and Katherine Mansfield...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 65.8	Available	Show All Room Types

Mercure Wellington Willis Street POPULAR ☆☆☆

355 Willis Street, 6001 Wellington Location Map

Mercure Willis Street Wellington is located in the Cuba quarter of Wellington offering comfort, convenience and all the amenities you would expect from a 3.5 star hotel. The hotel is a short walk to all of Wellington's iconic attractions plus the...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 99	Available	Show All Room Types

InterContinental Wellington POPULAR ☆☆☆☆☆

Featherston & Grey Streets 60000 Wellington Location Map

InterContinental Wellington is conveniently located in the heart of the capital's vibrant business and shopping district. It is the perfect base whether you are staying for business or pleasure. InterContinental Wellington has 232 guest rooms and suites and is a 100...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 246	Available	Show All Room Types

Kingsgate Hotel Wellington POPULAR ☆☆☆

24 Hawkestone Street, Wellington Location Map

The Kingsgate Hotel Wellington is located in New Zealand's oldest and historic suburb, Thorndon, 500 meters north of Wellington's city centre. Close to the bus, train, and ferry terminals, Parliament buildings, Botanical Gardens and has easy motorway access. The Kingsgate Hotel...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 129	Available	Show All Room Types

Amora Hotel Wellington POPULAR ☆☆☆☆½

170 Wakefield Street, 6011 Wellington Location Map

Amora Hotel Wellington, a fabulous, downtown hotel has just completed a total accommodation makeover redefining superior comfort and luxury with contemporary style in the Capital City. Most rooms command unobstructed views of Wellington Harbour and/or the city and we're located right...

Room Type	Average Rate	Availability	Max_Occupancy	Option
Deluxe Room	NZD 175.00	Available	2	Book Now
Club Room - Non Refundable - Breakfast included	NZD 237.00	Available	2	Book Now
Club Room - Breakfast included	NZD 245.00	Available	2	Book Now
Club Suite - Breakfast included	NZD 315.00	Available	2	Book Now

Hotel Novotel Wellington POPULAR ☆☆☆☆

133-137 The Terrace, 6001 Wellington Location Map

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The Novotel Wellington hotel is conveniently located in the heart of the city, close to the Te Papa Museum, Convention Centre, Parliament, Westpac Stadium and the waterfront as well as the many other attractions of the city. The hotel has direct...

Check Rates and Availability *From NZD 139

Comfort Hotel Wellington (POPULAR) ☆☆☆

213 Cuba Street, Dunlop Terrace, 6001 Wellington Location Map

Located in the heart of the city, the Comfort Hotel Wellington is perfectly situated for visiting the capital city. This Wellington hotel provides easy access to many popular attractions, including the Wellington Botanic Garden, Wellington Zoo, Westpac Stadium and Karori Wildlife...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 88.4	Available	Show All Room Types

Trinity Hotel Wellington ☆☆☆½

166 Willis Street, 6001 Wellington Location Map

Trinity Hotel Wellington was formerly the Just Hotel which was purchased by the Trinity Group in January 2008. Trinity Group consists of 19 hospitality and accommodation operations throughout the Wellington, Palmerston North and Hawkes Bay regions.

Trinity Hotel Wellington is a popular...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 80.1	Available	Show All Room Types

Copthorne Hotel Wellington Oriental Bay ☆☆☆☆

(Formerly "Kingsgate Hotel Oriental Bay Wellington"), 73 Roxburgh Street, 9555 Wellington Location Map

Nestled beneath the rolling hills, the Copthorne Wellington is located on Wellington's premier street address of Oriental Parade, and many of the rooms overlook Wellington's spectacular inner harbour. With it's prime position overlooking one of the most beautiful harbours in the...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 172	Available	Show All Room Types

Bay Plaza Hotel Wellington ☆☆☆

40-44 Oriental Parade, 6141 Wellington Location Map

Located on Wellington's exclusive Oriental Parade, the Bay Plaza Hotel Wellington is affordable quality accommodation offering harbour and city views in perfect proximity to the capitals vibrant city centre and superb leisure activities to experience and explore.

The Bay Plaza Hotel Wellington...

Room Type	Average Rate	Availability	Option
Lowest Room Rate from	NZD 99	Available	Show All Room Types

Mercure Wellington ☆☆☆

345 The Terrace, 6001 Wellington Location Map

Mercure Hotel Wellington enjoys a prime location at the top of the Terrace with spectacular views over the city and harbour. This hotel is an easy walk to the Cuba Quarter, funky boutiques, shops and famous Wellington attractions such as Te...

Check Rates and Availability *From NZD 82

The Wellesley Club And Boutique Hote l Wellington ☆☆☆½

2/8 Maginnity Street, Central Business District, Wellington Location Map

The Wellesley Hotel Wellington is superbly located in the heart of Wellington's Central Business District, only a few steps from Parliament and shopping's "Golden Mile", Lambton Quay. The charm and elegance of The Wellesley Hotel Wellington's splendid interior with its fine...

Room Type	Average Rate	Availability	Max_Occupancy	Option
Premium Room	NZD 219.00	Available	2	Book Now
Executive Room	NZD 235.00	Available	2	Book Now
Luxury Room	NZD 275.00	Available	2	Book Now

* Rates are an indicative only. For actual rates, please click Rates and Availability for more details.

Amend Stay Details

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
Meetings with CERT Australia on Cyber Security Issues and Usual 5 Semi-Annual Meeting	From - *Du* : January 20, 2012	To - *Au* : February 3, 2012
Location (City, Country) - *Lieu (Ville, Pays)* Canberra and Brisbane, Australia Wellington, New Zealand	Estimated total cost - *Coût total prévu* $38,559.26	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)* Agenda attached	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?* ☒Yes/Oui ☐No/Non	

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Windy Anderson Robert Pitcher	NS - NCSD CCIRC	257 Slater Street	613 991-7055 613-949-8318

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

Visit to CERT Australia facilities aimed at establishing strong operational relationships between our national CERTs and exchanging on current tools, processes and recently handled cyber security incidents of common interest such as the DNSChanger case.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

This visit will provide applicable lessons learned from a partner CERT facing similar resources and environment challenges. This will in turn provide opportunities to leverage mutual expertise and improve regular operational collaboration between CCIRC and CERT Australia.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

Windy Anderson, NCSD-CCIRC Director

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

Consultation is ongoing within Public Safety and our collective knowledge is shared throughout government through our ability to respond to cyber incidents.

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

R. Dixon — Name of participant's Director General
Nom du Directeur Générale du voyageur

Dec 28/11 — Date

Reviewed by/
Examiné par :

for/ — Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

30/12/11 — Date

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Approved by/
***Approuvé par*:**

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Date

PS023

Int'l Travel Request
W. Anderson & R. Pitcher (NCSD)
to Australia and New Zealand
Jan. 27-Feb. 3, 2012
Docket # 382805

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Australia - Currency: Australian Dollar (AUD)

Type of Accommodation	City	Meal Rate				Incidental Amount	Grand Total (Taxes Included)
		Breakfast	Lunch	Dinner	Meal Total		
C	Adelaide	27.45	37.40	52.20	117.05	37.46	154.51
C-75%	Adelaide	20.59	28.05	39.15	87.79	28.09	115.88
P	Adelaide	27.45	37.40	52.20	117.05	23.41	140.46
P-75%	Adelaide	20.59	28.05	39.15	87.79	17.56	105.35
C	Brisbane	24.70	49.90	63.65	138.25	44.24	182.49
C-75%	Brisbane	18.53	37.43	47.74	103.69	33.18	136.87
P	Brisbane	24.70	49.90	63.65	138.25	27.65	165.90
P-75%	Brisbane	18.53	37.43	47.74	103.69	20.74	124.43
C	Canberra	24.10	42.70	59.85	126.65	40.53	167.18
C-75%	Canberra	18.08	32.03	44.89	94.99	30.40	125.38
P	Canberra	24.10	42.70	59.85	126.65	25.33	151.98
P-75%	Canberra	18.08	32.03	44.89	94.99	19.00	113.99
C	Hobart	19.55	43.15	59.40	122.10	39.07	161.17
C-75%	Hobart	14.66	32.36	44.55	91.58	29.30	120.88
P	Hobart	19.55	43.15	59.40	122.10	24.42	146.52
P-75%	Hobart	14.66	32.36	44.55	91.58	18.32	109.89
C	Melbourne	27.20	43.75	63.95	134.90	43.17	178.07
C-75%	Melbourne	20.40	32.81	47.96	101.18	32.38	133.55
P	Melbourne	27.20	43.75	63.95	134.90	26.98	161.88
P-75%	Melbourne	20.40	32.81	47.96	101.18	20.24	121.41
C	Perth	27.05	45.25	63.10	135.40	43.33	178.73
C-75%	Perth	20.29	33.94	47.33	101.55	32.50	134.05
P	Perth	27.05	45.25	63.10	135.40	27.08	162.48
P-75%	Perth	20.29	33.94	47.33	101.55	20.31	121.86
C	Sydney	28.65	53.15	65.75	147.55	47.22	194.77
C-75%	Sydney	21.49	39.86	49.31	110.66	35.41	146.07
P	Sydney	28.65	53.15	65.75	147.55	29.51	177.06
P-75%	Sydney	21.49	39.86	49.31	110.66	22.13	132.80
C	Other	19.28	34.16	47.88	101.32	32.42	133.74
C-75%	Other	14.46	25.62	35.91	75.99	24.32	100.31
P	Other	19.28	34.16	47.88	101.32	20.26	121.58
P-75%	Other	14.46	25.62	35.91	75.99	15.20	91.19

Daily currency converter

Convert to and from Canadian dollars, using the latest noon rates.

Currency Converter

Amount: 1.00 **cash rate:**

From: ~~Canadian Dollar~~ New Zeal

To: ~~U.S. dollar~~ Cdn

>

Convert

Answer: 0.79

Exchange Rate: 0.7873

Summary: On December 29, 2011, 1.00 New Zealand dollar(s) = 0.79 Canadian Dollar(s), at an exchange rate of 0.7873 (using nominal rate).

Daily currency converter

Convert to and from Canadian dollars, using the latest noon rates.

Currency Converter

Amount: 1.00 cash rate: ☑

From: ~~Canadian Dollar~~ Aust.

To: ~~U.S. dollar~~ Cdn

Convert

Answer: 1.03

Exchange Rate: 1.0347

Summary: On December 29, 2011, 1.00 Australian dollar(s) = 1.03 Canadian Dollar(s), at an exchange rate of 1.0347 (using nominal rate).

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

New Zealand - Currency: New Zealand Dollar (NZD)

Type of Accommodation	City	Meal Rate				Incidental Amount	Grand Total (Taxes Included)
		Breakfast	Lunch	Dinner	Meal Total		
C	Auckland	31.60	56.10	70.20	157.90	50.53	208.43
C-75%	Auckland	23.70	42.08	52.65	118.43	37.90	156.32
P	Auckland	31.60	56.10	70.20	157.90	31.58	189.48
P-75%	Auckland	23.70	42.08	52.65	118.43	23.69	142.11
C	Wellington	25.50	55.60	70.85	151.95	48.62	200.57
C-75%	Wellington	19.13	41.70	53.14	113.96	36.47	150.43
P	Wellington	25.50	55.60	70.85	151.95	30.39	182.34
P-75%	Wellington	19.13	41.70	53.14	113.96	22.79	136.76
C	Other	20.40	44.48	56.68	121.56	38.90	160.46
C-75%	Other	15.30	33.36	42.51	91.17	29.17	120.34
P	Other	20.40	44.48	56.68	121.56	24.31	145.87
P-75%	Other	15.30	33.36	42.51	91.17	18.23	109.40

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada / Sécurité publique Canada

EMNS
Branch / Direction générale
NCSD

Routing Slip / Bordereau d'acheminement

File No / No de dossier : _382805_

Deadline for DM's signature / Échéancier pour la signature du S-M : _____

Title / Titre : MEMORANDUM TO THE DEPUTY MINITER – International Travel Authorization for Windy Anderson and Robert Pitcher: usual 5 Semi-Annual Meeting, Wellington, New Zealand, January 2o to February 3			**ACTION REQUIRED / MESURES À PRENDRE**	
Name / Nom	**Date**	**Initials / Initiales**	**Approval or signature / Approbation ou signature**	**Information**
Director General / Directeur général intérimaire **Robert Dick - NCSD**	Dec 29/11	RD	☒	☐
Director General International Affairs / Directrice générale des affaires internatineaux **Barbara Motzney** for	30/12/11	GM	☒	☐
Senior Assistant Deputy Minister EMNS / Sous-ministre adjointe principale GMUSN **Lynda Clairmont**			☒	☐
Assistant Deputy Minister CM / Sous-ministre adjointe GM **Gary Robertson**			☐	☒
Deputy Minister / Sous-ministre **William V. Baker**			☒	☐

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

UNCLASSIFIED

DATE:

File No.: 385262
RDIMS No.: 550276

MEMORANDUM FOR THE DEPUTY MINISTER

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEBSITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) websites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, 2012, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of Friday, January 20, 2012, most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these websites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Gregg Murphy

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

UNCLASSIFIED

DATE:

File No. :
RDIMS No.:

MEMORANDUM FOR THE DEPUTY MINISTER

INTERNATIONAL TRAVEL AUTHORIZATION
FOR WINDY ANDERSON TO TRAVEL TO
BUDAPEST, HUNGARY - APRIL17 TO APRIL18, 2012
(Signature required)

ISSUE

Your approval is sought for an international travel request for Mrs. Windy Anderson, Director CCIRC, to attend the International Watch and Warning Network (IWWN) conference in Budapest, Hungary, from April 17 to April 18, 2012.

BACKGROUND

The IWWN was established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities. The conference helps establish a clear path forward for the IWWN community to enhance global cyber situational awareness and incident response capabilities. Participating countries include: Australia, Canada, Finland, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States.

CONSIDERATIONS

The conference, hosted by CERT Hungary, brings together delegations from 15 countries to foster international collaboration on cyber watch, warning, and incident response, and identify mechanisms to further information sharing about critical infrastructure protection efforts. Country delegations include government cyber security policy makers, managers of computer security incident response teams ("CERTs"), and law enforcement representatives responsible for cyber-crime matters.

CCIRC involvement in these conferences is essential in ensuring CCIRC fulfills its mandate as Canada's National CERT. CCIRC maintains four types of relationships, those formally structured as with other governments, those of less formal but still of a structured nature such as with U5 CERTs, informal and unstructured relationships with trusted partners such as telecommunications providers and security researchers and, finally, those that are

.../2

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

informal and unstructured such as those with other national CERTs. Each relationship is important in its own way, however, the partnerships between national CERTs are critical in the exchange of Cyber defence information. These relationships are based on mutual trust and are greatly enhanced through the personal interactions of IWWN members. The opportunities for "face-to-face" meetings with a large group of peer international partners are both rare and essential.

The estimated cost of this trip is $4800.00. This estimate provides for a possible increase in airfare during the approval process. There is no conference fee for this event. The trip is forecasted in the National Cyber Security Directorate's travel cap plan.

RECOMMENDATION

It is recommended that you approve this travel request to Budapest, Hungary by signing the Travel Authority and Advance forms. My approval of this trip is noted in the International Travel Request.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures:

I approve:

_____
William V. Baker

Prepared by: Windy Anderson

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
International Watch and Warning Network	From - *Du* :	To - *Au* :
	April 17, 2012	April 18, 2012
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
Budapest, Hungary	$3,000.00	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?*	
The IWWN was established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities. The conference helps establish a clear path forward for the IWWN community to enhance global cyber situational awareness and incident response capabilities. Participating countries include: Australia, Canada, Finland, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States	☐ Yes/Oui	☒ No/Non

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Windy Anderson	NCSD	257 Slater Street 4th Floor	613-991-7055

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

This conference, hosted by CERT Hungary, brings together delegations from these 15 countries to foster international collaboration on cyber watch, warning, and incident response, and identify mechanisms to further information sharing about critical infrastructure protection efforts.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

This conference has a narrow scope - how to promote information sharing and foster internation collaboration on addressing cyber threats, attacks, and vulnerabilities. It will focuss on promoting improved security amongst the 15 countries listed above. The results of this conference will only improve CCIRC's ability to achieve its mandate. That, in turn, will directly aid in achieving Public Safety's first three priorities.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

None

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

NCSD, CSEC, U5 Partners

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travellers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

Name of participant's Director General
Nom du Directeur Générale du voyageur

Date

Reviewed by/
Examiné par :

Director General, International Affairs Directorate

Date

RDIMS / SGDDI # 462130

000066

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Directeur Générale, Direction générale des affaires internationales

Approved by/
Approuvé par :

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Date

PS023

Public Safety Canada / Sécurité publique Canada

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: February 27, 2012

To – A

Lynda Clairmont
Senior Assistant Deputy Minister
EMNS

Requested by – Demandé par

Windy Anderson,
Director CCIRC

Name of Conference – Titre de la conférence

International Watch and Warning Network (IWWM) Conference

Type of Conference – Genre de conférence

☒ International / Internationale ☐ National / Nationale ☐

Documents attached / Documentation jointe

☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur

CERT Hungary

Official Host – Hôte officiel

Hungary

Duration of Conference – Durée de la conférence

From / Du: 17 April To / À: 18 April

Location - Adresse

Budapest, Hungary

Agenda – Ordre du jour

The agenda for this year's conference has yet to be released. Based on last year's agenda, activities focus on enhancing the capabilities and collaboration of member CSIRTs. Working groups are established to develop Standard Operating Procedures (SOP) and Cyber exercises.

Purpose of Participation - Object de la participation

The IWWN was established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities. The conference helps establish a clear path forward for the IWWN community to enhance global cyber situational awareness and incident response capabilities. Participating countries include: Australia, Canada, Finland, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States. This conference, hosted by CERT Hungary, brings together delegations from these 15 countries to foster international collaboration on cyber watch, warning, and incident response, and identify mechanisms to further information sharing about critical infrastructure protection efforts. The opportunities for "face-to-face" meetings with a large group of international partners are both rare and essential.

The conference attendance is by invitation only and is free

Financial Coding – Code financier

223

Estimated Total Cost / Coût total prévu

$ 3,000.00

Recommended by – Recommandé par		Branch Approval – Approbation de la direction	
Signature	Date	Signature	Date
Assistant Deputy Minister – Sous-ministre adjoint		**Deputy Minister – Sous-ministre**	
Signature	Date	Signature	Date

MS-18 (4/04)

000068

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

UNCLASSIFIED

DATE:

File No.: NS 3010-386828
RDIMS No.: 590947

MEMORANDUM FOR THE DEPUTY MINISTER

CANADIAN CYBER INCIDENT RESPONSE CENTRE'S MANDATE

(Signature required)

ISSUE

Your approval is sought to finalize the Canadian Cyber Incident Response Centre's (CCIRC) mandate (**Tab A**), to communicate it to partners, and to use it as the basis to develop operational procedures.

BACKGROUND

Created in 2005 and housed within Public Safety Canada's National Cyber Security Directorate, CCIRC is Canada's national Computer Emergency Readiness Team (CERT). As you may know, CCIRC has received new resources as part of *Canada's Cyber Security Strategy* and the recently approved Treasury Board Submission on *Strengthening the Security of Federal Cyber Systems*. You should be aware of two issues: the need to align CCIRC's activities; and, CCIRC's new roles and responsibilities.

CCIRC's authority has been based on the Minister's roles under the *Department of Public Safety and Emergency Preparedness Act* and the *Emergency Management Act*. However, this directive is too broad and the proposed mandate will help CCIRC focus its activities, put in place more rigorous procedures, and create measurable deliverables. Going forward, the centre plans to anchor its work in three streams: national security, public safety, and economic prosperity.

CCIRC has also recently transitioned its area of responsibility from Government of Canada networks to critical infrastructure sectors outside the federal government (e.g. provinces, finance, energy and utilities, etc.). Moreover, CCIRC has recently moved from the Government Operations Centre to the National Cyber Security Directorate. As result of these changes, it has been identified that the centre needs an anchor to help achieve its objectives. As such, we are seeking your approval for a CCIRC specific mandate.

.../2

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

CONSIDERATIONS

Effectiveness and visibility are two of the main considerations regarding this directive.

CCIRC is in the process of repositioning itself to provide better services to Canada's critical infrastructure sectors. The proposed CCIRC specific mandate will allow us to develop operational procedures and products towards this aim. This in turn will help us achieve tangible deliverables in support of Public Safety's strategic outcome.

In addition, this specific directive clearly defines CCIRC as both Canada's CERT and Canada's national cyber coordination centre. This will enhance our visibility with other government departments, critical infrastructure partners, and international allies. Furthermore, this will strengthen our education and engagement processes with key stakeholders.

NEXT STEPS

You will find one document attached for your review, comment, and approval.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure: (1)

I approve:

_____
William V. Baker

Prepared by: Nate Klassen

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

CCIRC'S MANDATE:

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention, mitigation, and response to cyber events.

CCIRC provides authoritative advice to, and coordinates information sharing and event response among, all levels of government, international counterparts, critical infrastructure operators and information technology vendors.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

UNCLASSIFIED

DATE:

File No.: 387395
RDIMS No.: 572234

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

INTERNATIONAL TRAVEL AUTHORIZATIONFOR WINDY ANDERSON AND LUC BEAUDOIN TO TRAVEL TO MALTA JUNE 16-25, 2012

(Signature required)

ISSUE

Your approval is sought for an international travel request for Mrs. Windy Anderson and Mr. Luc Beaudoin to attend the Forum for Incident Response and Security Teams (FIRST) and the Computer Security Incident Response Team (CSIRT) conference in Malta, June 16-22, 2012.

BACKGROUND

The Canadian Cyber Incident Response Centre (CCIRC) is a member of the FIRST community. FIRST conferences are designed to promote FIRST organization goals of worldwide coordination and cooperation. It serves as the foundation for the improvement of computer security worldwide by sharing goals, ideas, and information. It provides a prime opportunity for those in the operating system, computer security and networking and telecommunications industries to gain focused access to a highly influential group of computer security incident response experts from around the world. Conference attendees commonly provide computer security advice within their own CSIRTs and suggest security strategies, provide technical solutions to security problems and deliver security education and training to their constituents.

CONSIDERATIONS

FIRST is the world's largest organization of recognized CSIRTs. Members comprise the vast majority of international interactions that CCIRC undertakes at the tactical and operational levels. Attendance is essential to ensure CCIRC is aware of and has its views heard with respect to information sharing protocols, special capabilities possessed by other CSIRTs and problems, trends and best practices. Meetings of this kind are also essential to establish and maintain points of contact and relationships with group members.

.../2

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

At the last Usual 5 (U5) Conference (United States, United Kingdom, New Zealand, Australia and Canada), all international travel to upcoming events was discussed in detail. It was noted that all five countries are strongly encouraged to have representatives at both the U5 Conferences and the FIRST Conference as these are the two most important venues for our forum. For all other conferences/trips, it was agreed that those countries participating would share their trip reports on the U5 Portal; thus saving money and resources for those countries unable to participate.

The justification for sending two representatives to this event is due to the number of sessions and parallel forums of relevance to CCIRC operations and where appropriate representation would be beneficial in order to build trust relationships. As a result, CCIRC director will be engaged in the CERT strategic and policy related discussions while the operations manager will participate in technical sessions, as seen in the conference agenda **(Tab D)**.

The estimated cost of this trip is $11,960.88 per person. While this estimate provides for a possible increase in airfare during the approval process, Mrs. Anderson and Mr. Beaudoin will be flying economy class and therefore, the actual trip cost is expected to be substantially less. The trip is forecasted in National Cyber Security's travel cap plan.

RECOMMENDATION

It is recommended that you approve Mrs. Anderson's and Mr. Beaudoin's travel to Malta to attend the FIRST conference and CSIRTs meeting, June 16-25, 2012 by signing the Travel Authority and Advance form **(Tab A)** and the Conference Request form **(Tab B)**. The approvals of this trip are noted in the International Travel Request **(Tab C)**.

Should you require additional information, please do not hesitate to contact me at 990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (4)

I approve:

_____

Graham Flack
Acting Deputy Minister

Prepared by: Windy Anderson

Public Safety Canada / Sécurité publique Canada

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: February 29, 2012

To – A
Deputy Minister,
Public Safety

Requested by – Demandé par
Windy Anderson,
Director CCIRC

Name of Conference – Titre de la conférence
24th Annual FIRST Conference and CSIRT

Type of Conference – Genre de conférence
☒ International / Internationale ☐ National / Nationale ☐

Documents attached / Documentation jointe
☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur
Microsoft, Cisco, European Network and Info Security Agency

Official Host – Hôte officiel
Malta

Duration of Conference – Durée de la conférence
From / Du: 16 June To / À: 25 June

Location - Adresse
Malta

Agenda – Ordre du jour
Attached

Purpose of Participation - Object de la participation

The 24th Annual FIRST Conference seeks to bridge a gap by focusing on the practical aspects of security and incident response in the face of a rush toward the adoption of cloud computing and other distributed architectures. Considering the inroads that mobile devices are making in our daily workplaces, perhaps it is time for security to redefine itself in some fundamental ways.

The Forum of Incident Response and Security Teams (FIRST) is a global non-profit organization dedicated to bringing together computer security incident response teams (CSIRTs) and includes response teams from over 240 corporations, government bodies, universities and other institutions spread across the Americas, Asia, Europe and Oceania. The annual FIRST conference provides a setting for conference participants to attend a wide range of presentations delivered by leading experts in both the CSIRT field and from the global security community. The conference also creates opportunities for networking, collaboration, and sharing technical information and management practices. The conference enables attendees to meet their peers and build confidential relationships across corporate disciplines and geographical boundaries.

Financial Coding – Code financier
PSABASE 223-2007-S0009S662

Estimated Total Cost / Coût total prévu
$ 11,960.88

Recommended by – Recommandé par
Signature _____ Date _____

Branch Approval – Approbation de la direction
Signature _____ Date _____

Assistant Deputy Minister – Sous-ministre adjoint
Signature _____ Date _____

Deputy Minister – Sous-ministre
Signature _____ Date _____

MS-18 (4/04)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
FIRST Conference, 24th Annual	From - *Du* : June 15, 2012	To - *Au* : June 25, 2012
Location (City, Country) - *Lieu (Ville, Pays)*: Malta (part of Europe)	Estimated total cost - *Coût total prévu*: $11,960.88 per person	

Description of meeting (provide agenda)
Description de l'événement (joindre l'ordre du jour)

FIRST is the world's largest organization of recognized CSIRTs. FIRST conferences are designed to promote the organization's goals of worldwide coordination and cooperation. It serves as the foundation for the improvement of computer security worldwide by sharing goals, ideas, and information. FIRST members, numbering over 250, include national and government CSIRTs, product vendor CSIRTS (e.g. Adobe and Cisco), and Critical Infrastructure CSIRTs (e.g. financial institutions and telcos). Conference attendees commonly provide computer security advice within their own Computer Security Incident Response Teams (CSIRTs) and suggest security strategies, provide technical solutions to security problems, and deliver security education and training to their constituents.

Pre-approved under Branch travel plans?
Pré-approuvé selon les directives sur les voyages de la direction générale?

☒ Yes/Oui ☐ No/Non

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Windy Anderson Luc Beaudoin	NS/NCSD	257 Slater Street 4th Floor	613-991-7055

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

Members comprise the vast majority of international interactions CCIRC undertakes at the tactical and operational levels. Attendance, by CCIRC personnel, is essential in ensuring CCIRC is aware of and has its views heard with respect to information sharing protocols, special capabilities possessed by other CSIRTs and problems, trends and best practices. CCIRC involvement in these conferences is essential in ensuring CCIRC fulfills its mandate as Canada's National CSIRT.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

Having a representative from Canada at this event will directly benefit Public Safety's first three priorities. The networking opportunties alone will help CCIRC advance its capabilities nationally and internationally in Cyber Security. There will be many discussions on how other Cyber Emergency Response Teams operate in other countries; this will allow the Director of CCIRC to come away from the conference with best practices that can be implemented within CCIRC. This will ultimately lead to a more effective and efficient team. Since we are concentrating on a US-Canada Cyber Action Plan this year, it will also be an opportunity to meet with the United States representatives to discuss what we hear at the conference and ensure both countries are aligned with their future direction.

For Mr. Beaudoin, it will be an opportunity to meet and exchange ideas with highly skilled technical experts from many countries in the field of cyber security. There are two full tracks of technical information that will be passed on and discussed with the participants.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

Possibly someone from CSEC, U5 Partners are all participating

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

NCSD, CIPD, CSEC, U5 Partners

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travellers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
***Appuyé par*:**

Name of participant's Director General
Nom du Directeur Générale du voyageur

Date

Reviewed by/
***Examiné par*:**

Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

Date

Approved by/
***Approuvé par*:**

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Date

PS023

Slack, Jessica

From: Slack, Jessica
Sent: May-31-12 1:17 PM
To: Filipps, Lisa
Subject: Fw: FOR INPUT: Media call on Cyber

Can u flip the atis to windy?

From: Anderson, Windy
Sent: Thursday, May 31, 2012 01:14 PM
To: Slack, Jessica
Cc: Matz, Mark; Binne, Christine
Subject: RE: FOR INPUT: Media call on Cyber

Jessica,

Since I do not have a copy of the documents you are talking about, I am finding it difficult to provide answers "out of context".

I can answer all the questions regarding the deck given to the DM (which are a lot of them) but the questions below – I will need the document or context to answer the questions.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them. (Seems like you have an answer to this one)?

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Any help would be appreciated. Getting the other questions answered.

Have a great day,

Windy

Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Slack, Jessica
Sent: May-31-12 12:40 PM

Pages 304 to / à 307

are duplicates of

sont des duplicatas des

pages 344 to / à 347

Slack, Jessica

From: Slack, Jessica
Sent: May-31-12 3:18 PM
To: Matz, Mark
Subject: RE: FOR INPUT: Media call on Cyber

Ok thanks!

From: Matz, Mark
Sent: May-31-12 3:17 PM
To: Slack, Jessica; Anderson, Windy
Cc: Binne, Christine
Subject: Re: FOR INPUT: Media call on Cyber

On it - We should have ready shortly.

From: Slack, Jessica
Sent: Thursday, May 31, 2012 03:14 PM
To: Anderson, Windy
Cc: Matz, Mark; Binne, Christine
Subject: RE: FOR INPUT: Media call on Cyber

Just checking in on this! Thanks...

From: Anderson, Windy
Sent: May-31-12 1:14 PM
To: Slack, Jessica
Cc: Matz, Mark; Binne, Christine
Subject: RE: FOR INPUT: Media call on Cyber

Jessica,

Since I do not have a copy of the documents you are talking about, I am finding it difficult to provide answers "out of context".

I can answer all the questions regarding the deck given to the DM (which are a lot of them) but the questions below – I will need the document or context to answer the questions.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them. (Seems like you have an answer to this one)?

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Any help would be appreciated. Getting the other questions answered.

Have a great day,

Windy

Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Slack, Jessica
Sent: May-31-12 12:40 PM
To: Hatfield, Adam; Matz, Mark; Anderson, Windy
Cc: Filipps, Lisa; Dick, Robert; Weir, Sarah
Subject: FOR INPUT: Media call on Cyber

Hi again,

Windy, I forgot to include you on the heads-up I sent earlier on this – apologies.

Please see below some suggested draft responses. I've mined some previous material we had on file so please feel free to tweak as you see fit what I have.

A number of questions require your answers so those are blank.

We will also need to consult with CSEC so I was hoping to have your input by 2:30. We will then check in with CSEC to ensure they have no concerns. I would like to be able to have a response ready by 4 o'clock to send to Robert for his approval.

Does that sound reasonable?

Happy to discuss.

Many thanks,
Jessica
613-949-4288

1. **Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):**

   - Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

   The Government of Canada remains concerned about threats to cyber security and is doing its part by implementing Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government.

   The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the

Pages 310 to / à 312

are duplicates of

sont des duplicatas des

pages 344 to / à 346

Swift, Andrew

From: Slack, Jessica
Sent: Thursday, May 31, 2012 4:57 PM
To: [redacted]@cse-cst.gc.ca; [redacted]@CSE-CST.GC.CA
Cc: Swift, Andrew; Filipps, Lisa
Subject: RE: Notification: Media call on Cyber

Categories: ATI PRINT

Further to Lisa's note, we are still working on responses with policy. Will get this to you as soon as we can, but may not be until tomorrow morning.
Reporter's deadline is end of day tomorrow.
Jessica

From: Filipps, Lisa
Sent: May-31-12 10:51 AM
To: [redacted]@cse-cst.gc.ca; [redacted]@CSE-CST.GC.CA
Cc: Slack, Jessica; Swift, Andrew
Subject: FW: Notification: Media call on Cyber

Good morning – we have received a media call which will require consultation with you. We are currently working with CCIRC and Cyber Security to develop responses. Please see below.

Thank you! Please don't hesitate to call me if you have any questions.

Lisa

Lisa Filipps
Communications Manager, Issues Management and Media Relations
Gestionnaire, gestion des enjeux et relations avec les médias
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269, avenue Laurier ouest
Ottawa ON K1A 0P8
T: 613-949-9741 | F: 613-954-0800
lisa.filipps@ps-sp.gc.ca

From: Slack, Jessica
Sent: Thursday, May 31, 2012 10:19 AM
To: Dick, Robert; Hatfield, Adam; Labelle, Sébastien; Matz, Mark
Cc: Filipps, Lisa
Subject: FW: Notification: Media call on Cyber

Good morning,

Just wanted to give you a heads-up that we received the call below further to an ATI just released.
We will go through these questions and provide some proposed messaging as a start and get back to you.

Jessica
613-949-4288

From: Slack, Jessica
Sent: May-31-12 10:11 AM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Mueller, Mike; Williams, Christpher
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca); Durand, Stéphanie; Swift, Andrew (Andrew.Swift@ps-sp.gc.ca); Champoux, Martin; Carta, John; Eke, Darren; Picard, Josée
Subject: Notification: Media call on Cyber

Good morning,

We received the call below from Bloomberg.

Consulting with policy. Proposed responses to follow. ATIs cites are attached for reference.

Jessica

Reporter's Name	
Media Outlet	**Bloomberg**
Call Date	**5/31/2012 11:00 AM**
Telephone	
E-mail address	**@bloomberg.net**
Deadline	**5/31/2012 5:00 PM**
Status	**Consulting**
Branch	**NS**
Subject	**TBD**
Questions	**I have some questions regarding two documents I recently received through ATIP. They are attached. My deadline is 5pm Friday.** **Here are my questions for each document:** **1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):** **- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?** **- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?** **- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?** **2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)** **- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?**

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Slack, Jessica

From: Matz, Mark
Sent: May-31-12 4:59 PM
To: Slack, Jessica; Anderson, Windy
Cc: Binne, Christine; Filipps, Lisa
Subject: RE: FOR INPUT: Media call on Cyber

We can send yet this evening – likely in the next 20 minutes.

From: Slack, Jessica
Sent: May-31-12 4:58 PM
To: Matz, Mark; Anderson, Windy
Cc: Binne, Christine; Filipps, Lisa
Subject: RE: FOR INPUT: Media call on Cyber

Thanks. Will you be able to get this back to us first thing tomorrow morning?
Reporter's deadline is 5, but we need to allow time for further approvals and consultation with CSE.
Jessica

From: Matz, Mark
Sent: May-31-12 4:48 PM
To: Slack, Jessica; Anderson, Windy
Cc: Binne, Christine; Filipps, Lisa
Subject: RE: FOR INPUT: Media call on Cyber

Will do!

From: Slack, Jessica
Sent: May-31-12 4:46 PM
To: Matz, Mark; Anderson, Windy
Cc: Binne, Christine; Filipps, Lisa
Subject: RE: FOR INPUT: Media call on Cyber

Mark, Windy

The reporter has come back with an additional question:

By the way, I should add a question on the first document, Mr. Baker's email:

- In the second paragraph of the memo, is [redacted] referring to cyber threats to Canada or cyber threats in general?

Can you please address this as well in your response?
Apologies- [redacted] just sent that to me.
Jessica

From: Matz, Mark
Sent: May-31-12 3:17 PM
To: Slack, Jessica; Anderson, Windy

Cc: Binne, Christine
Subject: Re: FOR INPUT: Media call on Cyber

On it - We should have ready shortly.

From: Slack, Jessica
Sent: Thursday, May 31, 2012 03:14 PM
To: Anderson, Windy
Cc: Matz, Mark; Binne, Christine
Subject: RE: FOR INPUT: Media call on Cyber

Just checking in on this! Thanks...

From: Anderson, Windy
Sent: May-31-12 1:14 PM
To: Slack, Jessica
Cc: Matz, Mark; Binne, Christine
Subject: RE: FOR INPUT: Media call on Cyber

Jessica,

Since I do not have a copy of the documents you are talking about, I am finding it difficult to provide answers "out of context".

I can answer all the questions regarding the deck given to the DM (which are a lot of them) but the questions below – I will need the document or context to answer the questions.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them. (Seems like you have an answer to this one)?

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Any help would be appreciated. Getting the other questions answered.

Have a great day,

Windy

Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Pages 318 to / à 321

are duplicates of

sont des duplicatas des

pages 344 to / à 347

Slack, Jessica

From: Slack, Jessica
Sent: May-31-12 5:24 PM
To: Filipps, Lisa
Subject: Re: FOR INPUT: Media call on Cyber

Ok...will send after robert approves, but unless u have strong feelings otherwise, will do tmrw a.m

From: Filipps, Lisa
Sent: Thursday, May 31, 2012 05:21 PM
To: Slack, Jessica
Subject: Fw: FOR INPUT: Media call on Cyber

We'll need to consult CI also!

From: Matz, Mark
Sent: Thursday, May 31, 2012 05:13 PM
To: Dick, Robert; Slack, Jessica; Hatfield, Adam; Anderson, Windy
Cc: Filipps, Lisa; Weir, Sarah; Fortunato, Stephanie
Subject: RE: FOR INPUT: Media call on Cyber

Robert, for your review. - mark

---

1. **Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):**

   - Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.

As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will switch to one email system, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses on cyber security issues.

The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

Cyber threats in general.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.

CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

- Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy for Critical Infrastructure identifies the following ten critical infrastructure sectors:
  - Health
  - Food
  - Finance
  - Water
  - Information and Communication Technology
  - Safety
  - Energy and utilities
  - Manufacturing
  - Government
  - Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?

CCIRC has staffed all 22 FTEs.

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?

Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. In addition to modernizing its cyber security lab, CCIRC is investing in building a highly skilled workforce that will provide enhanced services. For example, CCIRC is expanding its hours of service to fifteen per day, seven days a week to allow coast to coast coverage during critical hours.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Canada's Cyber Security Strategy focused CCIRC's activities on vital systems outside of federal governments. The process of formalizing CCIRC's mandate is underway.

From: Dick, Robert
Sent: May-31-12 12:44 PM
To: Slack, Jessica; Hatfield, Adam; Matz, Mark; Anderson, Windy
Cc: Filipps, Lisa; Weir, Sarah; Fortunato, Stephanie
Subject: Re: FOR INPUT: Media call on Cyber

Mark...

From: Slack, Jessica
Sent: Thursday, May 31, 2012 12:39 PM
To: Hatfield, Adam; Matz, Mark; Anderson, Windy
Cc: Filipps, Lisa; Dick, Robert; Weir, Sarah
Subject: FOR INPUT: Media call on Cyber

Hi again,

Windy, I forgot to include you on the heads-up I sent earlier on this – apologies.

Please see below some suggested draft responses. I've mined some previous material we had on file so please feel free to tweak as you see fit what I have.

A number of questions require your answers so those are blank.

We will also need to consult with CSEC so I was hoping to have your input by 2:30. We will then check in with CSEC to ensure they have no concerns. I would like to be able to have a response ready by 4 o'clock to send to Robert for his approval.

Does that sound reasonable?

Happy to discuss.

Many thanks,
Jessica
613-949-4288

Pages 325 to / à 327

are duplicates of

sont des duplicatas des

pages 344 to / à 346

Slack, Jessica

From: DeJong, Michael
Sent: June-01-12 9:29 AM
To: Slack, Jessica; Wong, Suki
Cc: Hunt, Ryan
Subject: RE: FOR REVIEW: Media call on Cyber

Hi Jessica – no concerns - thx

From: Slack, Jessica
Sent: June-01-12 9:18 AM
To: Wong, Suki; DeJong, Michael
Cc: Hunt, Ryan
Subject: FOR REVIEW: Media call on Cyber

Good morning,

We received the media call below regarding a Cyber related ATI released recently. The documents are attached for reference.
The responses below were provided by Robert Dick's group, but we wanted to ensure you had no concerns re critical infrastructure questions. –highlighted in yellow

Please get back to me no later than 11 if you have any concerns.

Many thanks,
Jessica

1. **Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):**

   - Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.

As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.

The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

Cyber threats in general.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.

CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy for Critical Infrastructure identifies the following ten critical infrastructure sectors:

- Health
- Food
- Finance
- Water
- Information and Communication Technology
- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?

CCIRC has staffed all 22 FTEs.

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?

Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. In addition to modernizing its cyber security lab, CCIRC is investing in building a highly skilled workforce that will provide enhanced services. For example, CCIRC is expanding its hours of service to fifteen per day, seven days a week to allow coast to coast coverage during critical hours.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Canada's Cyber Security Strategy focused CCIRC's activities on vital systems outside of federal governments. The process of formalizing CCIRC's mandate is underway.

From: Dick, Robert
Sent: May-31-12 12:44 PM
To: Slack, Jessica; Hatfield, Adam; Matz, Mark; Anderson, Windy
Cc: Filipps, Lisa; Weir, Sarah; Fortunato, Stephanie
Subject: Re: FOR INPUT: Media call on Cyber

Mark...

From: Slack, Jessica
Sent: Thursday, May 31, 2012 12:39 PM
To: Hatfield, Adam; Matz, Mark; Anderson, Windy
Cc: Filipps, Lisa; Dick, Robert; Weir, Sarah
Subject: FOR INPUT: Media call on Cyber

Hi again,

Windy, I forgot to include you on the heads-up I sent earlier on this – apologies.

Please see below some suggested draft responses. I've mined some previous material we had on file so please feel free to tweak as you see fit what I have.

A number of questions require your answers so those are blank.

We will also need to consult with CSEC so I was hoping to have your input by 2:30. We will then check in with CSEC to ensure they have no concerns. I would like to be able to have a response ready by 4 o'clock to send to Robert for his approval.

Does that sound reasonable?

Happy to discuss.

Pages 332 to / à 333

are duplicates

sont des duplicatas

Slack, Jessica

From: Slack, Jessica
Sent: June-01-12 10:38 AM
To: Matz, Mark; Anderson, Windy
Subject: RE: FOR INPUT: Media call on Cyber

Mark, Windy – thanks so much. I appreciate all your help on this!

From: Matz, Mark
Sent: June-01-12 10:30 AM
To: Slack, Jessica; Anderson, Windy
Subject: RE: FOR INPUT: Media call on Cyber

I would prefer to mention the expanded hours of service, because it's a good news story from our perspective. However, if you really think it's not helpful, I'll defer to your experience.

Otherwise, I'm fine with the proposed response! Thanks!

Yours ever, mark

From: Slack, Jessica
Sent: June-01-12 10:00 AM
To: Anderson, Windy; Matz, Mark
Subject: RE: FOR INPUT: Media call on Cyber

Windy – to clarify, does that mean you are ok with the revised response below?
Mark, can you confirm as well?

From: Anderson, Windy
Sent: June-01-12 9:51 AM
To: Slack, Jessica; Matz, Mark
Subject: RE: FOR INPUT: Media call on Cyber

This sentence is true, from me.

Have a great day,

Windy

Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Slack, Jessica
Sent: June-01-12 9:50 AM
To: Matz, Mark; Anderson, Windy
Subject: RE: FOR INPUT: Media call on Cyber

Mark, further to our discussion, how about this?
Not certain that we need the last sentence re expansion of service hours fits as the reporter wasn't asking about that...
Happy to discuss further!

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. CCIRC has successfully recruited the additional staff needed and is modernizing its cyber security lab.

From: Matz, Mark
Sent: June-01-12 9:18 AM
To: Slack, Jessica; Anderson, Windy
Subject: Re: FOR INPUT: Media call on Cyber

Will do!

From: Slack, Jessica
Sent: Friday, June 01, 2012 09:12 AM
To: Matz, Mark; Anderson, Windy
Subject: RE: FOR INPUT: Media call on Cyber

Mark and Windy – thanks for all your work on this.
Was hoping to have a quick chat re this question – could you or Windy give me a call?
Jessica
613-949-4288

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. In addition to modernizing its cyber security lab, CCIRC is investing in building a highly skilled workforce that will provide enhanced services. For example, CCIRC is expanding its hours of service to fifteen per day, seven days a week to allow coast to coast coverage during critical hours.

From: Dick, Robert
Sent: May-31-12 5:41 PM
To: Matz, Mark; Slack, Jessica; Hatfield, Adam; Anderson, Windy
Cc: Filipps, Lisa; Weir, Sarah; Fortunato, Stephanie
Subject: Re: FOR INPUT: Media call on Cyber

- an unnecessary "on" in the last sentence of the third para

- second para "this means the Government will consolidate its email systems". (I'm not sure if it technically will be one system, so this language is safer.

Great work!

From: Matz, Mark
Sent: Thursday, May 31, 2012 05:13 PM
To: Dick, Robert; Slack, Jessica; Hatfield, Adam; Anderson, Windy
Cc: Filipps, Lisa; Weir, Sarah; Fortunato, Stephanie
Subject: RE: FOR INPUT: Media call on Cyber

Robert, for your review. - mark

---

1. **Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):**

   - Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.

As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will switch to one email system, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses on cyber security issues.

The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

Cyber threats in general.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.

CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other

stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

- Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy for Critical Infrastructure identifies the following ten critical infrastructure sectors:
  - Health
  - Food
  - Finance
  - Water
  - Information and Communication Technology
  - Safety
  - Energy and utilities
  - Manufacturing
  - Government
  - Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?

CCIRC has staffed all 22 FTEs.

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?

Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. In addition to modernizing its cyber security lab, CCIRC is investing in building a highly skilled workforce that will provide enhanced services. For example, CCIRC is expanding its hours of service to fifteen per day, seven days a week to allow coast to coast coverage during critical hours.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Page 338

is a duplicate of

est un duplicata de la

page 344

Page 339
is a duplicate of
est un duplicata de la
page 346

Pages 340 to / à 341

are duplicates of

sont des duplicatas des

pages 346 to / à 347

Slack, Jessica

From: Swift, Andrew
Sent: June-01-12 11:14 AM
To: Slack, Jessica
Cc: Filipps, Lisa
Subject: RE: FOR REVIEW: Media call on Cyber

Looks great. I would send a copy to Shared Services as FYI as well, seeing as we mention them.

I would also hyperlink the reference to "The National Strategy for Critical Infrastructure".

Thx.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica
Sent: Friday, June 01, 2012 10:38 AM
To: Swift, Andrew
Cc: Filipps, Lisa
Subject: FW: FOR REVIEW: Media call on Cyber

Andrew,

Proposed response for approval. Mark Matz, Windy Anderson, Robert Dick have approved. Mike de Jong also reviewed re CI and had no concerns. Lisa has approved.

I will send this over to CSEC for their review.
Jessica

1. **Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):**

   - Mr. Baker says in his letter that the threat environment is ``likely worsening" and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.

As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.

The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

Cyber threats in general.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.

CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.

- The second page refers to ``critical infrastructure sectors." Which sectors does that include?

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy for Critical Infrastructure identifies the following ten critical infrastructure sectors:

- Health
- Food
- Finance
- Water
- Information and Communication Technology
- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?

CCIRC has staffed all 22 FTEs.

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?

Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. CCIRC has successfully recruited the additional staff needed and is modernizing its cyber security lab.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Canada's Cyber Security Strategy focused CCIRC's activities on vital systems outside of federal governments. The process of formalizing CCIRC's mandate is underway.

From: Dick, Robert
Sent: May-31-12 12:44 PM
To: Slack, Jessica; Hatfield, Adam; Matz, Mark; Anderson, Windy
Cc: Filipps, Lisa; Weir, Sarah; Fortunato, Stephanie
Subject: Re: FOR INPUT: Media call on Cyber

Mark...

From: Slack, Jessica
Sent: Thursday, May 31, 2012 12:39 PM
To: Hatfield, Adam; Matz, Mark; Anderson, Windy
Cc: Filipps, Lisa; Dick, Robert; Weir, Sarah
Subject: FOR INPUT: Media call on Cyber

Hi again,

Windy, I forgot to include you on the heads-up I sent earlier on this – apologies.

Please see below some suggested draft responses. I've mined some previous material we had on file so please feel free to tweak as you see fit what I have.

A number of questions require your answers so those are blank.

We will also need to consult with CSEC so I was hoping to have your input by 2:30. We will then check in with CSEC to ensure they have no concerns. I would like to be able to have a response ready by 4 o'clock to send to Robert for his approval.

Does that sound reasonable?

Happy to discuss.

Many thanks,
Jessica
613-949-4288

1. **Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):**

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is doing its part by implementing Canada's Cyber Security Strategy, an approach emphasizing working in partnership both inside and outside of government.

The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians.

The Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such as telecommunications networks, the financial sector, power grids and other vital systems – are getting the information they need to protect themselves and keep their systems secure. For example, the Canadian Cyber Incident Response Centre (CCIRC) monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats.

Another important element of the Strategy is Get Cyber Safe, the Government of Canada's national public awareness initiative. The getcybersafe.ca web site provides information that helps Canadians protect themselves and their families against a wide range of online threats.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Their roles are different as each organization address different pillars of the Cyber Security Strategy.

The work of Communications Security Establishment Canada supports Pillar 1 of the Strategy, "secure Government systems," while the work of the Canadian Cyber Incident Response Centre, supports Pillar 2, "partner to secure systems outside the Government of Canada."

As noted above, CCIRC monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats.

Specifically, CCIRC provides the following services to IT professionals and managers of critical infrastructure and other related industries: coordination and support for cyber incident response efforts; monitoring and analysis of the cyber threat environment; and information technology security-related technical advice, including information that can be used to help mitigate threats.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

From: Slack, Jessica
Sent: May-31-12 10:19 AM
To: Dick, Robert; Hatfield, Adam; Labelle, Sébastien; Matz, Mark
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca)
Subject: FW: Notification: Media call on Cyber

Good morning,

Just wanted to give you a heads-up that we received the call below further to an ATI just released.
We will go through these questions and provide some proposed messaging as a start and get back to you.

Jessica
613-949-4288

From: Slack, Jessica
Sent: May-31-12 10:11 AM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Mueller, Mike; Williams, Christpher
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca); Durand, Stéphanie; Swift, Andrew (Andrew.Swift@ps-sp.gc.ca); Champoux, Martin; Carta, John; Eke, Darren; Picard, Josée
Subject: Notification: Media call on Cyber

Good morning,

We received the call below from Bloomberg.

Consulting with policy. Proposed responses to follow. ATIs [redacted] cites are attached for reference.

Jessica

Reporter's Name	[redacted]
Media Outlet	**Bloomberg** s.19(1)
Call Date	**5/31/2012 11:00 AM**
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	**5/31/2012 5:00 PM**
Status	**Consulting**
Branch	**NS**
Subject	**TBD**
Questions	**I have some questions regarding two documents I recently received through ATIP. They are attached. My deadline is 5pm Friday.**

Here are my questions for each document:

1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?
- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?
- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?
- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Bue, Richard

From: Swift, Andrew
Sent: June-01-12 12:37 PM
To: Durand, Stéphanie; Slack, Jessica; Bue, Richard; Salewski, Shawn; Dubé, Rosanne
Cc: Eke, Darren; Carta, John; Filipps, Lisa; Picard, Josée; Champoux, Martin; Hannan, Andrew
Subject: RE: FOR APPROVAL: Media call on Cyber

Good idea. We will look into that.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Durand, Stéphanie
Sent: Friday, June 01, 2012 12:25 PM
To: Slack, Jessica; Bue, Richard; Salewski, Shawn; Dubé, Rosanne
Cc: Swift, Andrew; Eke, Darren; Carta, John; Filipps, Lisa; Picard, Josée; Champoux, Martin; Hannan, Andrew
Subject: Re: FOR APPROVAL: Media call on Cyber

Thanks - I'm fine with this.

Andrew S: for the future, can we look at beefing up our web presence to answer a reocurring question re roles and resp for cyber incidents...

From: Slack, Jessica
Sent: Friday, June 01, 2012 11:38 AM
To: Durand, Stéphanie; Bue, Richard; Salewski, Shawn; Dubé, Rosanne
Cc: Swift, Andrew; Eke, Darren; Carta, John; Filipps, Lisa; Picard, Josée; Champoux, Martin
Subject: FOR APPROVAL: Media call on Cyber

Stéphanie,

Proposed response for approval.

Mark Matz, Windy Anderson, Robert Dick have approved. Mike de Jong also reviewed re CI and had no concerns. Lisa and Andrew have approved and we have also checked in with CSEC who have no concerns.

We also shared Shared Services for their information.

Jessica

1. **Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):**

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.

As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.

The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

Cyber threats in general.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.

CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy for Critical Infrastructure identifies the following ten critical infrastructure sectors:

- Health
- Food
- Finance
- Water
- Information and Communication Technology
- Safety
- Energy and utilities

- Manufacturing
- Government
- Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?

CCIRC has staffed all 22 FTEs.

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?

Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. CCIRC has successfully recruited the additional staff needed and is modernizing its cyber security lab.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Canada's Cyber Security Strategy focused CCIRC's activities on vital systems outside of federal governments. The process of formalizing CCIRC's mandate is underway.

From: Slack, Jessica
Sent: May-31-12 10:11 AM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Mueller, Mike; Williams, Christpher
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca); Durand, Stéphanie; Swift, Andrew (Andrew.Swift@ps-sp.gc.ca); Champoux, Martin; Carta, John; Eke, Darren; Picard, Josée
Subject: Notification: Media call on Cyber

Good morning,

We received the call below from Bloomberg.

Consulting with policy. Proposed responses to follow. ATIs cites are attached for reference.

Jessica

s.19(1)

Reporter's Name

Media Outlet	**Bloomberg**
Call Date	**5/31/2012 11:00 AM**
Telephone	[redacted] s.19(1)
E-mail address	[redacted]@bloomberg.net
Deadline	**6/01/2012 5:00 PM**
Status	**Consulting**
Branch	**NS**
Subject	**TBD**
Questions	**I have some questions regarding two documents I recently received through ATIP. They are attached. My deadline is 5pm Friday.**

Here are my questions for each document:

1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?
- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?
- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?
- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Slack, Jessica

From: Slack, Jessica
Sent: June-01-12 12:42 PM
To: Swift, Andrew
Subject: RE: FOR APPROVAL: Media call on Cyber

Ok thanks

From: Swift, Andrew
Sent: June-01-12 12:41 PM
To: Slack, Jessica
Subject: RE: FOR APPROVAL: Media call on Cyber

We may want to hyperlink the cyber security strategy reference while we're at it.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica
Sent: Friday, June 01, 2012 12:38 PM
To: Carmichael, Julie; Mueller, Mike; Johnson, Mark; McGrath, Andrew; Williams, Christpher
Cc: Swift, Andrew; Filipps, Lisa; Durand, Stéphanie; Champoux, Martin; Eke, Darren; Carta, John; Hannan, Andrew
Subject: FOR APPROVAL: Media call on Cyber

s.19(1)

Julie- here are the responses to [redacted] questions for approval.
His deadline is end of day.
Jessica

1. **Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):**

   - Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.

As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian

Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.

The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

Cyber threats in general.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.

CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy for Critical Infrastructure identifies the following ten critical infrastructure sectors:

- Health
- Food
- Finance
- Water
- Information and Communication Technology
- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?

CCIRC has staffed all 22 FTEs.

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?

Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. CCIRC has successfully recruited the additional staff needed and is modernizing its cyber security lab.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Canada's Cyber Security Strategy focused CCIRC's activities on vital systems outside of federal governments. The process of formalizing CCIRC's mandate is underway.

From: Slack, Jessica
Sent: May-31-12 10:11 AM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Mueller, Mike; Williams, Christpher
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca); Durand, Stéphanie; Swift, Andrew (Andrew.Swift@ps-sp.gc.ca); Champoux, Martin; Carta, John; Eke, Darren; Picard, Josée
Subject: Notification: Media call on Cyber

Good morning,

We received the call below from Bloomberg.

Consulting with policy. Proposed responses to follow. ATIs he cites are attached for reference.

Jessica

Reporter's Name	[redacted]
Media Outlet	**Bloomberg**
Call Date	**5/31/2012 11:00 AM**
Telephone	[redacted] s.19(1)
E-mail address	[redacted]@bloomberg.net
Deadline	**6/01/2012 5:00 PM**
Status	**Consulting**
Branch	**NS**
Subject	**TBD**
Questions	**I have some questions regarding two documents I recently received through ATIP.**

They are attached. My deadline is 5pm Friday.

Here are my questions for each document:

1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?
- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?
- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?
- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Pages 356 to / à 359

are duplicates of

sont des duplicatas des

pages 360 to / à 363

Slack, Jessica

From: Slack, Jessica on behalf of PS Media Relations / Relations médias SP
Sent: June-01-12 2:18 PM
To: [redacted] (BLOOMBERG/ NEWSROOM:)'
Subject: RE: Cyberattacks vs. Canada

Of course.
Jessica

Jessica Slack
Spokesperson / Porte-parole
Media Relations / Relations avec les médias Public Safety Canada / Sécurité publique Canada
613-991-0657
media@ps-sp.gc.ca

-----Original Message-----
From: [redacted] (BLOOMBERG/ NEWSROOM:) [mailto [redacted]@bloomberg.net]
Sent: June-01-12 2:11 PM
To: PS Media Relations / Relations médias SP
Subject: RE: Cyberattacks vs. Canada

Can I have your full name and title, by the way? Otherwise, someone to attribute these statements to?

----- Original Message -----
From: PSMediaRelations@ps-sp.gc.ca
To: [redacted] BLOOMBERG/ NEWSROOM:)
At: 6/01 14:03:27

Hi [redacted]

Please find the answers to your questions below.

I hope this is helpful.

Regards,
Jessica

1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy<http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx>.

As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.

The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

Cyber threats in general.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.

CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?
Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy for Critical Infrastructure<http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx> identifies the following ten critical infrastructure sectors:

- Health
- Food
- Finance
- Water
- Information and Communication Technology
- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?

CCIRC has staffed all 22 FTEs.

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?

Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?

CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. CCIRC has successfully recruited the additional staff needed and is modernizing its cyber security lab.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?

We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Canada's Cyber Security Strategy focused CCIRC's activities on vital systems outside of federal governments. The process of formalizing CCIRC's mandate is underway.

-----Original Message-----
From: [redacted](BLOOMBERG/ NEWSROOM:) [mailto:[redacted]@bloomberg.net]
Sent: May-31-12 4:43 PM
To: PS Media Relations / Relations médias SP
Subject: RE: Cyberattacks vs. Canada

Thanks. By the way, I should add a question on the first document, Mr. Baker's email:

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

[redacted]

----- Original Message -----
From: PSMediaRelations@ps-sp.gc.ca<mailto:PSMediaRelations@ps-sp.gc.ca>
To:[redacted](BLOOMBERG/ NEWSROOM:)
At: 5/31 10:04:42

Hi [redacted]

We will check into these for you.

Jessica

-----Original Message-----
From: [redacted](BLOOMBERG/ NEWSROOM:)
[mailto:[redacted]@bloomberg.net]<mailto:[mailto:[redacted]@bloomberg.net]>
Sent: May-31-12 9:47 AM
To: PS Media Relations / Relations médias SP
Subject: Cyberattacks vs. Canada

Hi,

I have some questions regarding two documents I recently received through ATIP. They are attached. My deadline is 5pm Friday.

Here are my questions for each document:

1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?
- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?
- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?
- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Regards,

[redacted]Reporter, Bloomberg News
46 Elgin Street, Suite 110, Ottawa ON Canada K1P 5K6 office [redacted] cell [redacted]
[redacted]@bloomberg.net<mailto:[redacted]@bloomberg.net> http://www.bloomberg.com/news/canada/

Slack, Jessica

From: Slack, Jessica
Sent: June-01-12 6:15 PM
To: [redacted]@CSE-CST.GC.CA'; [redacted]@CSE-CST.GC.CA'
Cc: Swift, Andrew; Filipps, Lisa
Subject: Re: Notification: Media call on Cyber

The reporter received the response this afternoon, so I expect his story to be filed today or tomorrw.

From: Plamondon, Jean J. [mailto[redacted]@CSE-CST.GC.CA]
Sent: Friday, June 01, 2012 05:18 PM
To: Slack, Jessica; [redacted]@CSE-CST.GC.CA>
Cc: Swift, Andrew; Filipps, Lisa
Subject: RE: Notification: Media call on Cyber

Classification: UNCLASSIFIED

Jessica,

would appreciate an approximate deadline for the journalist's publication in order to advise MNDO.

Le directeur APSC
Jean Plamondon

Director
PACS
Tel. 613.991.7246

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: 1 juin 2012 10:42
To: Plamondon, Jean J.; [redacted]
Cc: Swift, Andrew; Filipps, Lisa
Subject: RE: Notification: Media call on Cyber

Good morning,
See policy approved responses below.
Please advise asap if you have any concerns. Portion referencing CSEC is highlighted.
Jessica

1. **Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):**

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.

As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.

The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

Cyber threats in general.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.

CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy for Critical Infrastructure identifies the following ten critical infrastructure sectors:

- Health
- Food
- Finance
- Water
- Information and Communication Technology
- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?

CCIRC has staffed all 22 FTEs.

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. CCIRC has successfully recruited the additional staff needed and is modernizing its cyber security lab.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.

- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?
Canada's Cyber Security Strategy focused CCIRC's activities on vital systems outside of federal governments. The process of formalizing CCIRC's mandate is underway.

From: Plamondon, Jean J. [mailto: [redacted]@CSE-CST.GC.CA]
Sent: May-31-12 5:16 PM
To: Slack, Jessica; [redacted]
Cc: Swift, Andrew; Filipps, Lisa
Subject: RE: Notification: Media call on Cyber
Classification: UNCLASSIFIED
Will be standing by.

Le directeur APSC
Jean Plamondon

Director
PACS
Tel. 613.991.7246

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: 31 mai 2012 16:57
To: Plamondon, Jean J.; [redacted]
Cc: Swift, Andrew; Filipps, Lisa
Subject: RE: Notification: Media call on Cyber

Further to Lisa's note, we are still working on responses with policy. Will get this to you as soon as we can, but may not be until tomorrow morning.
Reporter's deadline is end of day tomorrow.
Jessica

From: Filipps, Lisa
Sent: May-31-12 10:51 AM

To: [redacted]@cse-cst.gc.ca; [redacted]@CSE-CST.GC.CA
Cc: Slack, Jessica; Swift, Andrew
Subject: FW: Notification: Media call on Cyber

Good morning – we have received a media call which will require consultation with you. We are currently working with CCIRC and Cyber Security to develop responses. Please see below.

Thank you! Please don't hesitate to call me if you have any questions.

Lisa

Lisa Filipps
Communications Manager, Issues Management and Media Relations
Gestionnaire, gestion des enjeux et relations avec les médias
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269, avenue Laurier ouest
Ottawa ON K1A 0P8
T: 613-949-9741 | F: 613-954-0800
lisa.filipps@ps-sp.gc.ca

From: Slack, Jessica
Sent: Thursday, May 31, 2012 10:19 AM
To: Dick, Robert; Hatfield, Adam; Labelle, Sébastien; Matz, Mark
Cc: Filipps, Lisa
Subject: FW: Notification: Media call on Cyber

Good morning,

Just wanted to give you a heads-up that we received the call below further to an ATI just released.

We will go through these questions and provide some proposed messaging as a start and get back to you.

Jessica

613-949-4288

From: Slack, Jessica
Sent: May-31-12 10:11 AM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Mueller, Mike; Williams, Christpher
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca); Durand, Stéphanie; Swift, Andrew (Andrew.Swift@ps-sp.gc.ca); Champoux, Martin; Carta, John; Eke, Darren; Picard, Josée
Subject: Notification: Media call on Cyber

Good morning,

We received the call below from Bloomberg.

Consulting with policy. Proposed responses to follow. ATIs [redacted] cites are attached for reference.

Jessica

Reporter's Name	[redacted]
Media Outlet	**Bloomberg**
Call Date	**5/31/2012 11:00 AM**
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	**5/31/2012 5:00 PM**
Status	**Consulting**
Branch	**NS**
Subject	**TBD**
Questions	**I have some questions regarding two documents I recently received through ATIP. They are attached. My deadline is 5pm Friday.** **Here are my questions for each document:**

1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?
- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?
- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?
- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Slack, Jessica

From: Slack, Jessica
Sent: June-06-12 1:54 PM
To: Champoux, Martin
Subject: FW: Notification: Media call on Cyber
Attachments: ccirc atip may 12.pdf; ps atip cyberthreats may 12.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

And here are questions:
1) What is the government's current plan to combat cyber attacks?

2) In a recent article citing documents, it is suggested that the Canadian Cyber Incident Response Centre "faces challenges such as an unclear mandate, the absence of a "national emergency policy" for cyber security, old lab facilities and trouble attracting and retaining talent." Is this true, and is the ministry aiming to rectify these problems?

From: Slack, Jessica
Sent: May-31-12 10:11 AM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Mueller, Mike; Williams, Christpher
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca); Durand, Stéphanie; Swift, Andrew (Andrew.Swift@ps-sp.gc.ca); Champoux, Martin; Carta, John; Eke, Darren; Picard, Josée
Subject: Notification: Media call on Cyber

Good morning,

We received the call below from Bloomberg.

Consulting with policy. Proposed responses to follow. ATIs [redacted]cites are attached for reference.

Jessica

Reporter's Name	[redacted]
Media Outlet	**Bloomberg**
Call Date	**5/31/2012 11:00 AM**
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	**5/31/2012 5:00 PM**
Status	**Consulting**
Branch	**NS**
Subject	**TBD**

Questions

I have some questions regarding two documents I recently received through ATIP. They are attached. My deadline is 5pm Friday.

Here are my questions for each document:

1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):

- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?
- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?
- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)

- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?
- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?

Slack, Jessica

From: Slack, Jessica
Sent: July-10-12 4:48 PM
To: Swift, Andrew; Filipps, Lisa
Subject: RE: As Discussed

Full response on the q's stemming from the ATI is below...Most relevant high level lines are for the first question:

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.
As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.
Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.
The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.
- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?
Cyber threats in general.

Reporter's Name	[redacted]
Media Outlet	Bloomberg s.19(1)
Call Date	5/31/2012 11:00 AM
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	6/1/2012 5:00 PM
Status	Final
Branch	NS
Subject	Cyber Security Strategy
Questions	I have some questions regarding two documents I recently received through ATIP. They are attached. My deadline is 5pm Friday. Here are my questions for each document: 1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12): - Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning *to impact economic prosperity through loss of IP. Is this still the department's position?* - Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different? - The second page refers to ``critical infrastructure sectors.'' Which sectors does that include? 2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12) - The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have? - Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?

Pages 372 to / à 373

are duplicates of

sont des duplicatas des

pages 375 to / à 376

Slack, Jessica

From: Swift, Andrew
Sent: July-10-12 5:02 PM
To: Johnson, Mark
Cc: Carmichael, Julie; Filipps, Lisa; Slack, Jessica
Subject: RE: As Discussed

Hi Mark,
This article actually is from a Bloomberg piece that ran a couple weeks ago. The lines we used to respond to the original enquiry are below.
Andrew

Reporter's Name	[redacted]
Media Outlet	Bloomberg
Call Date	5/31/2012 11:00 AM
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	6/1/2012 5:00 PM
Status	Final
Branch	NS
Subject	Cyber Security Strategy
Questions	I have some questions regarding two documents I recently received through ATIP. They are attached. My deadline is 5pm Friday. Here are my questions for each document: 1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12): - Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position? - Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different? - The second page refers to ``critical infrastructure sectors.'' Which sectors does that include? 2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12) - The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have? - Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems? - Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed? - Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning? - Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?
Reporter and Outlet	[redacted]- Bloomberg
Actions Taken	No existing entries.
Draft Response	
Approvals	Windy Anderson, Mark Matz, Robert Dick, Lisa, Andrew, Stephanie, Julie

s.19(1)

1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):
- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?

The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.
As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.
Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.
The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.

- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?

Cyber threats in general.

- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?

Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.

CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.

- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy for Critical Infrastructure identifies the following ten critical infrastructure sectors:
- Health
- Food
- Finance
- Water
- Information and Communication Technology
- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)
- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?
CCIRC has staffed all 22 FTEs.
- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. CCIRC has successfully recruited the additional staff needed and is modernizing its cyber security lab.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?
Canada's Cyber Security Strategy focused CCIRC's activities on vital systems outside of federal governments. The process of formalizing CCIRC's mandate is underway.

From: Johnson, Mark
Sent: Tuesday, July 10, 2012 4:35 PM
To: Swift, Andrew
Cc: Carmichael, Julie
Subject: As Discussed

Could I see the lines we would use?

http://www.scmagazine.com/canada-suffers-from-poor-cyber-security-says-memo/article/249675/

Swift, Andrew

From: Carmichael, Julie
Sent: Thursday, July 12, 2012 8:30 AM
To: Swift, Andrew
Subject: Re: FYI: RCMP heads up CP enquiry re Anonymous investigation re Minister

Categories: ATI PRINT

Thanks

Julie Carmichael
A/Director of Communications
Office of the Minister of Public Safety
Julie.carmichael@ps-sp.gc.ca

----- Original Message -----
From: Swift, Andrew
Sent: Thursday, July 12, 2012 08:28 AM
To: Carmichael, Julie; Johnson, Mark; Mueller, Mike; McGrath, Andrew
Cc: Tomlinson, Jamie; Filipps, Lisa; Thibouthot, AkimIsabelle
Subject: FYI: RCMP heads up CP enquiry re Anonymous investigation re Minister

Julie,
See heads up below from RCMP. We will continue to monitor.
Andrew

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Julie Gagnon [mailto:julie.gagnon@rcmp-grc.gc.ca]
Sent: Wednesday, July 11, 2012 07:53 PM
To: Swift, Andrew
Cc: Tomlinson, Jamie; Filipps, Lisa; Derek Cefaloni <Derek.Cefaloni@rcmp-grc.gc.ca>; Marc Richer <Marc.Richer@rcmp-grc.gc.ca>
Subject: Heads up on call at A Div

Hello Andrew,

I just want to let you know that today our A Division office received a call from

Reporter from Canadian Press wanting to know if RCMP investigation into the videos Anonymous posted online re Minister Toews is still ongoing.

Our A Division office answered the followings:

Generally, only in the event that an investigation results in the laying of criminal charges, would the RCMP confirm its investigation, the nature of any charges laid and the identity of the individual (s) involved.
Should the investigation not generate sufficient evidence to support the laying of criminal charges, the RCMP would conclude its file and in most cases advise the complainant privately of this result.

Julie
Sgt. Julie Gagnon
RCMP National Communication Services / Services nationaux de communication de la GRC Sent from my wireless device
Depuis mon sans fil

Slack, Jessica

From: Fortunato, Stephanie
Sent: June-13-12 9:14 AM
To: Filipps, Lisa
Cc: Champoux, Martin; Slack, Jessica; Swift, Andrew; Dick, Robert; Clow, Patrick; Baulne, Lucie
Subject: RE: Stratfor incident
Attachments: PS-SP-#541955-2-Briefing Note - CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY- to DM - 2012-01-06.doc; PS-SP-#572420-v1-IC_EDITS_FOR_CYBERSECURITY_SUMMARY_FOR_CIOs_-_PILOT_-_FEB_2012.doc

Hi Lisa,

Attached are the two documents pertaining to the article circulating in the news. Since it was a matter that affected the federal government, CTEC (CSE) and the RCMP would be the best to answer specific questions related to the levels, departments, etc. CCIRC's involvement would be mitigating the risk with the provincial governments and CI sectors. Please let me know if you have any trouble opening the documents.

Thank you,

Stéphanie

From: Filipps, Lisa
Sent: June-13-12 8:24 AM
To: Clow, Patrick
Cc: Champoux, Martin; Slack, Jessica; Swift, Andrew; Fortunato, Stephanie
Subject: RE: Stratfor incident

Hi Patrick – can you advise of an ETA – with the press coverage MO is very interested.

From: Clow, Patrick
Sent: Tuesday, June 12, 2012 5:54 PM
To: Filipps, Lisa
Cc: Champoux, Martin; Slack, Jessica; Swift, Andrew; Fortunato, Stephanie
Subject: RE: Stratfor incident

Hi Lisa,

It appears TBS & SSC have also requested this information via NCSD contacts. I know that some material was provided through that channel. We can certainly assess the information requested first thing tomorrow.

Thank you

From: Filipps, Lisa
Sent: June-12-12 4:48 PM
To: Clow, Patrick
Cc: Champoux, Martin; Slack, Jessica; Swift, Andrew
Subject: Stratfor incident

Hi Patrick – I understand that Windy is away so I am reaching out to you in her absence. MO has asked us to find out more about what level of government executive would have had account information stolen as a result of the hacking of Stratfor. It would be helpful to know, besides what levels (EXs? DMs? Which departments?) what kind of information was stolen.

Would it be possible to get this information first thing in the morning? I will ask Martin Champoux to follow up with you tomorrow.

Thanks in advance!

Lisa

UNCLASSIFIED

DATE:

File No.: 384961
RDIMS No.: 541955

MEMORANDUM FOR THE DEPUTY MINISTER

CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

(Information only)

ISSUE

Eight hundred and eighty federal government workers and 109 provincial government users in nine provinces have been affected by the hacking of a private international intelligence agency.

BACKGROUND

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter, they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

CONSIDERATIONS

There are financial, workplace security, and privacy considerations regarding this incident.

First, there is a financial risk to all impacted individuals as the credit card information posted online contained the full 16 digit number, expiry date, and Card Verification Value number (i.e. everything needed to make purchases).

Second, compromised individuals could be victims of specific and targeted attacks, such as malicious emails, social engineering, and attempts to compromise workplace security.

Third, impacted individuals' privacy could be compromised as home/office telephone numbers and home/office addresses were released. Given the fact that 860,000 login credentials have been compromised, there is also a strong likelihood that additional downstream privacy risks exist for impacted individuals as a significant percentage of the population uses the same password for many Internet sites and work.

NEXT STEPS

There are three main actions that the Canadian Cyber Incident Response Centre (CCIRC) is taking to address this situation.

First, CCIRC is working with RCMP to identify federal government users registered with STRATFOR. Identified users will be notified through the Cyber Threat Evaluation Centre (CTEC).

Second, CCIRC has completed its analysis and identified provincial government users who have been affected. CCIRC has notified each provincial government's lead cyber security department.

Third, CCIRC has recommended that affected government employees change all Internet account passwords that use elements from their compromised password; monitor their credit card transactions and; contact their bank regarding the credit card breach.

CCIRC has closed this incident and will continue to monitor for any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Sandra Williston

Public Safety Canada | Sécurité publique Canada

Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CYBER SECURITY SUMMARY FOR CIOs

Reporting Period: JANUARY 28-FEBRUARY 11, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-003

Purpose

This product is intended to provide Chief Information Officers in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations. This product also provides contextual background information for the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Highlights

- Microsoft Office documents stolen from over 600 computers.
- Is your computer one of the thousands in Canada affected by Ghostclick? Check CCIRC approved site www.dns-ok.ca
- Ghostclick in Canada – Some Statistics
- In the news: Anonymous hacks websites of U.S., French Government & UN

Overview

Domestically, there were no significant cyber incidents. CCIRC handled 48 incidents during the reporting period. MS Office documents were stolen from over 600 computers in 19 identifiable organizations and 84 telecommunications service providers, which include internet service providers for the Canadian public and corporate sector. Malicious acts include coordinating cyber attacks on the financial sector of another country. A botnet that affected the Canadian energy utility sector in late 2011 was still active. Cyber criminals impersonated banks and the federal government to obtain financial and personal information from computer users (phishing). There were website defacements for health, education, municipal and provincial government sector organizations.

CCIRC Products Released:

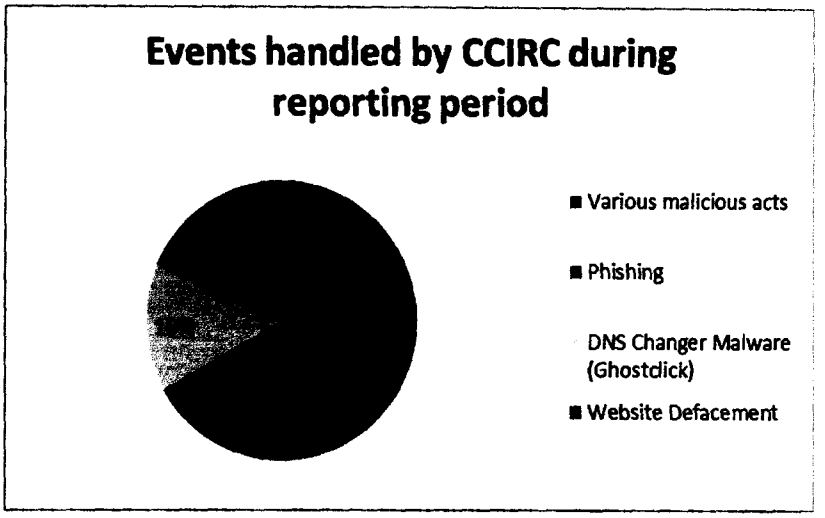
- Cyber Flash CF12-002: Malware uses Sendspace.com file-hosting site to store stolen documents.

Noteworthy News in the Media:

- Hackers attack websites of the French Government, US Department of Homeland Security and UN; Anonymous releases FBI conference call recording
- Hackers in Europe release names of persons involved in hate movements – includes 74 Canadians

NEW EVENTS REPORTED

Non-Federal Government Critical Infrastructure Sector



Microsoft Office Documents stolen from over 600 Canadian entities. A trusted partner alerted CCIRC that MS Excel and Word documents originating from over 600 Canadian computers were stolen and posted to a file-sharing website. Computers in question were compromised via a malicious executable file attachment to an e-mail. It was noted the malicious software attempts to contact a website in Russia. The impact of this incident is unknown to CCIRC.

CCIRC notified the identified entities, which included provincial health and municipal government entities, a financial institution, a utility, an auto parts manufacturer, post-secondary institutions. Telecommunications service providers were also notified so they could to notify their clients, whose data would have been stolen. CCIRC also sent Cyber Flash CF12-002 to all CCIRC stakeholders.

> ***Comment:*** *The impact of this incident is unknown at this time. It is likely that the threat actors intended to upload the stolen documents from this file-sharing website to obscure their identity and location.*
>
> *Malicious e-mails are a very common but still very effective method of compromising computer systems. Security researchers see this trend continuing in 2012 and CCIRC would agree. In fact, CCIRC sees that cyber criminals are becoming more effective by sending more tailored e-mails to individuals in organizations. Organizations need to implement a wide range of organizational measures that range from technical solutions to employee education.*

Canadian domain being used in cyber attacks. CCIRC learned that a Canadian domain was used to coordinate a Distributed Denial of Service cyber attack on websites of an allied country's financial sector. This domain was registered in Canada by an individual in Moscow, Russia, but the cyber attacks were traced to a computer in Latvia.

CCIRC assisted the ally country by contacting the Canadian domain name registrar and requesting it rectify the situation. CCIRC also notified the Canadian Internet Registration Authority (CIRA) and Canadian law enforcement. The malicious site is no longer active as of the writing of this report.

> ***Comment:*** *Many computer users/operators can and do block internet access from computers and websites known to reside in untrusted countries. Therefore, cyber criminals take advantage of the trusted on-line reputation of countries like Canada by registering an Internet domain name in Canada and appearing to be a Canadian website.*

Web related services such as domain name registration have an international client base and no rigorous identity verification process. International law enforcement is discussing this issue with the international domain name registrar community at the International Corporation for Assigned Names and Numbers (ICANN) meetings. ICANN is an international, non-profit group that plays a coordinating role for the Internet's naming system.

Botnet that affected the Canadian energy utility sector in late 2011 is still active. An energy utility partner reported that the Raumoni Perl Botnet that affected that organization three months ago was still active elsewhere and provided information about the controller to CCIRC. CCIRC's technical team is currently analyzing the associated data so Canadian victims can be identified and notified.

Canadian credit card information posted online. Credit card information of six Canadians was found to be posted online. This item is of interest because it appears to be a continuation of the STRATFOR website hacking in December 2011. In that incident, approximately 75,000 credit card numbers and 860,000 login credentials were posted online. In Canada, 880 federal government workers and 109 provincial government users in nine provinces were affected.

Comment: *There is little doubt we will continue TO see repercussions of the STRATFOR website hacking. The client information posted online includes government officials who are interested in STRATFOR's intelligence reports. As of the time of this writing, there were news reports of STRATFOR clients being targeted with malicious e-mails. These e-mails, purportedly originating from the STRATFOR CEO, asked clients to click on a link and fill out a form.*

Canadian computer part of an international malicious network (botnet). CCIRC learned a Canadian computer was part of a FastFlux botnet that appears to be controlled by a Russian website. A Fast Flux botnet is a malicious network of computers that can hide phishing and malware delivery sites behind an ever-changing network of compromised computers.

The Internet services for the Canadian entity are provided by a hosting provider in British Columbia. CCIRC contacted the parent company of the hosting provider and informed law enforcement.

Comment: *Zeus is a common trojan virus used by cyber criminals to gain access to computers and recruit them for botnets. It has evolved over time and proven to be very resilient. The international community keeps a reasonably up to date map of computers infected with this virus, called the "Zeus Tracker". Organizations are encouraged to check this map periodically to see if they are inadvertently hosting the Zeus virus.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonated Canadian financial institutions and tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in Russia, France, Vietnam, Germany and the U.S. Almost half of the phishing attempts originated from the U.S. The entity linked to the German website spoofed two different well known Canadian banks.

CCIRC notified the Phishing Intake Centres of the impersonated financial institutions. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website defacements. CCIRC discovered a provincial department of health's website was defaced. This was also observed by the local IT staff and mitigated before any loss of personal data or content occurred. Similarly, the websites of a first nation's health organization, an educational institution and student/community organization, were defaced.

CCIRC notified all the relevant technical contacts in each situation and offered mitigation advice where required.

> ***Comment:*** *Many websites have built-in technical vulnerabilities from the design stage. Website vulnerabilities such as cross-site scripting are well known to hackers. CCIRC is seeing instances where websites are scanned for well-known vulnerabilities with automated tools and lists of the vulnerable websites posted online.*
>
> *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

Federal Government Sector

Fraudulent Government of Canada website is malicious. A malicious website, spoofing a federal government department, solicited sensitive private information from computer users. It is unknown whether any information was given by users. This website was hosted in the U.S.

CCIRC contacted the Internet Service Provider hosting the website and requested remedial action. CCIRC also requested CIRA help deactivate this fraudulent domain and informed US CERT. While the malicious content from this website has now been removed, the website itself is still accessible by Internet users. CCIRC continues to work on this case.

Government of Canada Agency logo used in on-line extortion case. Cyber criminals, impersonating a Government of Canada agency, caused extortion messages to appear on some users' computers. The messages informed users that they were "caught" looking at child porn and that their internet access would be shut down immediately unless a ransom was paid. CCIRC has passed this case to Law Enforcement for investigation.

> ***Comment:*** *Trusted entities are frequently impersonated by cyber criminals for fraud purposes. At the time of this writing, the same scheme was being perpetrated outside Canada where cyber criminals impersonated Scotland Yard.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

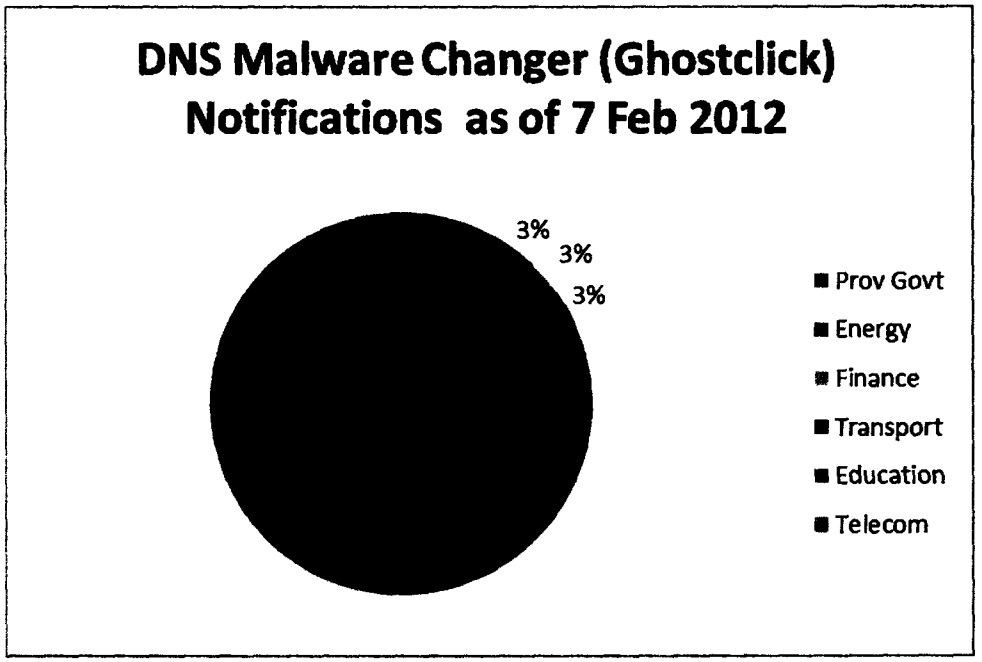
Ghostclick Fraud – DNS Changer malicious software. There were new and continued reports of infected computers in the provincial government, energy, finance, health, transportation, educational and telecommunication sectors.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012 {March 8 or 31st??) There are reports that the deadline may be extended to July 2012.

Canadians may now check to see if their computers have been affected by clicking on www.dns-ok.ca. This website, the result of a CCIRC-CIRA cooperation, is hosted by CIRA. Canada is now one of the four countries in the world that offer such a website to their citizens and the world.

Operation Ghostclick in Canada – as seen by CCIRC

- Initial count: 20,481
- Current count: 16,671
- 11th in 54 countries with more than 1000 IPs
- Most improved: Universities



While 65% of the remaining infections seen by CCIRC in Canada are traced to the telecommunications companies, it is more than likely that it is the companies' customers' computers that remain infected. These telecommunications companies provide Internet service to corporate and individual clients.

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in.

NOTEWORTHY NEWS IN THE MEDIA:

Hacker Group Anonymous releases FBI conference call recording and hacks DHS website. As what is widely presumed to be a resumption of Anonymous's Operation against law enforcement, the hacker group eavesdropped on an internal conference call at the FBI. The recording of that call was then released publicly. FBI has confirmed the recording was authentic. The hacker group was able to accomplish this by obtaining the conference call information e-mail sent to invited participants.

Anonymous also took credit for hacking of US Department of Homeland Security's website. Though this happened on the same Friday as the event above, the exact reason is unknown. The DHS website was back online within minutes of the incident.

The French Government website is hacked by Anonymous. The reason given for this hacking was opposition to ACTA, the controversial Anti-Counterfeiting Trade Agreement (ACTA). The same week, hundreds of people across 36 cities in France demonstrated against ACTA. The European Parliament has not yet ratified this agreement but 22 members of the EU, including France, have signed on. Canada has also signed ACTA.

Hackers in Europe release names of persons involved with hate movements, including 74 Canadians. The identities were revealed on a website called Nazi Leaks, which is now offline.

The UN website is hacked. TeamPoison, a hacker group loosely associated with Anonymous, hacked the UN's website. Though the group cited they were for "freedom on the internet" (sic), the exact reason was unclear.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

OUR ORGANIZATION

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest.

CCIRC operates in conjunction with the Government Operations Centre within Public Safety Canada, and is a key component of the government's all-hazards approach to emergency management and national security.

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Slack, Jessica

From: Slack, Jessica on behalf of PS Media Relations / Relations médias SP
Sent: June-19-12 9:12 AM
To: Swift, Andrew (Andrew.Swift@ps-sp.gc.ca)
Subject: FW: RCMP

E-mail address is [redacted]
I googled the address but didn't see anything very relevant/telling.

s.19(1)

From: [redacted]
Sent: June-18-12 11:30 PM
To: PS Media Relations / Relations médias SP
Subject: RCMP

Hi Julie,

You should really keep your nose out of the RCMP's businss. I know [redacted] but here in Canada our politicians keep their nose out of the RCMP's business. Understand? If they fucked up - which they did (and everybody knows it), then the families that suffered deserve an apology, not some watered down excuse aimed at diminishing their guilt. That's just lame and weak.....we want leaders in this country, not douchebags like your boss.

Bye the way, your $90million investment into cyber security won't do a thing. You can throw all the $$ in the world at it, but unless you have the right people working, its all for nothing. And trust me, none of them want to work for a bunch of corrupt and perverted politicians.....but they (Anonymous) are watching - probably you too.....that you can pretty much bet on.

ps, does the Minister know of any babysitters? Neighbour is looking to go out for the night:)

Swift, Andrew

From: Julie Gagnon <julie.gagnon@rcmp-grc.gc.ca>
Sent: Tuesday, June 19, 2012 12:19 PM
To: Swift, Andrew; Derek Cefaloni; Greg Cox; Marc Richer
Cc: Wilson, Barbara; Champoux, Martin; Durand, Stéphanie
Subject: Re: FW: Anonymous arrested? Six nabbed for cyber attacks on Quebec websites...
Attachments: Communiqué-DEME-2 (2)_2.doc

Categories: ATI PRINT

SQ was the lead for this matter and RCMP only assisted. Please see attached news release sent out by SQ.

Julie

>>> "Swift, Andrew" <Andrew.Swift@ps-sp.gc.ca> 6/19/2012 11:34 AM >>>

Marc/Greg/Julie,
See story below. Do you have any further details on the role of the RCMP?
Andrew

****

Jun 19 2012 10:51:00 - Source: CP [The Canadian Press]

Anonymous arrested? Six nabbed for cyber attacks on Quebec websites (Que-Cyber-Attacks) MONTREAL _ Six people have been arrested in connection with attacks that paralyzed Quebec websites.

The arrests were made in an operation that involved five police forces _ the **>RCMP<**, the Surete du Quebec, and three municipal forces.

Members of the group are expected to face a variety of charges, including mischief, conspiracy, and unlawful use of a computer.
Three of them are minors.

The arrests took place in Rimouski, Sherbrooke, Forestville, Montreal and Longueuil, Que.

Police are saying little else _ such as whether those arrested are suspected of acting under the guise of the activist group Anonymous, or what websites they're accused of attacking.

In an act of opposition to the province's protest law, self-described members of Anonymous have hacked into a variety of websites linked to the Quebec government _ including the province's education and public-safety departments, as well as that of the provincial Liberal party.

Those charged will appear via videoconference before a judge at Montreal's courthouse.

``Police authorities want to indicate that they take this kind of crime very seriously,'' the police said in a statement.

``They will use every means at their disposition to find the authors. These people expose themselves to criminal charges, regardless of whatever intention prompted their action.''

The police offered no other clues about the case, other than to say the attacks were on ``public'' and ``parapublic'' websites. They said they did not want to jeopardize their ongoing case by sharing details.

INDEX: NATIONAL JUSTICE POLITICS
Visit thecanadianpress.com for more services from The Canadian Press, Canada's trusted news leader.

COMMUNIQUÉ

POUR DIFFUSION IMMÉDIATE

Engagés dans la sécurité et le bien-être des citoyens !

Le 19 juin 2012

Objet : Arrestations liées aux cyber-attaques contre des sites publics

Ce matin la Sûreté du Québec, en collaboration avec les services de police de Montréal, de Laval, de Longueuil et de la Gendarmerie royale du Canada, a procédé à six arrestations et six perquisitions en lien avec les attaques informatiques perpétrées depuis le 18 mai dernier contre des sites publics et parapublics.

Ces arrestations ont eu lieu à Rimouski, Sherbrooke, Forestville, Montréal et Longueuil.

Ces individus, dont trois jeunes d'âge mineur, pourraient faire face à des accusations de méfaits, de méfaits sur des données, d'utilisation non autorisée d'un ordinateur et de complot. Ils devraient comparaître par vidéoconférence devant un juge du palais de justice de Montréal.

Les autorités policières indiquent qu'elles prennent ce genre de crimes très au sérieux et qu'elles déploient tous les moyens à leur disposition pour en retracer les auteurs. Ces derniers s'exposent à des accusations criminelles, quelle que soit l'intention derrière leur geste.

D'ailleurs, afin de mener à bien cette enquête, la Sûreté du Québec a mis sur pied une équipe intégrée composée du Service de police de la Ville de Montréal, du Service de la protection des citoyens de Laval, du Service de police de la Ville de Longueuil et de la Gendarmerie royale du Canada.

La Sûreté du Québec tient également à souligner la collaboration du CERT/AQ, qui s'occupe de la sécurité informatique de l'administration québécoise. Cet organisme relève du Centre des services partagés du Québec.

À noter qu'aucune autre communication ne sera faite dans ce dossier pour ne pas nuire à l'enquête en cours.

- 30-

Service des communications avec les médias
Sûreté du Québec
Montréal
514 598-4848
www.sq.gouv.qc.ca

1701, rue Parthenais, Montréal (Québec) H2K 3S7 Tél.: 514 598-4848 Télécopieur : 598-4917

Swift, Andrew

From: Clow, Patrick
Sent: Wednesday, June 20, 2012 7:31 AM
To: Swift, Andrew; Anderson, Windy; Dick, Robert
Cc: Durand, Stéphanie; Champoux, Martin; Wilson, Barbara
Subject: RE: Anonymous arrested? Six nabbed for cyber attacks on Quebec websites...

Categories: ATI PRINT

Good morning Andrew,

We do not believe there will be implications of significance on CCIRCs work. With respect to hacktivist activity targeting Québec government web sites, notifications were sent in May to the provincial Computer Emergency Response Team (CERT/AQ) as a mitigative action in line with our mandate. CCIRC was not involved in the investigative process related to these arrests.

Thank you

Patrick Clow, CISSP
Manager, Technical Services | Gestionnaire, Services Techniques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-944-4074 Facsimile | Télécopieur +1 613-991-3574 Patrick.Clow@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Swift, Andrew
Sent: June-19-12 11:45 AM
To: Anderson, Windy; Clow, Patrick; Dick, Robert
Cc: Durand, Stéphanie; Champoux, Martin; Wilson, Barbara
Subject: FW: Anonymous arrested? Six nabbed for cyber attacks on Quebec websites...

Windy/Patrick/Robert,
Just following up on the wire story below. I've sent a note to RCMP for details on their involvement. Can you advise of any implications on your directorate's work?
Andrew

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques Communications Directorate | Direction générale des communications Public Safety Canada | Sécurité publique Canada Telephone | Téléphone : 613-991-3549 Fax | Télécopieur : 613-954-2000 Email | Courriel : Andrew.Swift@ps-sp.gc.ca

Jun 19 2012 10:51:00 - Source: CP [The Canadian Press]

Anonymous arrested? Six nabbed for cyber attacks on Quebec websites (Que-Cyber-Attacks)

MONTREAL _ Six people have been arrested in connection with attacks that paralyzed Quebec websites.

The arrests were made in an operation that involved five police forces _ the **>RCMP<**, the Surete du Quebec, and three municipal forces.

Members of the group are expected to face a variety of charges, including mischief, conspiracy, and unlawful use of a computer.
Three of them are minors.

The arrests took place in Rimouski, Sherbrooke, Forestville, Montreal and Longueuil, Que.

Police are saying little else _ such as whether those arrested are suspected of acting under the guise of the activist group Anonymous, or what websites they're accused of attacking.

In an act of opposition to the province's protest law, self-described members of Anonymous have hacked into a variety of websites linked to the Quebec government _ including the province's education and public-safety departments, as well as that of the provincial Liberal party.

Those charged will appear via videoconference before a judge at Montreal's courthouse.

``Police authorities want to indicate that they take this kind of crime very seriously,'' the police said in a statement.

``They will use every means at their disposition to find the authors. These people expose themselves to criminal charges, regardless of whatever intention prompted their action.''

The police offered no other clues about the case, other than to say the attacks were on ``public'' and ``parapublic'' websites. They said they did not want to jeopardize their ongoing case by sharing details.

INDEX: NATIONAL JUSTICE POLITICS
Visit thecanadianpress.com for more services from The Canadian Press, Canada's trusted news leader.

Slack, Jessica

From: Matz, Mark
Sent: August-16-12 12:16 PM
To: Slack, Jessica; Clow, Patrick; Dick, Robert; Weir, Sarah; Fortunato, Stephanie
Cc: Filipps, Lisa
Subject: RE: DDoS attacks - [redacted] - PostMedia - URGENT

Thanks Jessica – we're on it, and will get back to you by 2!

Yours ever, mark

From: Slack, Jessica
Sent: August-16-12 12:04 PM
To: Matz, Mark; Clow, Patrick; Dick, Robert; Weir, Sarah; Fortunato, Stephanie
Cc: Filipps, Lisa
Subject: FW: DDoS attacks - [redacted] - PostMedia - URGENT
Importance: High

Good morning – see request below from Postmedia. You will likely have seen the story that ran this morning re a SSC ATI release (below for reference).

Not sure that we would/could confirm what the reporter is asking.

Please let me know and if not, please advise if you agree with the response below – I've kept it rather brief as I know this reporter is aware of the Strategy and these are our most recent lines about it.

Grateful for a response by 2 p.m. as reporter's deadline is 4.

Many thanks,
Jessica

PROPOSED RESPONSE:

We do not comment nor provide details on security-related incidents.

That said, there are measures in place to address cyber incidents.

Since the release of the Cyber Security Strategy, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents. In 2011, we introduced Government IT Shared Services initiative to transform the way government manages IT telecommunications, desktop computer services, data centres, IT security services and consolidates Internet access points.

From: Ted Francis [mailto:Ted.Francis@ssc-spc.gc.ca]
Sent: August-16-12 11:22 AM
To: Slack, Jessica
Subject: DDoS attacks - [redacted] - PostMedia

Hey Jessica,

As discussed, please confirm if you would like to work together on this response or if PS will take the lead.

"Just wanted to confirm that I would be receiving some answers today. Also wanted to confirm the number of targeted cyber attacks on government systems monthly/daily. I understood that there are thousands of incidents monthly, but just wanted to confirm the accuracy of that number. I just want to be able to put the two successful attacks into context and having an overall number from Shared Services Canada would be really helpful. Let me know what time today you think I would be able to receive a response. My deadline is again 4 p.m., and I'm not sure I'll have as much leeway as yesterday. (Ironically, we're having technical problems today and we're short on bodies for editing.)
Thanks again for all your help."

Thanks

Ted Francis
Media Relations | Relations avec les medias
Shared Services Canada | Services Partagés Canada
613-996-0478
434 Queen Street
PO Box 9808 STN T CSC
Ottawa, Ontario
K1G 4A8
ted.francis@ssc-spc.gc.ca

Hacker group Anonymous blamed for parliamentary website outage System went down in mid-February JORDAN PRESS, Postmedia News

A group of online hacktivists took down the parliamentary website earlier this year, striking after the government introduced a controversial online surveillance bill.

IT security staff with Shared Services Canada identified the group known as Anonymous as being behind the attack that shut down the House of Commons website for more than four hours in mid-February, according to documents released to Postmedia News under access to information laws.

When the outage happened on Feb. 17, right in the midst of an online outcry over the government's anti-cybercrime legislation, staff in the House of Commons wouldn't say publicly why the website was down.

"As you may be aware, parl. gc.ca is currently under an Anonymous DDoS (distributed denial of service) attack," reads an unsigned email sent Feb. 17 to Stephan Aube, the chief information officer for the House of Commons.

A DDoS attack occurs when online users hijack computers to flood a website with traffic and overload its server to bring down or slow down a webpage.

The documents don't say how the Commons staff determined that Anonymous was behind the attack.

"This DDoS attack against House of Commons is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," noted Shared Service Canada IT operations worker Denis Godin in an internal email sent in the middle of the DDoS attack. "They are also flooding his (Toews) email account @ parl.gc.ca and his (Twitter) account."

When he introduced bill C-30, Toews said opposition critics could either side with the government, or with child pornographers, a statement he later apologized for but one that caused an Internet backlash against C-30 and Toews.

A follow-up email Godin sent a few minutes later noted that someone should have known "an Internet storm was a brewing."

"I'm somewhat surprised that we weren't advised/put on (heightened) awareness."

The attack was the second successful one during the first four months of the year. The first came just two weeks earlier in February when unidentified attackers, or an attacker, struck the Canada Revenue Agency and Canada Border Services Agency web servers with a DDoS attack.

During the CRA attack, three of the attacking computers used Amazon's EC2 platform, which allows users to rent a virtual computer on the company's website from which to run programs. A fourth computer was based in Kiev, Ukraine, according to a Feb. 13 email from Ken Robinson, the CRA's senior IT security specialist.

In a letter to Postmedia News that accompanied the release of the documents, Shared Services Canada said that "no other attacks against government of Canada IT systems were successful and at no time was the integrity of government of Canada information holdings compromised."

In the Anonymous attack, federal cyber-security workers came up with a "workaround," according to the incident report, to partially restore service before a permanent solution could be found.

According to the series of emails and incident reports, the DDoS attacks started early on the morning of Feb. 17 and affected House of Commons servers from 6: 26 a.m. until 2 p.m. House of Commons users, including every member of Parliament, had service problems until 2: 45 p.m.

Cyber-security staff used "filters" to block out the attacking computers, but had to block access to the parl.gc.ca website to keep its systems from crashing.

"We will stay on 'high alert' all week-end and ready to reapply the filters if required," wrote Patrice Nadeau, a cyber-security worker with Shared Services Canada, after the Feb. 17 attack was over.

The attack on Canada's parliamentary website was one of a series of distributed denial of service attacks the online movement carried out in the early part of 2012.

Anonymous claimed responsibility for taking down the websites of the Federal Bureau of Investigation, the Central Intelligence Agency, and the U.S. justice department among others, in the days before allegedly attacking the Canadian government's website. ILLUS: REUTERS FILE / The February attack against the House of Commons website "is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," reads an internal email sent from IT security staff.;

Slack, Jessica

From: MARIE-HELENE.ROUILLARD@forces.gc.ca
Sent: August-16-12 12:44 PM
To: Slack, Jessica
Subject: RE: Postmedia story this morning

Just got back to the office.

I believed Ted has spoke to you about this.

I will be replacing Ted for the upcoming two weeks starting next Monday. If you require anything, please send an email to Ted, as I will be seating at his desk.

Thanks

-----Message d'origine-----
De : Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Envoyé : Thursday, 16, August, 2012 09:39 AM À : Rouillard MH@ADM(PA)@Ottawa-Hull Objet : Postmedia story this morning

Hi Marie-Helene,

I left you a voicemail this morning regarding the story below.

Grateful if you could share any lines you may have prepared for the release of the ATI.

In addition, could I ask you to please ensure that whenever possible, we be given a heads-up about releases such as this? An e-mail to our media inbox would ensure the media relations team here at PS would be informed. For ease of reference, that is media@ps-sp.gc.ca.

Thanks so much!
Jessica

Jessica Slack
Media Relations
613-949-4288

Hacker group Anonymous blamed for parliamentary website outage System went down in mid-February JORDAN PRESS, Postmedia News

A group of online hacktivists took down the parliamentary website earlier this year, striking after the government introduced a controversial online surveillance bill.

IT security staff with Shared Services Canada identified the group known as Anonymous as being behind the attack that shut down the House of Commons website for more than four hours in mid-February, according to documents released to Postmedia News under access to information laws.

When the outage happened on Feb. 17, right in the midst of an online outcry over the government's anti-cybercrime legislation, staff in the House of Commons wouldn't say publicly why the website was down.

"As you may be aware, parl. gc.ca is currently under an Anonymous DDoS (distributed denial of service) attack," reads an unsigned email sent Feb. 17 to Stephan Aube, the chief information officer for the House of Commons.

A DDoS attack occurs when online users hijack computers to flood a website with traffic and overload its server to bring down or slow down a webpage.

The documents don't say how the Commons staff determined that Anonymous was behind the attack.

"This DDoS attack against House of Commons is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," noted Shared Service Canada IT operations worker Denis Godin in an internal email sent in the middle of the DDoS attack. "They are also flooding his (Toews) email account @ parl.gc.ca and his (Twitter) account."

When he introduced bill C-30, Toews said opposition critics could either side with the government, or with child pornographers, a statement he later apologized for but one that caused an Internet backlash against C-30 and Toews.

A follow-up email Godin sent a few minutes later noted that someone should have known "an Internet storm was a brewing."

"I'm somewhat surprised that we weren't advised/put on (heightened) awareness."

The attack was the second successful one during the first four months of the year. The first came just two weeks earlier in February when unidentified attackers, or an attacker, struck the Canada Revenue Agency and Canada Border Services Agency web servers with a DDoS attack.

During the CRA attack, three of the attacking computers used Amazon's EC2 platform, which allows users to rent a virtual computer on the company's website from which to run programs. A fourth computer was based in Kiev, Ukraine, according to a Feb. 13 email from Ken Robinson, the CRA's senior IT security specialist.

In a letter to Postmedia News that accompanied the release of the documents, Shared Services Canada said that "no other attacks against government of Canada IT systems were successful and at no time was the integrity of government of Canada information holdings compromised."

In the Anonymous attack, federal cyber-security workers came up with a "workaround," according to the incident report, to partially restore service before a permanent solution could be found.

According to the series of emails and incident reports, the DDoS attacks started early on the morning of Feb. 17 and affected House of Commons servers from 6: 26 a.m. until 2 p.m. House of Commons users, including every member of Parliament, had service problems until 2: 45 p.m.

Cyber-security staff used "filters" to block out the attacking computers, but had to block access to the parl.gc.ca website to keep its systems from crashing.

"We will stay on 'high alert' all week-end and ready to reapply the filters if required," wrote Patrice Nadeau, a cyber-security worker with Shared Services Canada, after the Feb. 17 attack was over.

The attack on Canada's parliamentary website was one of a series of distributed denial of service attacks the online movement carried out in the early part of 2012.

Anonymous claimed responsibility for taking down the websites of the Federal Bureau of Investigation, the Central Intelligence Agency, and the U.S. justice department among others, in the days before allegedly attacking the Canadian government's website. ILLUS: REUTERS FILE / The February attack against the House of Commons website "is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," reads an internal email sent from IT security staff.;

Slack, Jessica

From: Ted Francis <Ted.Francis@ssc-spc.gc.ca>
Sent: August-16-12 1:31 PM
To: Slack, Jessica
Subject: RE: DDoS attacks - [redacted] - PostMedia

Jessica,

A quick question, I've attached the questions we received from [redacted] yesterday...We are still working on these responses, but I waned to know if responding to Q4 is something that PS would normally tackle?

Postmedia News
[redacted]
Twitter.com/ [redacted]

Call received: Wednesday, August 15, 2012 at 9:30
Deadline: Wednesday, August 15, 2012 by 16:00

Context:
The reporter is working on a story regarding the two DDoS attacks in February on the CRA and the parl.gc.ca server. I wanted to confirm:

Response:

Q1. What work Allstream is contracted to perform;
Q2. How much the contracts are worth (I've seen a few on the proactive disclosure list);
Q3. Whether the company is still contracted?
Q4. Also, I'm hoping to get some comment about under what circumstances would Shared Services Canada or any other department responsible for cybersecurity be told by the government to be on high alert for potential targeted cyber attacks?

Q5. There is a mention of an "Anonymous DDoS" attack on the parl.gc.ca site on Feb. 17. Just wanted to confirm that "Anonymous," which is capitalized in both English and French, refers to the online collective and not to unknown attackers.

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: Thursday, August 16, 2012 11:48 AM
To: Ted Francis
Subject: RE: DDoS attacks - [redacted] - PostMedia

For sure!

From: Ted Francis [mailto:Ted.Francis@ssc-spc.gc.ca]
Sent: August-16-12 11:47 AM

To: Slack, Jessica
Subject: RE: DDoS attacks - [redacted] - PostMedia

Jessica,

Would you mind sharing the response with us before sending it to the reporter?

Thanks

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: Thursday, August 16, 2012 11:43 AM
To: Ted Francis
Subject: RE: DDoS attacks [redacted] - PostMedia

Our media inbox is media@ps-sp.gc.ca
Do you have [redacted] e-mail address???

From: Ted Francis [mailto:Ted.Francis@ssc-spc.gc.ca]
Sent: August-16-12 11:42 AM
To: Slack, Jessica
Subject: RE: DDoS attacks - [redacted] - PostMedia
Jessica,
What PS contact information should we provide to the reporter..
Here is the reporter's information:
Postmedia News
[redacted]
Twitter.com [redacted]
[redacted]

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: Thursday, August 16, 2012 11:28 AM
To: Ted Francis
Subject: RE: DDoS attacks - [redacted] - PostMedia

Hi Ted,
We can respond. Please send over reporter's contact info and we will get in touch to let [redacted] know we will be responding...
We will provide some high-level info re Cyber Security Strategy...
Jessica

From: Ted Francis [mailto:Ted.Francis@ssc-spc.gc.ca]
Sent: August-16-12 11:22 AM
To: Slack, Jessica
Subject: DDoS attacks - [redacted] - PostMedia
Hey Jessica,
As discussed, please confirm if you would like to work together on this response or if PS will take the lead.

"Just wanted to confirm that I would be receiving some answers today. Also wanted to confirm the number of targeted cyber attacks on government systems monthly/daily. I understood that there are thousands of incidents monthly, but just wanted to confirm the accuracy of that number. I just want to be able to put the two successful attacks into context and having an overall number from Shared Services Canada would be really helpful. Let me know what time today you think I would be able to receive a response. My deadline is again 4 p.m., and I'm not sure I'll have as much leeway as yesterday. (Ironically, we're having technical problems today and we're short on bodies for editing.)
Thanks again for all your help."

Thanks

Ted Francis
Media Relations | Relations avec les medias
Shared Services Canada | Services Partagés Canada
613-996-0478
434 Queen Street
PO Box 9808 STN T CSC
Ottawa, Ontario
K1G 4A8
ted.francis@ssc-spc.gc.ca

Slack, Jessica

From: Filipps, Lisa
Sent: August-16-12 1:41 PM
To: Slack, Jessica
Subject: FW: Trapwire

From: Durand, Stéphanie
Sent: Thursday, August 16, 2012 1:34 PM
To: Filipps, Lisa
Subject: Fw: Trapwire

Fyi

From: Marc Richer [mailto:Marc.Richer@rcmp-grc.gc.ca]
Sent: Thursday, August 16, 2012 12:47 PM
To: Carmichael, Julie; Johnson, Mark
Cc: Durand, Stéphanie; Lavoie, Daniel; Greg Cox <Greg.Cox@rcmp-grc.gc.ca>; Karyn Curtis <karyn.curtis@rcmp-grc.gc.ca>; Steven Dunn <Steven.Dunn@rcmp-grc.gc.ca>
Subject: RE: Trapwire

Julie/Mark,

After extensive discussion, the RCMP's response is slightly modified, but essentially the same.

- the RCMP complies with all legislation and policies , however we will not confirm nor deny the use of a specific technique.

We have no new media calls since the TStar on Tuesday.

Marc

>>> "Carmichael, Julie" <Julie.Carmichael@ps-sp.gc.ca> 2012-08-16 10:00 >>>
Marc,

Do you have an update on this? s.21(1)(b)

You'll notice several stories in the media today on this - [redacted] My understanding is the latter.

Can you please confirm and let me how this will be communicated to the outlets who are reporting on this.

Thanks,

Julie

-----Original Message-----
From: Marc Richer [mailto:Marc.Richer@rcmp-grc.gc.ca]
Sent: August-15-12 9:04 PM
To: Johnson, Mark; Karyn Curtis
Cc: Carmichael, Julie; Greg Cox; Steven Dunn
Subject: Re: Trapwire

Fyi

Partial discussion this evening with operational sector, will continue in the am .

Will update tomorrow.

-----Original Message-----
From: "Johnson, Mark" <Mark.Johnson@ps-sp.gc.ca>
To: Richer, Marc <Marc.Richer@rcmp-grc.gc.ca>
Cc: Dunn, Steven <Steven.Dunn@rcmp-grc.gc.ca>
Cc: Cox, Greg <Greg.Cox@rcmp-grc.gc.ca>
To: Curtis, Karyn <karyn.curtis@rcmp-grc.gc.ca>
Cc: Carmichael, Julie <Julie.Carmichael@ps-sp.gc.ca>

Sent: 08/15/2012 19:57:53
Subject: Re: Trapwire

Thx

----- Original Message -----
From: Marc Richer [mailto:Marc.Richer@rcmp-grc.gc.ca]
Sent: Wednesday, August 15, 2012 07:54 PM
To: Johnson, Mark; Karyn Curtis <karyn.curtis@rcmp-grc.gc.ca>
Cc: Carmichael, Julie; Greg Cox <Greg.Cox@rcmp-grc.gc.ca>; Steven Dunn <Steven.Dunn@rcmp-grc.gc.ca>
Subject: Re: Trapwire

Following up.
Will get back to you

-----Original Message-----
From: "Johnson, Mark" <Mark.Johnson@ps-sp.gc.ca>
To: Richer, Marc <Marc.Richer@rcmp-grc.gc.ca>
Cc: Dunn, Steven <Steven.Dunn@rcmp-grc.gc.ca>
To: Curtis, Karyn <karyn.curtis@rcmp-grc.gc.ca>
Cc: Carmichael, Julie <Julie.Carmichael@ps-sp.gc.ca>

Sent: 08/15/2012 19:44:54
Subject: Re: Trapwire

Now with the story:

Trapwire is watching you in Ottawa
by Jesse Brown on Wednesday, August 15, 2012 5:46pm -

Have you heard of Trapwire? It's a formerly obscure counter-terrorist surveillance network, created by a company run by ex-CIA agents, that links together thousands of ordinary, privately owned security cameras, digitally analyzing the footage they generate and delivering it to various police departments and branches of the U.S. federal government. It's been making headlines in the U.S. since Wikileaks exposed its existence, and online chatter has been obsessively focused on it ever since. There's been endless analysis, opinion, misinformation and clarification (here's a credible run-down of the story so far). Everyone from NBC to Anonymous is talking about it, but the Canadian media has yet to take notice. Which is surprising, since Trapwire is apparently live in Ottawa.

Wikileaks has leaked emails from private security firm Stratfor, who market Trapwire. One of them, written by Stratfor vice president Fred Burton, says:

"Trapwire is in place at every HVT in NYC, DC, London, Ottawa and LA."

In U.S. Military parlance, an HVT is a "high-value target," like a federal government building, a military structure or a travel hub. Ottawa has lots of those, and apparently they all house cameras that are spying on Canadians and feeding the footage to Trapwire.

Trapwire's menace has been overhyped. It does not collect facial recognition data, as has been rumoured. Neither does it allow authorities to track individuals as they move from camera site to camera site. These myths have been debunked, as journalists and security analysts learn more about what the Trapwire network does in fact do. Nevertheless, the language around is, admittedly, fuzzy. Trapwire claims to "detect patterns of behavior indicative of pre-operational planning." What does this mean? Does Trapwire watch for individuals who visit and stake out several possible targets? How can it tell them apart from sight-seeing tourists? What exactly indicates "pre-operational planning"? Have there been enough terrorist operations to provide a viable dataset on which Trapwire can base its scrutiny? The mechanics and effectiveness of the system is very much in doubt.

Regardless of whether or not Trapwire works, it's still a cause for concern. By piggybacking on privately owned cameras and linking them to government authorities, Trapwire circumvents privacy laws and law enforcement protocols. Annalee Newitz at Gawker's i09 blog argues persuasively that the whole thing probably violates U.S. Constitutional law. Noah Scachtman at Wired documents the sleazy dealings between Trapwire and Stratfor as they colluded to sell expensive licenses (starting at $20,000) to government agencies and private clients.

Add to this the one crucial question for us Canadians. If Trapwire's activity does indeed extend to Ottawa, who's on the receiving end of the data flow? Is it our government or is Homeland Security spying on Canadians as well?

----- Original Message -----
From: Johnson, Mark
Sent: Wednesday, August 15, 2012 07:43 PM
To: 'Marc.Richer@rcmp-grc.gc.ca' <Marc.Richer@rcmp-grc.gc.ca>; 'karyn.curtis@rcmp-grc.gc.ca' <karyn.curtis@rcmp-grc.gc.ca>
Cc: 'Steven.Dunn@rcmp-grc.gc.ca' <Steven.Dunn@rcmp-grc.gc.ca>; Carmichael, Julie
Subject: Re: Trapwire

Adding Julie for awareness. See the story below.

s.21(1)(b)

----- Original Message -----
From: Johnson, Mark
Sent: Wednesday, August 15, 2012 07:24 PM
To: 'Marc.Richer@rcmp-grc.gc.ca' <Marc.Richer@rcmp-grc.gc.ca>; 'karyn.curtis@rcmp-grc.gc.ca' <karyn.curtis@rcmp-grc.gc.ca>
Cc: 'Steven.Dunn@rcmp-grc.gc.ca' <Steven.Dunn@rcmp-grc.gc.ca>
Subject: Re: Trapwire

----- Original Message -----

From: Marc Richer [mailto:Marc.Richer@rcmp-grc.gc.ca]
Sent: Wednesday, August 15, 2012 07:04 PM
To: Johnson, Mark; Karyn Curtis <karyn.curtis@rcmp-grc.gc.ca>
Cc: Steven Dunn <Steven.Dunn@rcmp-grc.gc.ca>
Subject: Re: Trapwire

s.21(1)(b)

Mark

[redacted]

Response: In general, due to security considerations, we would not discuss or confirm/deny which technologies and/or systems we may or may not be employing.

Marc Richer, Insp
Acting Director General | Directeur Général intérimaire National Communication Services | Services nationaux de communication Royal Canadian Mounted Police |Gendarmerie Royale du Canada
73 promenade Leikin Drive
Ottawa, ON K1A 0R2
613 843 4561

From wireless/de sans fil
-----Original Message-----
From: "Johnson, Mark" <Mark.Johnson@ps-sp.gc.ca>
Cc: Richer, Marc <Marc.Richer@rcmp-grc.gc.ca>
Cc: Dunn, Steven <Steven.Dunn@rcmp-grc.gc.ca>
To: Curtis, Karyn <karyn.curtis@rcmp-grc.gc.ca>

Sent: 08/15/2012 18:54:33
Subject: Re: Trapwire

Yes. I saw this in the media.

I'm just letting you know what we will say, and want to make sure all are on the same page.

----- Original Message -----
From: Karyn Curtis [mailto:karyn.curtis@rcmp-grc.gc.ca]
Sent: Wednesday, August 15, 2012 06:40 PM
To: Johnson, Mark
Cc: Marc Richer <Marc.Richer@rcmp-grc.gc.ca>; Steven Dunn <Steven.Dunn@rcmp-grc.gc.ca>
Subject: Re: Trapwire

Mark, Comms advises that the following media response was provided to PS Comms yesterday:
s.19(1)
Reporter: [redacted] Toronto Star
Issue: Would like to know if the rumours on WikiLeaks are founded in that the RCMP is allegedly using technology called 'TrapWire'
Response: In general, due to security considerations, we would not discuss or confirm/deny which technologies and/or systems we may or may not be employing.

Cheers.
KC

-----Original Message-----
From: "Johnson, Mark" <Mark.Johnson@ps-sp.gc.ca>
Cc: Dunn, Steven <Steven.Dunn@rcmp-grc.gc.ca>
To: Curtis, Karyn <karyn.curtis@rcmp-grc.gc.ca>

Sent: 08/15/2012 17:03:32
Subject: Trapwire

s.21(1)(b)

Hi Karyn,

See the story below on Trapwire. [redacted]

Thanks,

Mark

Privacy Commissioner keeping a watchful eye on Wikileak'd #Trapwire alleged revelations by Kady O'Malley<http://www.cbc.ca/news/politics/inside-politics-blog/author/kady-omalley/> Posted: August 15, 2012 3:12 PM Last Updated: August 15, 2012 3:39 PM

For those who wondered whether Canada's privacy defender in chief Jennifer Stoddart is paying attention to the latest Wikileaks-triggered controversy over the contents of hundreds of leaked emails that allegedly originated with US-based intelligence gathering firm Stratfor<http://io9.com/5933966/wikileaks-reveals-trapwire-a-government-spy-network-that-uses-ordinary-surveillance-cameras>, and what the Toronto Star describes<http://www.thestar.com/news/world/article/1242239--wikileaks-email-cache-reveals-intelligence-company-s-interest-in-canada> as the "possibly Orwellian" nature of Trapwire<http://www.trapwire.com/trapwire.html>, the proprietary surveillance software that may or may not be in use in Canada.

Here's what her office had to say when I asked about it:

We have read reports stemming from Wikileaks' sharing of correspondence from the subscription-based, geopolitical analysis firm Stratfor which asserted that TrapWire technology may be at use in Canada. We however have not evaluated this technology or learned of its use within Canada outside of this report of a third-party report. Our Office however is interested in initiatives that would use such surveillance technology and impact on privacy in pursuit of greater security. As a result, we will continue following developments on this story closely.

Upon sizing-up such programs, we guide our analysis by asking the organization to answer the following four questions to weigh reasonable limitations on rights and freedoms in a free and democratic society:

Is the measure demonstrably necessary to meet a specific need?
Is it likely to be effective in meeting that need?
Is the loss of privacy proportional to the need?
Is there a less privacy-invasive way of achieving the same end?

Once more, our Office will continue monitoring developments and assessing information on this issue.

They've also promised to keep me informed of any "significant developments" related to this story on their end -- and you can be assured that if and when that happens, I'll keep you in the loop, too.

Slack, Jessica

From: Fortunato, Stephanie
Sent: August-16-12 2:09 PM
To: Slack, Jessica; Matz, Mark; Clow, Patrick; Dick, Robert; Weir, Sarah
Cc: Filipps, Lisa
Subject: RE: DDoS attacks - [redacted] PostMedia - URGENT

Hi Jessica,

Robert is currently in a meeting with the A/DM until 2:45pm. He may not be able to check his berry until then.

Steph

From: Slack, Jessica
Sent: August-16-12 2:08 PM
To: Matz, Mark; Clow, Patrick; Dick, Robert; Weir, Sarah; Fortunato, Stephanie
Cc: Filipps, Lisa
Subject: RE: DDoS attacks - [redacted] PostMedia - URGENT

Excellent! Can you confirm if Robert has approved?

From: Matz, Mark
Sent: August-16-12 2:06 PM
To: Slack, Jessica; Clow, Patrick; Dick, Robert; Weir, Sarah; Fortunato, Stephanie
Cc: Filipps, Lisa
Subject: RE: DDoS attacks - [redacted] - PostMedia - URGENT

Hi Jessica,

Your proposed response looks good. We would not comment on the number or types of threats that GoC face, nor indeed provide any detail on these matters since this would describe the Government's cyber capacity and may reveal information to those who are looking to penetrate GoC networks. In any case, CSEC is the lead for this kind of information and we would want to consult with them if there were ever a question of publicly releasing information.

With that said, we would suggest only minor changes to your paragraph to correct the name of Shared Services, and highlight a bit more strongly that the GoC is serious about the security of its networks.

Hope that gives you what you need! Please let us know if there's anything else.

Yours ever, mark

We do not comment nor provide details on specific security-related incidents.

That said, there are robust measures in place to address cyber incidents and ensure the resilience of Government networks.

Pages 411 to / à 413
are duplicates of
sont des duplicatas des
pages 427 to / à 429

Pages 414 to / à 416

are duplicates of

sont des duplicatas des

pages 423 to / à 425

Slack, Jessica

From: Filipps, Lisa
Sent: August-16-12 2:44 PM
To: Slack, Jessica; Manning, Kerri
Subject: FW: Trapwire

Updated line from RCMP.

-----Original Message-----
From: Marc Richer [mailto:Marc.Richer@rcmp-grc.gc.ca]
Sent: Thursday, August 16, 2012 2:43 PM
To: Carmichael, Julie; Johnson, Mark; Karyn Curtis
Cc: Filipps, Lisa; Durand, Stéphanie; Lavoie, Daniel; Greg Cox; Steven Dunn
Subject: Re: Trapwire

Updated line:

- the RCMP will not confirm nor deny the use of a specific investigative technique. Rest assured the RCMP complies with Privacy and other legislation as well as relevant policies

Marc

-----Original Message-----
From: "Carmichael, Julie" <Julie.Carmichael@ps-sp.gc.ca>
To: Richer, Marc <Marc.Richer@rcmp-grc.gc.ca>
Cc: Dunn, Steven <Steven.Dunn@rcmp-grc.gc.ca>
Cc: Cox, Greg <Greg.Cox@rcmp-grc.gc.ca>
To: Curtis, Karyn <karyn.curtis@rcmp-grc.gc.ca>
To: Johnson, Mark <Mark.Johnson@ps-sp.gc.ca>

Sent: 08/16/2012 10:00:21
Subject: RE: Trapwire

Marc,

Do you have an update on this?

s.21(1)(b)

You'll notice several stories in the media today on this [redacted]

Can you please confirm and let me how this will be communicated to the outlets who are reporting on this.

Thanks,

Julie

-----Original Message-----
From: Marc Richer [mailto:Marc.Richer@rcmp-grc.gc.ca]
Sent: August-15-12 9:04 PM

Pages 418 to / à 421

are duplicates of

sont des duplicatas des

pages 406 to / à 409

Page 422

is a duplicate of

est un duplicata de la

page 409

Dubé, Rosanne

From: Dubé, Rosanne
Sent: Thursday, August 16, 2012 2:55 PM
To: Salewski, Shawn; Bue, Richard
Subject: RE: FOR DG APPROVAL- MEDIA REQUEST -Cyber

Printed for SD

Rosanne Dubé
Administrative Officer | Agente administrative
Office of the Director General, Communications | Bureau de la Directrice générale, Communications
Public Safety Canada | Sécurité publique Canada
Ottawa, Canada K1A 0P8
Telephone | Téléphone 613 949-4485 / Facsimile | Télécopieur 613 993-7062

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Slack, Jessica
Sent: Thursday, August 16, 2012 2:29 PM
To: Durand, Stéphanie; Dubé, Rosanne; Ellis, Kelly Lynn; Salewski, Shawn; Bue, Richard
Cc: Filipps, Lisa; Manning, Kerri
Subject: FOR DG APPROVAL- MEDIA REQUEST -Cyber

Stéphanie,

Shared Services asked for assistance with one of the questions from Postmedia further to the story they ran this morning (below for reference) re Anonymous and the shut-down of the parliamentary website.

Mark Matz has approved but Robert is in a meeting with the DM for the next little while. Will advise if he requests any changes.

Reporter's deadline is 4 so quick approval is requested asap. I have shared this with SSC and CSEC. PS will respond to this question after all are comfortable.
Jessica

FOR APPROVAL:

We do not comment nor provide details on specific security-related incidents.

That said, there are robust measures in place to address cyber incidents and ensure the resilience of Government networks.

Since the release of the Cyber Security Strategy, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents. In 2011, Shared Services Canada was created to transform the way government manages telecommunications, desktop computer services, data centres, and IT security services. By streamlining the Government of Canada's computer systems and consolidating Internet access points, the Government is strengthening the security of its networks, as well as making its operations more efficient and effective.

Reporter's Name	[redacted]
Media Outlet	Post Media
Call Date	8/16/2012 1:00 PM
Telephone	
E-mail address	[redacted]@postmedia.com
Deadline	8/16/2012 4:00 PM
Status	Consulting
Branch	
Subject	DDoS attacks
Questions	"Just wanted to confirm that I would be receiving some answers today. Also wanted to confirm the number of targeted cyber attacks on government systems monthly/daily. I understood that there are thousands of incidents monthly, but just wanted to confirm the accuracy of that number. I just want to be able to put the two successful attacks into context and having an overall number from Shared Services Canada would be really helpful. Let me know what time today you think I would be able to receive a response. My deadline is again 4 p.m., and I'm not sure I'll have as much leeway as yesterday. (Ironically, we're having technical problems today and we're short on bodies for editing.) Thanks again for all your help."

Hacker group Anonymous blamed for parliamentary website outage System went down in mid-February JORDAN PRESS, Postmedia News

A group of online hacktivists took down the parliamentary website earlier this year, striking after the government introduced a controversial online surveillance bill.

IT security staff with Shared Services Canada identified the group known as Anonymous as being behind the attack that shut down the House of Commons website for more than four hours in mid-February, according to documents released to Postmedia News under access to information laws.

When the outage happened on Feb. 17, right in the midst of an online outcry over the government's anti-cybercrime legislation, staff in the House of Commons wouldn't say publicly why the website was down.

"As you may be aware, parl. gc.ca is currently under an Anonymous DDoS (distributed denial of service) attack," reads an unsigned email sent Feb. 17 to Stephan Aube, the chief information officer for the House of Commons.

A DDoS attack occurs when online users hijack computers to flood a website with traffic and overload its server to bring down or slow down a webpage.

The documents don't say how the Commons staff determined that Anonymous was behind the attack.

"This DDoS attack against House of Commons is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," noted Shared Service Canada IT operations worker Denis Godin in an internal email sent in the middle of the DDoS attack. "They are also flooding his (Toews) email account @ parl.gc.ca and his (Twitter) account."

When he introduced bill C-30, Toews said opposition critics could either side with the government, or with child pornographers, a statement he later apologized for but one that caused an Internet backlash against C-30 and Toews.

A follow-up email Godin sent a few minutes later noted that someone should have known "an Internet storm was a brewing."

"I'm somewhat surprised that we weren't advised/put on (heightened) awareness."

The attack was the second successful one during the first four months of the year. The first came just two weeks earlier in February when unidentified attackers, or an attacker, struck the Canada Revenue Agency and Canada Border Services Agency web servers with a DDoS attack.

During the CRA attack, three of the attacking computers used Amazon's EC2 platform, which allows users to rent a virtual computer on the company's website from which to run programs. A fourth computer was based in Kiev, Ukraine, according to a Feb. 13 email from Ken Robinson, the CRA's senior IT security specialist.

In a letter to Postmedia News that accompanied the release of the documents, Shared Services Canada said that "no other attacks against government of Canada IT systems were successful and at no time was the integrity of government of Canada information holdings compromised."

In the Anonymous attack, federal cyber-security workers came up with a "workaround," according to the incident report, to partially restore service before a permanent solution could be found.

According to the series of emails and incident reports, the DDoS attacks started early on the morning of Feb. 17 and affected House of Commons servers from 6: 26 a.m. until 2 p.m. House of Commons users, including every member of Parliament, had service problems until 2: 45 p.m.

Cyber-security staff used "filters" to block out the attacking computers, but had to block access to the parl.gc.ca website to keep its systems from crashing.

"We will stay on 'high alert' all week-end and ready to reapply the filters if required," wrote Patrice Nadeau, a cyber-security worker with Shared Services Canada, after the Feb. 17 attack was over.

The attack on Canada's parliamentary website was one of a series of distributed denial of service attacks the online movement carried out in the early part of 2012.

Anonymous claimed responsibility for taking down the websites of the Federal Bureau of Investigation, the Central Intelligence Agency, and the U.S. justice department among others, in the days before allegedly attacking the Canadian government's website. ILLUS: REUTERS FILE / The February attack against the House of Commons website "is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," reads an internal email sent from IT security staff.;

Slack, Jessica

From: Dick, Robert
Sent: August-16-12 3:04 PM
To: Slack, Jessica
Subject: Re: DDoS attacks - [redacted] PostMedia - URGENT

Yes. Mark's approval is all you need.

From: Slack, Jessica
Sent: Thursday, August 16, 2012 02:21 PM
To: Dick, Robert
Subject: RE: DDoS attacks - [redacted] - PostMedia - URGENT

So you approve? ☺

From: Dick, Robert
Sent: August-16-12 2:21 PM
To: Matz, Mark; Slack, Jessica; Clow, Patrick; Weir, Sarah; Fortunato, Stephanie
Cc: Filipps, Lisa
Subject: Re: DDoS attacks - [redacted] - PostMedia - URGENT

Agreed with Mark. I think there's merit to contextualizing number of probes, attempted penetrations etc, but it's a decision for csec.

From: Matz, Mark
Sent: Thursday, August 16, 2012 02:11 PM
To: Slack, Jessica; Clow, Patrick; Dick, Robert; Weir, Sarah; Fortunato, Stephanie
Cc: Filipps, Lisa
Subject: RE: DDoS attacks - [redacted] - PostMedia - URGENT

Robert's on this message, so he can reply – but generally he's indicated that my shop should take responsibility for triaging the requests; for short ones such as this, we are to go directly to you; for more complex requests, we would flag it for his direct attention.

I'll wait for my boss to confirm or deny. ☺

From: Slack, Jessica
Sent: August-16-12 2:08 PM
To: Matz, Mark; Clow, Patrick; Dick, Robert; Weir, Sarah; Fortunato, Stephanie
Cc: Filipps, Lisa
Subject: RE: DDoS attacks - [redacted] - PostMedia - URGENT

Excellent! Can you confirm if Robert has approved?

From: Matz, Mark
Sent: August-16-12 2:06 PM
To: Slack, Jessica; Clow, Patrick; Dick, Robert; Weir, Sarah; Fortunato, Stephanie
Cc: Filipps, Lisa
Subject: RE: DDoS attacks - [redacted] - PostMedia - URGENT

Hi Jessic

Your proposed response looks good. We would not comment on the number or types of threats that GoC face, nor indeed provide any detail on these matters since this would describe the Government's cyber capacity and may reveal information to those who are looking to penetrate GoC networks. In any case, CSEC is the lead for this kind of information and we would want to consult with them if there were ever a question of publicly releasing information.

With that said, we would suggest only minor changes to your paragraph to correct the name of Shared Services, and highlight a bit more strongly that the GoC is serious about the security of its networks.

Hope that gives you what you need! Please let us know if there's anything else.

Yours ever, mark

We do not comment nor provide details on specific security-related incidents.

That said, there are robust measures in place to address cyber incidents and ensure the resilience of Government networks.

Since the release of the Cyber Security Strategy, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents. In 2011, Shared Services Canada was created to transform the way government manages telecommunications, desktop computer services, data centres, and IT security services. By streamlining the Government of Canada's computer systems and consolidating Internet access points, the Government is strengthening the security of its networks, as well as making its operations more efficient and effective.

From: Slack, Jessica
Sent: August-16-12 12:04 PM
To: Matz, Mark; Clow, Patrick; Dick, Robert; Weir, Sarah; Fortunato, Stephanie
Cc: Filipps, Lisa
Subject: FW: DDoS attacks - [redacted] - PostMedia - URGENT
Importance: High

Good morning – see request below from Postmedia. You will likely have seen the story that ran this morning re a SSC ATI release (below for reference).

Not sure that we would/could confirm what the reporter is asking.

Please let me know and if not, please advise if you agree with the response below – I've kept it rather brief as I know this reporter is aware of the Strategy and these are our most recent lines about it.

Grateful for a response by 2 p.m. as reporter's deadline is 4.

Many thanks,
Jessica

PROPOSED RESPONSE:

We do not comment nor provide details on security-related incidents.

That said, there are measures in place to address cyber incidents.

Since the release of the Cyber Security Strategy, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents. In 2011, we introduced Government IT Shared Services initiative to transform the way government manages IT telecommunications, desktop computer services, data centres, IT security services and consolidates Internet access points.

From: Ted Francis [mailto:Ted.Francis@ssc-spc.gc.ca]
Sent: August-16-12 11:22 AM
To: Slack, Jessica
Subject: DDoS attacks - [redacted] - PostMedia

Hey Jessica,

As discussed, please confirm if you would like to work together on this response or if PS will take the lead.

"Just wanted to confirm that I would be receiving some answers today. Also wanted to confirm the number of targeted cyber attacks on government systems monthly/daily. I understood that there are thousands of incidents monthly, but just wanted to confirm the accuracy of that number. I just want to be able to put the two successful attacks into context and having an overall number from Shared Services Canada would be really helpful. Let me know what time today you think I would be able to receive a response. My deadline is again 4 p.m., and I'm not sure I'll have as much leeway as yesterday. (Ironically, we're having technical problems today and we're short on bodies for editing.)
Thanks again for all your help."

Thanks

Ted Francis
Media Relations | Relations avec les medias
Shared Services Canada | Services Partagés Canada
613-996-0478
434 Queen Street
PO Box 9808 STN T CSC
Ottawa, Ontario
K1G 4A8
ted.francis@ssc-spc.gc.ca

Hacker group Anonymous blamed for parliamentary website outage System went down in mid-February JORDAN PRESS, Postmedia News

A group of online hacktivists took down the parliamentary website earlier this year, striking after the government introduced a controversial online surveillance bill.

IT security staff with Shared Services Canada identified the group known as Anonymous as being behind the attack that shut down the House of Commons website for more than four hours in mid-February, according to documents released to Postmedia News under access to information laws.

When the outage happened on Feb. 17, right in the midst of an online outcry over the government's anti-cybercrime legislation, staff in the House of Commons wouldn't say publicly why the website was down.

"As you may be aware, parl. gc.ca is currently under an Anonymous DDoS (distributed denial of service) attack," reads an unsigned email sent Feb. 17 to Stephan Aube, the chief information officer for the House of Commons.

A DDoS attack occurs when online users hijack computers to flood a website with traffic and overload its server to bring down or slow down a webpage.

The documents don't say how the Commons staff determined that Anonymous was behind the attack.

"This DDoS attack against House of Commons is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," noted Shared Service Canada IT operations worker Denis Godin in an internal email sent in the middle of the DDoS attack. "They are also flooding his (Toews) email account @ parl.gc.ca and his (Twitter) account."

When he introduced bill C-30, Toews said opposition critics could either side with the government, or with child pornographers, a statement he later apologized for but one that caused an Internet backlash against C-30 and Toews.

A follow-up email Godin sent a few minutes later noted that someone should have known "an Internet storm was a brewing."

"I'm somewhat surprised that we weren't advised/put on (heightened) awareness."

The attack was the second successful one during the first four months of the year. The first came just two weeks earlier in February when unidentified attackers, or an attacker, struck the Canada Revenue Agency and Canada Border Services Agency web servers with a DDoS attack.

During the CRA attack, three of the attacking computers used Amazon's EC2 platform, which allows users to rent a virtual computer on the company's website from which to run programs. A fourth computer was based in Kiev, Ukraine, according to a Feb. 13 email from Ken Robinson, the CRA's senior IT security specialist.

In a letter to Postmedia News that accompanied the release of the documents, Shared Services Canada said that "no other attacks against government of Canada IT systems were successful and at no time was the integrity of government of Canada information holdings compromised."

In the Anonymous attack, federal cyber-security workers came up with a "workaround," according to the incident report, to partially restore service before a permanent solution could be found.

According to the series of emails and incident reports, the DDoS attacks started early on the morning of Feb. 17 and affected House of Commons servers from 6: 26 a.m. until 2 p.m. House of Commons users, including every member of Parliament, had service problems until 2: 45 p.m.

Cyber-security staff used "filters" to block out the attacking computers, but had to block access to the parl.gc.ca website to keep its systems from crashing.

"We will stay on 'high alert' all week-end and ready to reapply the filters if required," wrote Patrice Nadeau, a cyber-security worker with Shared Services Canada, after the Feb. 17 attack was over.

The attack on Canada's parliamentary website was one of a series of distributed denial of service attacks the online movement carried out in the early part of 2012.

Anonymous claimed responsibility for taking down the websites of the Federal Bureau of Investigation, the Central Intelligence Agency, and the U.S. justice department among others, in the days before allegedly attacking the Canadian government's website. ILLUS: REUTERS FILE / The February attack against the House of Commons website "is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," reads an internal email sent from IT security staff.;

Slack, Jessica

From: Slack, Jessica
Sent: August-16-12 3:42 PM
To: AkimIsabelle.Thibouthot@pco-bcp.gc.ca
Subject: FW: FOR MO APPROVAL- MEDIA REQUEST -Cyber

Hi Akim,

We are waiting on MO's approval, but wanted to check in with you. Any concerns?
Thanks,
Jessica

From: Slack, Jessica
Sent: August-16-12 3:13 PM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; AkimIsabelle.Thibouthot@pco-bcp.gc.ca
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca); Manning, Kerri; Carta, John; Champoux, Martin; Austria, Jamela; Durand, Stéphanie
Subject: FW: FOR DG APPROVAL- MEDIA REQUEST -Cyber

Julie,

SSC sent this question our way – stemming from the Postmedia story that ran this morning (below for reference). Proposed response to reporter's question re number of attacks on government systems is below-
Reporter's deadline is 4 p.m.

Jessica

FOR APPROVAL:

We do not comment nor provide details on specific security-related incidents.

That said, there are robust measures in place to address cyber incidents and ensure the resilience of Government networks.

Since the release of the Cyber Security Strategy, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents. In 2011, Shared Services Canada was created to transform the way government manages telecommunications, desktop computer services, data centres, and IT security services. By streamlining the Government of Canada's computer systems and consolidating Internet access points, the Government is strengthening the security of its networks, as well as making its operations more efficient and effective.

Reporter's Name	[redacted]
Media Outlet	Post Media
Call Date	8/16/2012 1:00 PM
Telephone	
E-mail address	[redacted]@postmedia.com
Deadline	8/16/2012 4:00 PM

Pages 431 to / à 432
are duplicates of
sont des duplicatas des
pages 434 to / à 435

Slack, Jessica

From: Carmichael, Julie
Sent: August-16-12 4:00 PM
To: Slack, Jessica
Cc: Filipps, Lisa
Subject: RE: FOR MO APPROVAL- MEDIA REQUEST -Cyber

Approved

From: Slack, Jessica
Sent: August-16-12 3:54 PM
To: Carmichael, Julie
Cc: Filipps, Lisa
Subject: FW: FOR MO APPROVAL- MEDIA REQUEST -Cyber

Just following up...thanks!

From: Slack, Jessica
Sent: August-16-12 3:13 PM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; AkimIsabelle.Thibouthot@pco-bcp.gc.ca
Cc: Filipps, Lisa (Lisa.Filipps@ps-sp.gc.ca); Manning, Kerri; Carta, John; Champoux, Martin; Austria, Jamela; Durand, Stéphanie
Subject: FW: FOR DG APPROVAL- MEDIA REQUEST -Cyber

Julie,

SSC sent this question our way – stemming from the Postmedia story that ran this morning (below for reference). Proposed response to reporter's question re number of attacks on government systems is below- Reporter's deadline is 4 p.m.

Jessica

FOR APPROVAL:

We do not comment nor provide details on specific security-related incidents.

That said, there are robust measures in place to address cyber incidents and ensure the resilience of Government networks.

Since the release of the Cyber Security Strategy, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents. In 2011, Shared Services Canada was created to transform the way government manages telecommunications, desktop computer services, data centres, and IT security services. By streamlining the Government of Canada's computer systems and consolidating Internet access points, the Government is strengthening the security of its networks, as well as making its operations more efficient and effective.

Reporter's Name [redacted]

Media Outlet Post Media

Call Date	8/16/2012 1:00 PM
Telephone	
E-mail address	[redacted]@postmedia.com
Deadline	8/16/2012 4:00 PM
Status	Consulting
Branch	
Subject	DDoS attacks
Questions	"Just wanted to confirm that I would be receiving some answers today. Also wanted to confirm the number of targeted cyber attacks on government systems monthly/daily. I understood that there are thousands of incidents monthly, but just wanted to confirm the accuracy of that number. I just want to be able to put the two successful attacks into context and having an overall number from Shared Services Canada would be really helpful. Let me know what time today you think I would be able to receive a response. My deadline is again 4 p.m., and I'm not sure I'll have as much leeway as yesterday. (Ironically, we're having technical problems today and we're short on bodies for editing.) Thanks again for all your help."

Hacker group Anonymous blamed for parliamentary website outage System went down in mid-February JORDAN PRESS, Postmedia News

A group of online hacktivists took down the parliamentary website earlier this year, striking after the government introduced a controversial online surveillance bill.

IT security staff with Shared Services Canada identified the group known as Anonymous as being behind the attack that shut down the House of Commons website for more than four hours in mid-February, according to documents released to Postmedia News under access to information laws.

When the outage happened on Feb. 17, right in the midst of an online outcry over the government's anti-cybercrime legislation, staff in the House of Commons wouldn't say publicly why the website was down.

"As you may be aware, parl. gc.ca is currently under an Anonymous DDoS (distributed denial of service) attack," reads an unsigned email sent Feb. 17 to Stephan Aube, the chief information officer for the House of Commons.

A DDoS attack occurs when online users hijack computers to flood a website with traffic and overload its server to bring down or slow down a webpage.

The documents don't say how the Commons staff determined that Anonymous was behind the attack.

"This DDoS attack against House of Commons is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," noted Shared Service Canada IT operations worker Denis Godin in an internal email sent in the middle of the DDoS attack. "They are also flooding his (Toews) email account @ parl.gc.ca and his (Twitter) account."

When he introduced bill C-30, Toews said opposition critics could either side with the government, or with child pornographers, a statement he later apologized for but one that caused an Internet backlash against C-30 and Toews.

A follow-up email Godin sent a few minutes later noted that someone should have known "an Internet storm was a brewing."

"I'm somewhat surprised that we weren't advised/put on (heightened) awareness."

The attack was the second successful one during the first four months of the year. The first came just two weeks earlier in February when unidentified attackers, or an attacker, struck the Canada Revenue Agency and Canada Border Services Agency web servers with a DDoS attack.

During the CRA attack, three of the attacking computers used Amazon's EC2 platform, which allows users to rent a virtual computer on the company's website from which to run programs. A fourth computer was based in Kiev, Ukraine, according to a Feb. 13 email from Ken Robinson, the CRA's senior IT security specialist.

In a letter to Postmedia News that accompanied the release of the documents, Shared Services Canada said that "no other attacks against government of Canada IT systems were successful and at no time was the integrity of government of Canada information holdings compromised."

In the Anonymous attack, federal cyber-security workers came up with a "workaround," according to the incident report, to partially restore service before a permanent solution could be found.

According to the series of emails and incident reports, the DDoS attacks started early on the morning of Feb. 17 and affected House of Commons servers from 6: 26 a.m. until 2 p.m. House of Commons users, including every member of Parliament, had service problems until 2: 45 p.m.

Cyber-security staff used "filters" to block out the attacking computers, but had to block access to the parl.gc.ca website to keep its systems from crashing.

"We will stay on 'high alert' all week-end and ready to reapply the filters if required," wrote Patrice Nadeau, a cyber-security worker with Shared Services Canada, after the Feb. 17 attack was over.

The attack on Canada's parliamentary website was one of a series of distributed denial of service attacks the online movement carried out in the early part of 2012.

Anonymous claimed responsibility for taking down the websites of the Federal Bureau of Investigation, the Central Intelligence Agency, and the U.S. justice department among others, in the days before allegedly attacking the Canadian government's website. ILLUS: REUTERS FILE / The February attack against the House of Commons website "is likely directly related to Public Safety Minister Vic Toews' recent and controversial appearance in the news," reads an internal email sent from IT security staff.;

Slack, Jessica

From: Slack, Jessica
Sent: August-20-12 3:41 PM
To: Greg Cox (Greg.Cox@rcmp-grc.gc.ca)
Cc: Wilson, Barbara
Subject: FW: Bloomberg News question about hacking threat

Hi Greg,

Just checking in to see if this reporter has contacted you as well??
Jessica

From: Slack, Jessica
Sent: August-20-12 2:58 PM
To: Matz, Mark; Anderson, Windy
Cc: Fortunato, Stephanie; Weir, Sarah
Subject: FW: Bloomberg News question about hacking threat

Hi Mark, Windy

See request below.

I've pulled together a few bullets as a start...can you have a look and revise as appropriate?
Grateful for a response by 10 a.m. tomorrow...
Let me know if you have any questions or wish to discuss.

Thanks,
Jessica
613-949-4288

PROPOSED RESPONSE:
While we do not comment on specific threats, we can say that the Government of Canada, in consultation with its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of national critical infrastructure against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

Reporter's Name	[redacted]	s.19(1)
Media Outlet	Bloomberg News Ottawa	
Call Date	8/20/2012 2:00 PM	

s.19(1)

Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	
Status	Consulting
Branch	
Subject	SCE
Questions	Hello, I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands. The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre. The memos warn governments and corporations to guard against cyber-attacks from Anonymous. For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector," the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers." Can you comment on: What kind of threat does the Anonymous hacker group pose to Canada's energy industry today? Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

Pages 438 to / à 439

are duplicates of

sont des duplicatas des

pages 440 to / à 441

Wilson, Barbara

From: Wilson, Barbara
Sent: Tuesday, August 21, 2012 11:02 AM
To: Slack, Jessica
Subject: RE: Bloomberg News question about hacking threat

Yes. Good

Barbara Wilson
Senior Communications Advisor
Issues management and media relations
Conseillère principale en communications
Gestion des enjeux et relations avec les médias
Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue W/ 269, avenue Laurier ouest
Ottawa, (ON) K1P 0P8
(613) 944-4920
barbara.wilson@ps-sp.gc.ca

From: Slack, Jessica
Sent: Tuesday, August 21, 2012 10:10 AM
To: Wilson, Barbara
Subject: FW: Bloomberg News question about hacking threat

For approval please.
Jessica

From: Matz, Mark
Sent: August-21-12 9:59 AM
To: Slack, Jessica; Anderson, Windy
Cc: Fortunato, Stephanie; Weir, Sarah
Subject: Re: Bloomberg News question about hacking threat

This response is good. We won't say anything directly on specific instances. I'd only suggest a minor change to mention "vital systems", not just CI, as CCIRC's focus.

- mark

While we do not comment on specific threats, we can say that the Government of Canada, in consultation with its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including national critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

From: Slack, Jessica
Sent: Monday, August 20, 2012 02:57 PM
To: Matz, Mark; Anderson, Windy
Cc: Fortunato, Stephanie; Weir, Sarah
Subject: FW: Bloomberg News question about hacking threat

Hi Mark, Windy

See request below.

I've pulled together a few bullets as a start...can you have a look and revise as appropriate?

Grateful for a response by 10 a.m. tomorrow...

Let me know if you have any questions or wish to discuss.

Thanks,
Jessica

613-949-4288

PROPOSED RESPONSE:

While we do not comment on specific threats, we can say that the Government of Canada, in consultation with its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of national critical infrastructure against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

Reporter's Name [redacted]
Media Outlet Bloomberg News Ottawa
Call Date 8/20/2012 2:00 PM
Telephone [redacted]
E-mail address [redacted]@bloomberg.net
Deadline
Status Consulting
Branch
Subject SCE
Questions Hello,

s.19(1)

I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands.

The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre.
The memos warn governments and corporations to guard against cyber-attacks from Anonymous.
For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector,'' the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers.''

Can you comment on:

What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?
Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

Slack, Jessica

From: Slack, Jessica
Sent: August-21-12 11:16 AM
To: Miller, Kevin
Cc: Wilson, Barbara
Subject: RE: For approval: Bloomberg

Thanks. RCMP received a call from him as well so I am going to share this response with them before I go to SD...

From: Miller, Kevin
Sent: August-21-12 11:15 AM
To: Slack, Jessica
Cc: Wilson, Barbara
Subject: RE: For approval: Bloomberg

Approved. Thanks.
K

From: Slack, Jessica
Sent: Tuesday, August 21, 2012 11:09 AM
To: Miller, Kevin
Cc: Wilson, Barbara
Subject: For approval: Bloomberg

Kevin,

For approval please.
This has been approved by cyber policy and Barb.

Jessica

PROPOSED RESPONSE
While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including national critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

Reporter's Name	[redacted]	s.19(1)
Media Outlet	Bloomberg News Ottawa	
Call Date	8/20/2012 2:00 PM	
Telephone	[redacted]	

E-mail address	[redacted]@bloomberg.net s.19(1)
Deadline	8/23/2012 5:00 PM
Status	Consulting
Branch	
Subject	SCE
Questions	Hello, I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands. The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre. The memos warn governments and corporations to guard against cyber-attacks from Anonymous. For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector," the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers." Can you comment on: What kind of threat does the Anonymous hacker group pose to Canada's energy industry today? Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

Slack, Jessica

From: Slack, Jessica
Sent: August-21-12 11:20 AM
To: Greg Cox (Greg.Cox@rcmp-grc.gc.ca)
Cc: Wilson, Barbara
Subject: Bloomberg call re Anonymous

Greg,

Wanted to share our proposed response (in approvals) since this reporter had contacted RCMP as well.
Let me know if there are any concerns.
Jessica
613-949-4288

PROPOSED RESPONSE
While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including national critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

Questions

Hello,

I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands.
The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre.
The memos warn governments and corporations to guard against cyber-attacks from Anonymous.
For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector," the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers."

Can you comment on:

What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?
Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

Slack, Jessica

From: Stephanie Dumoulin <Stephanie.Dumoulin@rcmp-grc.gc.ca>
Sent: August-21-12 4:03 PM
To: Slack, Jessica
Subject: Re: Fwd: Bloomberg Question about Anonymous Memo on Oil Sands

Hi Jessica, these are pretty standard lines so we do not have any concerns!

Thanks for sharing,

Stephanie
-----Original Message-----
From: "Slack, Jessica" <Jessica.Slack@ps-sp.gc.ca>
To: Dumoulin, Stephanie <Stephanie.Dumoulin@rcmp-grc.gc.ca>

Sent: 8/21/2012 4:01:03 PM
Subject: RE: Fwd: Bloomberg Question about Anonymous Memo on Oil Sands

Let me know if there are any concerns with PS response..
Thanks!
Jessica

From: Stephanie Dumoulin [mailto:Stephanie.Dumoulin@rcmp-grc.gc.ca]
Sent: August-21-12 11:36 AM
To: Jean-Bruno.Villeneuve@international.gc.ca; Jessica.Seguin@international.gc.ca
Cc: Slack, Jessica; David Falls; Greg Cox; Marc-Andre Massie
Subject: Re: Fwd: Bloomberg Question about Anonymous Memo on Oil Sands

Yes please. Also, did you receive a call on this?

>>> <Jean-Bruno.Villeneuve@international.gc.ca<mailto:Jean-Bruno.Villene
>>> uve@international.gc.ca>> 8/21/2012 11:34 AM >>>
Are you still trying to track down the DFAIT ATI release? I can get it if you need it.

From: Stephanie Dumoulin [mailto:Stephanie.Dumoulin@rcmp-grc.gc.ca]<mailto:[mailto:Stephanie.Dumoulin@rcmp-grc.gc.ca]>
Sent: Tuesday, August 21, 2012 11:32 AM
To: Villeneuve, Jean-Bruno -BCM; Séguin, Jessica -BCM
Cc: Jessica.Slack@ps-sp.gc.ca<mailto:Jessica.Slack@ps-sp.gc.ca> <Jessica.Slack@ps-sp.gc.ca<mailto:Jessica.Slack@ps-sp.gc.ca>>; David Falls <David.Falls@rcmp-grc.gc.ca<mailto:David.Falls@rcmp-grc.gc.ca>>; Greg Cox <Greg.Cox@rcmp-grc.gc.ca<mailto:Greg.Cox@rcmp-grc.gc.ca>>; Marc-Andre Massie <Marc-Andre.Massie@rcmp-grc.gc.ca<mailto:Marc-Andre.Massie@rcmp-grc.gc.ca>>
Subject: Re: Fwd: Bloomberg Question about Anonymous Memo on Oil Sands

Further to my previous email, the ATIP # is A-2011-02421. Also, PS received a call as well. Here is their proposed response (in approvals) along with the reporter's question to them for everyone's awareness:

PROPOSED RESPONSE

While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including national critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

Questions

Hello,

I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands.
The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre.
The memos warn governments and corporations to guard against cyber-attacks from Anonymous.
For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector,'' the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers.''

Can you comment on:

What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?
Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

>>> Stephanie Dumoulin 8/21/2012 11:22 AM >>>
Hello,

We received a media request yesterday (see request below) stemming from an ATIP that was apparently released by DFAIT. We are trying to locate this ATIP file in order to provide an educated response since the source information from this ATIP comes from the RCMP. We don't have the file number but can always get it from the reporter if needed.

Would you be able to provide us with a copy? Also, would you have received a media request from this individual as well? Either way, we will be coordinating our response with you once our lines are finalized.

Thanks,

Stéphanie

Stéphanie Dumoulin
Communications Strategist | Conseillère en communications National Communication Services | Services nationaux de communication Royal Canadian Mounted Police | Gendarmerie royale du Canada
Tel: | Tél: 613.993.1977

s.16(2)

BB:

stephanie.dumoulin@rcmp-grc.gc.ca<mailto:stephanie.dumoulin@rcmp-grc.gc.ca>

>>> (BLOOMBERG/ NEWSROOM:)"
>>> @bloomberg.net>> 8/20/2012 1:52
>>> PM >>>
Hello Cpl. Falls,

I am writing a story based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands.
The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre.
The memos warn governments and corporations to guard against cyber-attacks from Anonymous.
One from the RCMP is titled `Cyber Threat to Canada's Oil Sand Petroleum Industry' and was written July 14, 2011.
There is also a report from the RCMP that was distributed around DFAIT on Jan. 3, 2012 about a breach at the Stratfor security company that may have led to phishing e-mails being sent to energy companies.

Can you comment on:

What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?
Has your agency warned energy companies about the risks of a cyber-attack from Anonymous? What kinds of officials were memos from your department sent to-- i.e., corporate or government Information Technology officers, ministers, deputy ministers, energy company executives?

Thank you,

Bloomberg News Ottawa

Page 450

is a duplicate

est un duplicata

Wilson, Barbara

From: Wilson, Barbara
Sent: Tuesday, August 21, 2012 7:55 PM
To: Durand, Stéphanie
Cc: Slack, Jessica; Miller, Kevin
Subject: Re: For DG approval: Bloomberg on Anonymous

Will verify re consult.

From: Durand, Stéphanie
Sent: Tuesday, August 21, 2012 05:42 PM
To: Slack, Jessica; Tomlinson, Jamie; Dubé, Rosanne; Salewski, Shawn; Bue, Richard
Cc: Miller, Kevin; Manning, Kerri; Wilson, Barbara; Carta, John
Subject: RE: For DG approval: Bloomberg on Anonymous

Pls share with NRCan, Environment, CSIS and CSE.
Did you also consult with Critical Infrastructure team at PS, not just cyber policy?
Thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Slack, Jessica
Sent: Tuesday, August 21, 2012 4:09 PM
To: Durand, Stéphanie; Tomlinson, Jamie; Dubé, Rosanne; Salewski, Shawn; Bue, Richard
Cc: Miller, Kevin; Manning, Kerri; Wilson, Barbara; Carta, John
Subject: For DG approval: Bloomberg on Anonymous

For DG approval. Reporter's deadline is Thursday.
This has been approved by cyber policy and shared with the RCMP. Barb and Kevin have approved on behalf of Lisa and Andrew.

Thanks,
Jessica

PROPOSED RESPONSE
While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including national critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

Reporter's Name	[redacted]
Media Outlet	Bloomberg News Ottawa
Call Date	8/20/2012 2:00 PM
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	8/23/2012 5:00 PM
Status	Consulting
Branch	
Subject	SCE
Questions	Hello,

s.19(1)

I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands.
The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre.
The memos warn governments and corporations to guard against cyber-attacks from Anonymous.
For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector," the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers."

Can you comment on:

What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?
Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

Slack, Jessica

From: Wong, Suki
Sent: August-22-12 9:37 AM
To: Slack, Jessica
Cc: DeJong, Michael; Hunt, Ryan
Subject: FW:

See changes. Tx!

----- Original Message -----
From: Slack, Jessica
Sent: Wednesday, August 22, 2012 08:16 AM
To: DeJong, Michael; Wong, Suki
Cc: Wilson, Barbara
Subject:

Mike, Suki

Please see request below. Proposed response, cleared by cyber policy, is below.

Could you let me know by 11 this morning if you are ok with it or if you would have anything to add?

Thanks,
Jessica

PROPOSED RESPONSE

While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including ~~national~~ critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides tanalytical releases, as well as a variety of information products and services specifically for IT professionals~~, and managers of~~ critical infrastructure sectors and other related industries.

REQUEST
Reporter's Name s.19(1)

Media Outlet Bloomberg News Ottawa s.19(1)

Call Date 8/20/2012 2:00 PM

Telephone [redacted] E-mail address [redacted]@bloomberg.net Deadline 8/23/2012 5:00 PM

Status Consulting

Branch Subject SCE

Questions Hello,

I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands.

The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre.

The memos warn governments and corporations to guard against cyber-attacks from Anonymous.

For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector,'' the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers.''

Can you comment on:

What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?

Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

Pages 455 to / à 457

are duplicates of

sont des duplicatas des

pages 463 to / à 465

Slack, Jessica

From: Slack, Jessica
Sent: August-22-12 1:56 PM
To: 'Johnson,Mark [NCR]'; Perras, Jacinthe
Subject: RE: Media request : Bloomberg on Anonymous targetting oilsands

Thanks to you both!

From: Johnson,Mark [NCR] [mailto:Mark.Johnson@ec.gc.ca]
Sent: August-22-12 1:51 PM
To: Perras, Jacinthe; Slack, Jessica
Cc: Viau, Michelle; Khoury, Cathy
Subject: RE: Media request : Bloomberg on Anonymous targetting oilsands

Good on our end as well, thx.

Mark Johnson
Conseiller en relations avec les médias | Media Relations Advisor
Direction générale des communications | Communications Branch
Environnement Canada | Environment Canada
10, rue Wellington, 23e étage | 10 Wellington, 23rd Floor
Gatineau (Québec) K1A 0H3
Tél: 819-934-8095 Fax: 819-994-1412 BB: [redacted] s.19(1)
Mark.Johnson@ec.gc.ca
Gouvernement du Canada | Government of Canada
Site Web | Website www.ec.gc.ca

From: Perras, Jacinthe [mailto:Jacinthe.Perras@NRCan-RNCan.gc.ca]
Sent: August 22, 2012 1:50 PM
To: Slack, Jessica; Johnson,Mark [NCR]
Cc: Viau, Michelle; Khoury, Cathy
Subject: Media request : Bloomberg on Anonymous targetting oilsands

Thanks Jessica! We have no concerns.

Jacinthe

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: August 22, 2012 09:57
To: Perras, Jacinthe; mark.johnson@ec.gc.ca
Cc: Wilson, Barbara
Subject: Media request : Bloomberg on Anonymous targetting oilsands
Importance: High

Pages 459 to / à 460

are duplicates of

sont des duplicatas des

pages 486 to / à 487

Slack, Jessica

From: Slack, Jessica
Sent: August-22-12 2:05 PM
To: [redacted]
Cc: Wilson, Barbara
Subject: RE: Media request : Bloomberg on Anonymous targetting oilsands

Many thanks, [redacted] Will ensure you and [redacted] are on our contact list.

From: [redacted] [mailto: [redacted] @CSE-CST.GC.CA]
Sent: August-22-12 2:04 PM
To: Slack, Jessica
Subject: FW: Media request : Bloomberg on Anonymous targetting oilsands
Importance: High

Classification: UNCLASSIFIED

Jessica,
Thank you for this information. CSEC agrees with the proposed MRLs.

[redacted]

P.S. For your information, [redacted] does not work in communications anymore. Please forward any other MRLs to myself and [redacted]

From: [redacted]
Sent: August 22, 2012 11:47 AM
To: [redacted] Plamondon, Jean J.
Subject: FW: Media request : Bloomberg on Anonymous targetting oilsands
Importance: High

Classification: UNCLASSIFIED

[redacted] Jean,

Please see below request from Public Safety.

[redacted]

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: August 22, 2012 10:07 AM
To: [redacted]
Subject: Media request : Bloomberg on Anonymous targetting oilsands
Importance: High

Hello [redacted]

See request below. Am also sharing with CSIS, EC and NRCan.

This is policy approved - grateful if you could advise if you have any concerns on your end by 2 p.m. so I can proceed with further approvals.
Thanks,
Jessica

PROPOSED RESPONSE

While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Reporter's Name	[redacted]
Media Outlet	Bloomberg News Ottawa
Call Date	8/20/2012 2:00 PM
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	8/23/2012 5:00 PM
Status	Consulting
Branch	
Subject	SCE
Questions	Hello, I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands. The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre. The memos warn governments and corporations to guard against cyber-attacks from Anonymous. For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector," the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers." Can you comment on: What kind of threat does the Anonymous hacker group pose to Canada's energy industry today? Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

s.19(1)

Bue, Richard

From: Tomlinson, Jamie
Sent: August-22-12 2:06 PM
To: Slack, Jessica
Cc: Dubé, Rosanne; Bue, Richard; Salewski, Shawn; Miller, Kevin; Wilson, Barbara; Manning, Kerri; Carta, John
Subject: RE: For DG approval: Bloomberg on Anonymous

Approved.

thanks

From: Slack, Jessica
Sent: August-22-12 1:55 PM
To: Tomlinson, Jamie
Cc: Dubé, Rosanne; Bue, Richard; Salewski, Shawn; Miller, Kevin; Wilson, Barbara; Manning, Kerri; Carta, John
Subject: FW: For DG approval: Bloomberg on Anonymous

Jamie, for approval in Stephanie's absence.

At PS this has been approved by cyber and CI policy.

I have shared it also with CSIS, CSEC, RCMP, NRCan and EC.
Jessica

PROPOSED RESPONSE

While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

From: Durand, Stéphanie
Sent: August-21-12 5:43 PM
To: Slack, Jessica; Tomlinson, Jamie; Dubé, Rosanne; Salewski, Shawn; Bue, Richard
Cc: Miller, Kevin; Manning, Kerri; Wilson, Barbara; Carta, John
Subject: RE: For DG approval: Bloomberg on Anonymous

Pls share with NRCan, Environment, CSIS and CSE.
Did you also consult with Critical Infrastructure team at PS, not just cyber policy?
Thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Slack, Jessica
Sent: Tuesday, August 21, 2012 4:09 PM
To: Durand, Stéphanie; Tomlinson, Jamie; Dubé, Rosanne; Salewski, Shawn; Bue, Richard
Cc: Miller, Kevin; Manning, Kerri; Wilson, Barbara; Carta, John
Subject: For DG approval: Bloomberg on Anonymous

For DG approval. Reporter's deadline is Thursday.
This has been approved by cyber policy and shared with the RCMP. Barb and Kevin have approved on behalf of Lisa and Andrew.

Thanks,
Jessica

PROPOSED RESPONSE
While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including national critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

Reporter's Name	[redacted]
Media Outlet	Bloomberg News Ottawa
Call Date	8/20/2012 2:00 PM
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	8/23/2012 5:00 PM
Status	Consulting
Branch	
Subject	SCE
Questions	Hello,

s.19(1)

I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands.
The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre.
The memos warn governments and corporations to guard against cyber-attacks from Anonymous.
For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector,'' the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers.''

Can you comment on:

What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?
Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

Slack, Jessica

From: Carmichael, Julie
Sent: August-22-12 2:32 PM
To: Slack, Jessica; Johnson, Mark; McGrath, Andrew; Thibouthot, AkimIsabelle
Cc: Tomlinson, Jamie; Wilson, Barbara; Miller, Kevin; Manning, Kerri
Subject: RE: FOR MO approval: Bloomberg on Anonymous and oilsands

Approved

From: Slack, Jessica
Sent: August-22-12 2:13 PM
To: Carmichael, Julie; Johnson, Mark; McGrath, Andrew; Thibouthot, AkimIsabelle
Cc: Tomlinson, Jamie; Wilson, Barbara; Miller, Kevin; Manning, Kerri
Subject: FOR MO approval: Bloomberg on Anonymous and oilsands

Julie- for approval please.

We've shared with CSIS, CSEC, RCMP, EC and NRCan for awareness...reporter has also contacted CSIS and RCMP.

Thanks,
Jessica

PROPOSED RESPONSE

While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Reporter's Name	[redacted]
Media Outlet	Bloomberg News Ottawa
Call Date	8/20/2012 2:00 PM
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	8/23/2012 5:00 PM
Status	Consulting
Branch	
Subject	SCE
Questions	Hello,

I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands.
The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre.
The memos warn governments and corporations to guard against cyber-attacks from Anonymous.
For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector,'' the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers.''

Can you comment on:

What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?
Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

Slack, Jessica

From: Slack, Jessica on behalf of PS Media Relations / Relations médias SP
Sent: August-22-12 2:43 PM
To: [redacted]
Subject: RE: Bloomberg News question about hacking threat

Hi [redacted]

While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Regards,
Jessica

Jessica Slack
Spokesperson / Porte-parole
Media Relations / Relations avec les médias
Public Safety Canada / Sécurité publique Canada
613-991-0657
media@ps-sp.gc.ca

-----Original Message-----
From: [redacted] (BLOOMBERG/ NEWSROOM:) [mailto:[redacted]@bloomberg.net]
Sent: August-20-12 1:20 PM
To: PS Media Relations / Relations médias SP
Subject: RE: Bloomberg News question about hacking threat

I am looking to file a final version of this on Friday.

-- [redacted]

----- Original Message -----
From: PSMediaRelations@ps-sp.gc.ca
To: [redacted] (BLOOMBERG/ NEWSROOM:)
At: Aug 20 2012 13:18:47

Hi [redacted]

I will look into this for you.
Please advise us of your deadline.

Jessica

-----Original Message-----
From: [redacted](BLOOMBERG/ NEWSROOM:) [mailto:[redacted]@bloomberg.net]
Sent: August-20-12 1:17 PM
To: PS Media Relations / Relations médias SP
Subject: Bloomberg News question about hacking threat

Hello,

I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands.

The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre.

The memos warn governments and corporations to guard against cyber-attacks from Anonymous.

For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector,'' the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers.''

Can you comment on:

What kind of threat does the Anonymous hacker group pose to Canada's energy industry and/or your company today?

Has your company received government warnings about the risks of a cyber-attack from Anonymous?

Thank you,

[redacted]Bloomberg News Ottawa

[redacted]Reporter, Bloomberg News
46 Elgin Street, Suite 110, Ottawa ON Canada K1P 5K6 Phone -[redacted]Mobile [redacted]
[redacted]@bloomberg.net Ottawa Bureau: +1-613-667-4800; Ottawanews@bloomberg.net; Fax [redacted]
http://www.bloomberg.com/news/canada/ Twitter: @[redacted]

Swift, Andrew

From: Issues / Enjeux
Sent: Wednesday, August 22, 2012 3:55 PM
To: McDonald, Jessica; Picard, Josée; Swift, Andrew; Filipps, Lisa; Manning, Kerri; Champoux, Martin; Wilson, Barbara; Slack, Jessica; Miller, Kevin; Duval, Jean Paul; Van Criekingen, Jane; Taillefer, Lucie
Subject: FW: Media call - Due 3:30pm.

Categories: ATI PRINT

From: Carmichael, Julie
Sent: August-22-12 3:55:08 PM (UTC-05:00) Eastern Time (US & Canada)
To: 'Tahera MUFTI'
Cc: Williams, Christpher; Issues / Enjeux
Subject: RE: Media call - Due 3:30pm.

Approved

From: Tahera MUFTI [mailto:
Sent: August-22-12 1:42 PM
To: Carmichael, Julie
Cc: Williams, Christpher; Issues / Enjeux
Subject: Media call - Due 3:30pm.

s.19(1)

Hi Julie,

reporter for *Bloomberg News*, contacted me to ask me about an ITAC assessment he's received. He specifically wanted to know if Anonymous still poses a threat to the Alberta Oil Sands, and wanted to find out how our agency provides information about threats to the energy sector.

Here are our responses, approved by DG CB and ADP:

I cannot publicly discuss details about specific operational activities, but it's no secret that threats to Canada's critical infrastructure are real and will persist. There have been, for example, well-publicized attacks to our energy sector.

As for your inquiry about how we warn industry partners about threats to their sectors: In the ATIP package you received you'll see some threat assessments produced by the Integrated Terrorism Assessment Centre (ITAC). ITAC disseminates these assessments to key partners and stakeholders - within government and the private sector. There are other lines of communication too, but ITAC plays an important role.

Do you approve?

Tahera

s.15(1) - Subv

Tahera Mufti
Canadian Security Intelligence Service (CSIS) / Service canadien du renseignement de sécurité (SCRS)
Media and Public Liaison Program / Programme des relations avec les médias et le public
(613)231-0100

Slack, Jessica

From: Slack, Jessica
Sent: August-23-12 2:45 PM
To: Wilson, Barbara; Miller, Kevin
Subject: FW: Fwd: Bloomberg Question about Anonymous Memo on Oil Sands
Attachments: ML-ATIP-Anonymous Memo on Oilsands.doc

Fyi.

From: Stephanie Dumoulin [mailto:Stephanie.Dumoulin@rcmp-grc.gc.ca]
Sent: August-23-12 2:42 PM
To: Jean-Bruno.Villeneuve@international.gc.ca; Jessica.Seguin@international.gc.ca; Slack, Jessica
Cc: Greg Cox; Marc-Andre Massie
Subject: Re: Fwd: Bloomberg Question about Anonymous Memo on Oil Sands

Hello everyone,

Four your awareness, here are our approved media lines that we will be using to respond to this media request this afternoon. Thank you Jean-Bruno for sending the ATIP package over to us, it was very helpful.

Regards,

Stéphanie

>>> <Jean-Bruno.Villeneuve@international.gc.ca> 8/21/2012 11:36 AM >>>
No calls. I will track it down and send it.

From: Stephanie Dumoulin [mailto:Stephanie.Dumoulin@rcmp-grc.gc.ca]
Sent: Tuesday, August 21, 2012 11:35 AM
To: Villeneuve, Jean-Bruno -BCM; Séguin, Jessica -BCM
Cc: Jessica.Slack@ps-sp.gc.ca <Jessica.Slack@ps-sp.gc.ca>; David Falls <David.Falls@rcmp-grc.gc.ca>; Greg Cox <Greg.Cox@rcmp-grc.gc.ca>; Marc-Andre Massie <Marc-Andre.Massie@rcmp-grc.gc.ca>
Subject: Re: Fwd: Bloomberg Question about Anonymous Memo on Oil Sands

Yes please. Also, did you receive a call on this?

>>> <Jean-Bruno.Villeneuve@international.gc.ca> 8/21/2012 11:34 AM >>>
Are you still trying to track down the DFAIT ATI release? I can get it if you need it.

From: Stephanie Dumoulin [mailto:Stephanie.Dumoulin@rcmp-grc.gc.ca]
Sent: Tuesday, August 21, 2012 11:32 AM
To: Villeneuve, Jean-Bruno -BCM; Séguin, Jessica -BCM
Cc: Jessica.Slack@ps-sp.gc.ca <Jessica.Slack@ps-sp.gc.ca>; David Falls <David.Falls@rcmp-grc.gc.ca>; Greg Cox <Greg.Cox@rcmp-grc.gc.ca>; Marc-Andre Massie <Marc-Andre.Massie@rcmp-grc.gc.ca>
Subject: Re: Fwd: Bloomberg Question about Anonymous Memo on Oil Sands

Pages 473 to / à 474
are duplicates of
sont des duplicatas des
pages 447 to / à 448

Pages 475 to / à 476
are duplicates of
sont des duplicatas des
pages 480 to / à 481

Pages 477 to / à 478

are duplicates of

sont des duplicatas des

pages 484 to / à 485

Page 479

is a duplicate of

est un duplicata de la

page 485

RCMP·GRC
ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

MEDIA LINES / QUESTIONS & ANSWERS
ATIP – Anonymous Memo on Oilsands

ISSUE

A media request was received based on government memos showing that the hacker group Anonymous targeted Canada's energy industry in July 2011 because of objections to developing Alberta's oil sands.

BACKGROUND

The documents were obtained by ATIP through DFAIT and contain memos from several government departments, including DFAIT, RCMP, Public Safety, Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre. The memos warn governments and corporations to guard against cyber-attacks from Anonymous. One from the RCMP is titled `Cyber Threat to Canada's Oil Sand Petroleum Industry' and was written July 14, 2011. There is also a report from the RCMP that was distributed around DFAIT on Jan. 3, 2012 about a breach at the Stratfor security company that may have led to phishing e-mails being sent to energy companies. The reporter has also approached Public Safety on this matter.

MEDIA LINES

- As Canada's national police force, the RCMP assists in the identification of criminal threats to Canada's critical infrastructure and develops criminal intelligence that may be used by first responders and the private sector to assess and mitigate risks associated to criminal threats.

- The RCMP Critical Infrastructure Intelligence Team's (CIIT) primary objective is to produce and provide timely, relevant and actionable intelligence in support of the RCMP's investigations and for the benefit of the CI stakeholders.

QUESTIONS AND ANSWERS:

Q1 What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?

A1 The RCMP CIIT continuously monitors the full landscape to detect credible and/or potential criminal threats to Canada's critical infrastructure, including threats against the energy sector. Although we cannot comment on specific threats posed by certain groups or individuals, we can say that the RCMP is committed to protecting the safety and security of Canada's critical infrastructure and has made it a national security priority.

Q2 Has your agency warned energy companies about the risks of a cyber-attack from Anonymous?

A2 CIIT produces criminal intelligence to support the RCMP's criminal investigations, and also provides both classified and un-classified intelligence products in the form of intelligence bulletins, briefs and assessments, to its private sector partners on an ongoing basis.

Q3 What kinds of officials were memos from your department sent to-- i.e., corporate or government Information Technology officers, ministers, deputy ministers, energy company executives?

A3 CIIT has developed and maintains mutually beneficial partnerships with more than fifty energy sector companies including the: major electricity production and transmission companies; the nuclear industry; up-stream and down-stream petroleum companies; and pipeline companies. The energy sector associations including the: Canadian Electricity Association, Canadian Association of Petroleum Producers; Canadian Gas Association; Canadian Energy Pipeline Association; Canadian Petroleum Products Institute. CIIT also shares its products with several provincial and federal Government Departments, as well as the federal energy sector regulators including the: National Energy Board, Canadian Nuclear Safety Commission; Canada - Newfoundland and Labrador Offshore Petroleum Board and the Canada - Nova Scotia Offshore Petroleum Boards; Atomic Energy of Canada Limited.

Q4 Can you provide comments on Strafor security breach that has a Canadian nexus?

A4 Although we cannot comment on specific incidents, we can say that the RCMP is committed to protecting the safety and security of Canada's critical infrastructure and has made it a national security priority.

Prepared by:
Stephanie Dumoulin - Communication Strategist, NSCI — August 22, 2012

Approved by:
Sgt. Greg Cox, A/Director, National Media Relations — August 23, 2012
C/Supt. Larry Tremblay, Acting A/Commr NSCI — August 23, 2012

Slack, Jessica

From: Slack, Jessica
Sent: August-27-12 9:41 AM
To: Champoux, Martin
Subject: FW: Media call - Due 3:30pm.

From: Issues / Enjeux
Sent: August-22-12 1:42 PM
To: McDonald, Jessica; Picard, Josée; Swift, Andrew; Filipps, Lisa; Manning, Kerri; Champoux, Martin; Wilson, Barbara; Slack, Jessica; Miller, Kevin; Duval, Jean Paul; Van Criekingen, Jane; Taillefer, Lucie
Subject: FW: Media call - Due 3:30pm.

From: Tahera MUFTI
Sent: Wednesday, August 22, 2012 1:41:51 PM (UTC-05:00) Eastern Time (US & Canada)
To: Carmichael, Julie
Cc: Williams, Christpher; Issues / Enjeux
Subject: Media call - Due 3:30pm.

Hi Julie, s.19(1)

[redacted] reporter for *Bloomberg News*, contacted me to ask me about an ITAC assessment he's received. He specifically wanted to know if Anonymous still poses a threat to the Alberta Oil Sands, and wanted to find out how our agency provides information about threats to the energy sector.

Here are our responses, approved by DG CB and ADP:

I cannot publicly discuss details about specific operational activities, but it's no secret that threats to Canada's critical infrastructure are real and will persist. There have been, for example, well-publicized attacks to our energy sector.

As for your inquiry about how we warn industry partners about threats to their sectors: In the ATIP package you received you'll see some threat assessments produced by the Integrated Terrorism Assessment Centre (ITAC). ITAC disseminates these assessments to key partners and stakeholders - within government and the private sector. There are other lines of communication too, but ITAC plays an important role.

Do you approve?

Tahera
[redacted] s.15(1) - Subv

Tahera Mufti
Canadian Security Intelligence Service (CSIS) / Service canadien du renseignement de sécurité (SCRS)
Media and Public Liaison Program / Programme des relations avec les médias et le public
(613)231-0100

Slack, Jessica

From: Slack, Jessica
Sent: August-27-12 9:47 AM
To: Champoux, Martin
Subject: FW: FYI - RCMP Heads up - Bloomberg Question about Anonymous Memo on Oil Sands
Attachments: ML-ATIP-Anonymous Memo on Oilsands.doc

From: Miller, Kevin
Sent: August-23-12 3:10 PM
To: Carmichael, Julie
Cc: Johnson, Mark; Mueller, Mike; McGrath, Andrew; Durand, Stéphanie; Tomlinson, Jamie; Wilson, Barbara
Subject: FYI - RCMP Heads up - Bloomberg Question about Anonymous Memo on Oil Sands

Hi Julie,

FYI – Please see heads up below from the RCMP regarding a media request they received related to an ATIP on the hacker group Anonymous targeting Canada's Energy Sector (specifically the Oilsands in AB).

We will monitor for coverage.

Thanks,

Kevin

From: Greg Cox [mailto:Greg.Cox@rcmp-grc.gc.ca]
Sent: Thursday, August 23, 2012 2:57 PM
To: Miller, Kevin
Cc: Durand, Stéphanie; Marc Richer; Nikic, Peter
Subject: Re: Fwd: Bloomberg Question about Anonymous Memo on Oil Sands

Four your awareness, here are our approved media lines that we will be using to respond to this media request this afternoon.

MEDIA LINES / QUESTIONS & ANSWERS

ATIP – Anonymous Memo on Oilsands

ISSUE

A media request was received based on government memos showing that the hacker group Anonymous targeted Canada's energy industry in July 2011 because of objections to developing Alberta's oil sands.

BACKGROUND

The documents were obtained by ATIP through DFAIT and contain memos from several government departments, including DFAIT, RCMP, Public Safety, Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre. The memos warn governments and corporations to guard against cyber-attacks from Anonymous. One from the RCMP is titled `Cyber Threat to Canada's Oil Sand Petroleum Industry' and was written July 14, 2011. There is also a report from the RCMP that was distributed around DFAIT on Jan. 3, 2012 about a breach at the Stratfor security company that may have led to phishing e-mails being sent to energy companies. The reporter has also approached Public Safety on this matter.

MEDIA LINES

- As Canada's national police force, the RCMP assists in the identification of criminal threats to Canada's critical infrastructure and develops criminal intelligence that may be used by first responders and the private sector to assess and mitigate risks associated to criminal threats.

- The RCMP Critical Infrastructure Intelligence Team's (CIIT) primary objective is to produce and provide timely, relevant and actionable intelligence in support of the RCMP's investigations and for the benefit of the CI stakeholders.

QUESTIONS AND ANSWERS:

Q1 What kind of threat does the Anonymous hacker group pose to Canada's energy industry today?

A1 The RCMP CIIT continuously monitors the full landscape to detect credible and/or potential criminal threats to Canada's critical infrastructure, including threats against the energy sector. Although we cannot comment on specific threats posed by certain groups or individuals, we can say that the RCMP is committed to protecting the safety and security of Canada's critical infrastructure and has made it a national security priority.

Q2 Has your agency warned energy companies about the risks of a cyber-attack from Anonymous?

A2 CIIT produces criminal intelligence to support the RCMP's criminal investigations, and also provides both classified and un-classified intelligence products in the form of intelligence bulletins, briefs and assessments, to its private sector partners on an ongoing basis.

Q3 What kinds of officials were memos from your department sent to-- i.e., corporate or government Information Technology officers, ministers, deputy ministers, energy company executives?

A3 CIIT has developed and maintains mutually beneficial partnerships with more than fifty energy sector companies including the: major electricity production and transmission companies; the nuclear industry; up-stream and down-stream petroleum companies; and pipeline companies. The energy sector associations including the: Canadian Electricity Association, Canadian Association of Petroleum Producers; Canadian Gas Association; Canadian Energy Pipeline Association; Canadian Petroleum Products Institute. CIIT also shares its products with several provincial and federal Government Departments, as well as the federal energy sector regulators including the: National Energy Board, Canadian Nuclear Safety Commission; Canada - Newfoundland and Labrador Offshore Petroleum Board and the Canada - Nova Scotia Offshore Petroleum Boards; Atomic Energy of Canada Limited.

Q4 Can you provide comments on Strafor security breach that has a Canadian nexus?

A4 Although we cannot comment on specific incidents, we can say that the RCMP is committed to protecting the safety and security of Canada's critical infrastructure and has made it a national security priority.

Greg

Paulson, Erika

From: Paulson, Erika
Sent: Tuesday, August 28, 2012 12:50 PM
To: Slack, Jessica
Subject: RE: Media request : Bloomberg on Anonymous targetting oilsands

Thanks ☺

Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

From: Slack, Jessica
Sent: Tuesday, August 28, 2012 12:50 PM
To: Paulson, Erika
Subject: FW: Media request : Bloomberg on Anonymous targetting oilsands

FYI...

From: Perras, Jacinthe [mailto:Jacinthe.Perras@NRCan-RNCan.gc.ca]
Sent: August-22-12 1:50 PM
To: Slack, Jessica; mark.johnson@ec.gc.ca
Cc: Viau, Michelle; Khoury, Cathy
Subject: Media request : Bloomberg on Anonymous targetting oilsands

Thanks Jessica! We have no concerns.

Jacinthe

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: August 22, 2012 09:57
To: Perras, Jacinthe; mark.johnson@ec.gc.ca
Cc: Wilson, Barbara
Subject: Media request : Bloomberg on Anonymous targetting oilsands
Importance: High

Good morning Mark and Jacinthe,

Please see media request below.

Just wanted to share for your awareness.

Our policy approved response is below. If you have any concerns, grateful if you could get back to me by 2 p.m. today so I can proceed with further approvals.

Many thanks,
Jessica

PROPOSED RESPONSE

While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Reporter's Name	[redacted] **s.19(1)**
Media Outlet	Bloomberg News Ottawa
Call Date	8/20/2012 2:00 PM
Telephone	[redacted]
E-mail address	[redacted]@bloomberg.net
Deadline	8/23/2012 5:00 PM
Status	Consulting
Branch	
Subject	SCE
Questions	Hello, I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands. The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre. The memos warn governments and corporations to guard against cyber-attacks from Anonymous. For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector,'' the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers.'' Can you comment on: What kind of threat does the Anonymous hacker group pose to Canada's energy industry today? Has your agency warned energy companies about the risk of a cyber attack from Anonymous?

Austria, Jamela

From: Austria, Jamela
Sent: Tuesday, August 28, 2012 1:08 PM
To: 'Jennifer.Fry@NRCan-RNCan.gc.ca'; 'Robert.Stewart@NRCan-RNCan.gc.ca'; 'Micheline.Joanisse@NRCan-RNCan.gc.ca'
Cc: Carta, John; Paulson, Erika
Subject: RE: Security/infrastructure
Attachments: PS MLs - cyber threats to CI

Hello!

Following Erika's note to you with our media lines – do these lines help? Please let me know if you need anything else.

Thanks!

Jamela Austria
Senior Communications Advisor | Conseillière principale en communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-1675
Mobile | Cellulaire : [redacted]
Fax | Télécopieur : 613-954-0800
E-mail | Courriel: jamela.austria@ps-sp.gc.ca

s.19(1)

From: Carta, John
Sent: Tuesday, August 28, 2012 9:06 AM
To: 'Jennifer.Fry@NRCan-RNCan.gc.ca'
Cc: 'Micheline.Joanisse@NRCan-RNCan.gc.ca'; 'Robert.Stewart@NRCan-RNCan.gc.ca'; Austria, Jamela
Subject: Re: Security/infrastructure

Hey gang - I hope everyone's good!

[redacted] but Jamela can help you out (Jamela, Jamie approved a response a couple of days ago on this, I think).

We do have some messages, but they don't say much. We don't really comment on this kind of thing in detail except to articulate what various roles are.

[redacted]

From: Fry, Jennifer [mailto:Jennifer.Fry@NRCan-RNCan.gc.ca]
Sent: Tuesday, August 28, 2012 08:53 AM
To: Carta, John
Cc: Joanisse, Micheline <Micheline.Joanisse@NRCan-RNCan.gc.ca>; Stewart, Robert <Robert.Stewart@NRCan-RNCan.gc.ca>
Subject: Security/infrastructure

Hi John, how's it going? I've been asked to follow up on a clipping from this morning regarding the security of Imperial Oil computers -- do you folks have any messaging on this kind of security breach?

Police identify 'Anonymous' threat

Greg Quinn reported that the RCMP and the Communications Security Establishment have warned energy companies such as ***Imperial Oil Ltd. that their computers may be attacked by the Anonymous hacker group because of the industry's work developing Alberta's oilsands.*** According to document obtained under freedom of information legislation, the security agencies investigated threats against the industry between the start of 2011 and mid-March. The RCMP conducted a threat assessment after the group that calls itself Anonymous issued a press release in July 2011 accusing oilsands companies of being greedy and harming the environment. The RCMP assessment said, "The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector. Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers." Queen's University's Thomas Dean, said the hackers are attracted to high-profile projects such as the Keystone XL pipeline, adding that the chance of an attack rests on whether the industry makes new international headlines (Montreal Gazette, B13, 28 August 2012: Winnipeg Press, B4; Calgary Herald, D4; Winnipeg Free Press, B4)

Jennifer Fry 613-944-6361
Communications Manager, Nuclear and Energy Policy
Gestionnaire des communications, politiques nucléaire et énergétique
Communications and Marketing Branch
Direction des communications et du marketing
Natural Resources Canada - *Ressources naturelles Canada*

Austria, Jamela

From: Paulson, Erika
Sent: Tuesday, August 28, 2012 12:54 PM
To: jennifer.fry@NRCan-RNCan.gc.ca
Cc: Champoux, Martin; Slack, Jessica; Austria, Jamela
Subject: PS MLs - cyber threats to CI

Hi Jen,
Apologies for the late response – my telephone's been on the fritz and my voicemail messages only came through now. RE your Q on PS MLs, please find them below courtesy of my issues management team (cc'd here). They were prepped last week and have not changed since.
They tell me your colleague Jacinthe had reviewed last week and advised NRCan had no concerns.

I understand RCMP and CSIS also had MLs. You may want to touch base with them for their latest.

Hopefully this is helpful.

Cheers,
Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

From: Champoux, Martin
Sent: Tuesday, August 28, 2012 12:46 PM
To: Paulson, Erika
Subject: voila

PS Lines

- While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

- The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

- The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Martin Champoux
Senior Communications Advisor | Conseiller principal en communications
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-5967
Fax | Télécopieur : 613-993-7062
Email | Courriel : Martin.Champoux@ps-sp.gc.ca

Austria, Jamela

From: Austria, Jamela
Sent: Tuesday, August 28, 2012 4:56 PM
To: McRae, Marley
Subject: Hopefully helpful media lines

Hi Marley,

Jessica Slack sent this list of media lines on cyber security – I thought I'd forward these to you in case they helped with developing messaging for the OAG report and/or the federal storyline. Please let me know what you think.

Thanks!
j

From: Slack, Jessica
Sent: Tuesday, August 28, 2012 11:15 AM
To: Austria, Jamela
Subject: Various cyber responses as promised....hope it helps!

Subject: Cyber Security

Questions:

I am including some questions below. I understand you might not be able to arrange an interview with the Director.If a phone interview is hard to schedule perhaps you could just secure some answers via email. Perhaps the answers can be attributed to the Director

hope you could provide us with some comments or a statement from Director Robert Dick.

Here are the questions:

1) Recently there were published reports of a leaked an Aug 2011 Public Safety Ministry memo (http://business.financialpost.com/2012/06/06/secret-memo-warns-of-canadian-cyber-threat-after-nortel-attack/) indicating that Canada suffers from poor security against cyber attacks that have targeted both government offices and private businesses.How true is this assessment today? Does our cyber security posture remain inadequate?

2) The government's cyber security strategy in in 2010 pledged to secure government computers.However the Canadian government continues to be a target of foreign hackers (http://business.financialpost.com/2012/06/06/secret-memo-warns-of-canadian-cyber-threat-after-nortel-attack/) and event recently Service Ontario's kiosks had to be put out of service because of a breach. Where would you say the deficiencies are in the national cyber security strategy? Does the directorate adequate personnel, enough budget to deliver on its mandate? Are policy or legislation part of the problem?

3) What are the major cyber security threats against government and business networks in Canada? Are they foreign of homegrown threats? What countries or governments are you keeping a close watch on?

4) What measures is the Canadian federal government taking to strengthen its own systems and the networks that underlie national security, public safety?

5) How closely does the directorate collaborate with its US counterparts or other similar government bodies in other countries?

6) Some Canadian companies such as Nortel and and Potash Corp. have been targets of cyber espionage. What is the directorate doing to protect Canadian companies? How

is the directorate coordinating efforts with the business sector?

7) What cyber crime trends and threats do you believe will the government face in the next 24 months?

Jean Paul, I can work with emailed answers to the questions. I hope we can attribute the answers to the Director and also get a statement from him.

Our deadline is Aug. 5. We can extend to Aug. 6.

Kindly email me or call me if you have questions.

Draft Response

1) Recently there were published reports of a leaked an Aug 2011 Public Safety Ministry memo (http://business.financialpost.com/2012/06/06/secret-memo-warns-of-canadian-cyber-threat-after-nortel-attack/) indicating that Canada suffers from poor security against cyber attacks that have targeted both government offices and private businesses. How true is this assessment today? Does our cyber security posture remain inadequate?

Since the release of the Cyber Security Strategy, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents. In 2011, we introduced Government IT Shared Services initiative to transform the way government manages IT telecommunications, desktop computer services, data centres, IT security services and consolidates Internet access points.

Furthermore, we are in the process of changing how we manage cyber incident response coordination for Government of Canada systems through the changed roles of Communications Security Establishment of Canada and Canadian Cyber Incident Response Centre. We have clarified roles and mandates of these organizations in order to strengthen and improve Canada's ability to identify, prevent and mitigate cyber security incidents.

2) The government's cyber security strategy in in 2010 pledged to secure government computers. However the Canadian government continues to be a target of foreign hackers (http://business.financialpost.com/2012/06/06/secret-memo-warns-of-canadian-cyber-threat-after-nortel-attack/) and event recently Service Ontario's kiosks had to be put out of service because of a breach. Where would you say the deficiencies are in the national cyber security strategy? Does the directorate adequate personnel, enough budget to deliver on its mandate? Are policy or legislation part of the problem?

The Government of Canada is continuously working to enhance cyber security in Canada by identifying cyber threats and vulnerabilities, and by preparing for and responding to all kinds of cyber incidents to better protect Canada and Canadians. That is why the Government of Canada announced in 2010 an investment of $90 million over five years, and $18 million in ongoing funding, towards the Strategy.

The Government has also established collaborative mechanisms with the provinces and territories and key critical infrastructure sectors. As a first priority, we are engaging the energy, telecommunications and finance sectors. Collaboration with telecommunications is ongoing and initial engagement with the energy sector has begun.

We are working with our key partners, including provinces, territories and priority critical infrastructure sectors, to develop joint action plans to improve cyber security in Canada.

3) What are the major cyber security threats against government and business networks in Canada? Are they foreign of homegrown threats? What countries or governments are you keeping a close watch on?

Cyber threats exist in varying degrees of complexity, but the most sophisticated cyber threats typically come from the intelligence and military services of foreign states. In most cases, these attackers are well resourced, patient and persistent. Their typical purpose is to gain political, economic, commercial or military advantage.

Canadians trust Government with their personal and corporate information, and also trust Government to deliver services to them. They also trust that the Government will act to defend Canada's cyber sovereignty and protect and advance our national security and economic interests. As such, the Government is putting in place the necessary structures, tools and personnel to meet its obligations for cyber security. This is Pillar 1 of Canada`s Cyber Strategy.

Pillar 2 of the strategy safeguards Canada's economic prosperity and Canadians' security by ensuring they can continue to depend on the smooth functioning of

systems outside the Government. In cooperation with provincial and territorial governments and the private sector, the Government will support initiatives and take steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors.
With the 3rd and final Pillar of the strategy, the Government of Canada will assist Canadians in getting the information they need to protect themselves and their families online, and strengthen the ability of law enforcement agencies to combat cybercrime.

4) What measures is the Canadian federal government taking to strengthen its own systems and the networks that underlie national security, public safety?
As stated in a previous response, the Government of Canada is continuously working to enhance cyber security in Canada by identifying cyber threats and vulnerabilities, and by preparing for and responding to all kinds of cyber incidents. This reflects the Government's commitment to help secure Canada's cyber systems and protect Canadians online.
In recognition that cyber security is the responsibility of all Canadians, Public Safety Canada has also launched a national public awareness initiative. Helping Canadians to be secure online is a key priority of Canada's Cyber Security Strategy. Cyber Security Awareness Month is an initiative to engage online Canadians to take action, and to provide them with the information they need to protect themselves and their families. This past October, in recognition of Cyber Security Awareness Month the Government of Canada launched a website with important information on cyber security for all Canadians: www.getcybersafe.ca.

5) How closely does the directorate collaborate with its US counterparts or other similar government bodies in other countries?
Cyber threats do not stop at borders. It is important that all countries work together in the area of cyber security.
Because we are neighbours and our economies and infrastructure are connected, the Government of Canada works closely with the United States. The Canadian Cyber Incident Response Centre collaborates regularly with the United States Computer Emergency Readiness Team and other international partners to detect and counter malicious cyber activity.
As part of the Border Action Plan released December 2011, Canada and the United States committed to enhancing our already strong bilateral cyber security cooperation to better protect vital government and critical digital infrastructure and increase both countries' ability to respond jointly and effectively to cyber incidents. Coordination between Canadian and U.S. cyber-security operations centers will be improved and allowed for both our countries to better prevent and respond to cyber incidents.
In addition to the United States, Canada is working on cyber security with other allies such as the UK, Australia and New Zealand. We are also working with international organizations such as Interpol, NATO, the Organization of American States and the Organization for Security and Cooperation in Europe.

6) Some Canadian companies such as Nortel and and Potash Corp. have been targets of cyber espionage. What is the directorate doing to protect Canadian companies? How is the directorate coordinating efforts with the business sector?
The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of national critical infrastructure against cyber incidents.
The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

7) What cyber crime trends and threats do you believe will the government face in the next 24 months?
We will not speculate on unknown or potential threats.

Branch	NS
Subject	Cyber Crime
Questions	I'm a freelance journalist here in Toronto and I'm working on an assignment for one of my clients, Security Matters Magazine, which as it sounds looks at security issues, both physical and virtual.

I would like to arrange an interview with National Cyber Security DG Robert Dick on the phone for a few minutes to chat in the next few days or so about the story which looks at cyber crime in Canada.

Specifically, what is Canada'a IT security posture: better or worse in 2012. It's a discussion around the most current threats to Canadian businesses, and the strategies companies can take to combat such attacks.

I'm also looking for stats on how Canada fares against other countries in terms of cyber attacks, phishing, etc. and how our practices compared in terms of laws and counter measures.

****

I chatted with Dave Black at the RCMP and he suggests Mr. Dick.

The questions are basic. Looking at three levels, though really only two. Government and Corporate and then consumer.

On the government side, state sponsored cyber snooping seems to be on the increase. What have we seen and what have we done in reaction?

On the Corporate site are they doing the right things? Where are the security breaches happening and are the more likely to be internal or external.

Finally, are the origins of attacks more likely to be overseas? Which jurisdictions are the biggest risk? We know Nigeria for example is the hotbed of romance fraud and phishing...what about other attacks.

s.19(1)

Also, does PSC have any stats?

Reporter and Outlet — [redacted] - Security Matters Magazine

Actions Taken — No existing entries.

Draft Response

Approvals — Mark Matz, Lisa, Andrew, Jamie, Julie

Final Response

Note that as we do not comment on specific security threats nor speculate on the potential origins or targets of malicious cyber activities, we are not able to fully answer all of your questions. However, we have compiled some information you may find helpful.
The Government of Canada is focused on cyber security, because this represents the real risks that citizens, businesses, and governments face. The internet has provided incredible opportunities for people to communicate and work together, yet this means that the internet also holds valuable information about people's private lives, about corporate operations, and about governments. Unfortunately, that can make the online world the target of fraud, theft, and even espionage.
Criminals are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, and spread criminal material. Sometimes this is led by organized crime; sometimes these crimes are perpetrated by individuals who are seeking thrills, pursuing a political agenda, or are trying to achieve notoriety or fame. As has been reported in the media, some corporations and foreign governments use cyber space as a way to conduct espionage, such as to steal trade secrets and research.
These are the types of cyber threats we are seeing every day and the ones the Government is working to address by implementing Canada's Cyber Security Strategy. This Strategy takes a whole-of-government approach to addressing cyber threats to government, critical assets and information, and Canadians. This Strategy is already providing concrete benefits.
As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic

network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.

The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email. For more information, please visit http://www.fightspam.gc.ca/eic/site/030.nsf/eng/home.

Of course, cyber threats are borderless so it is important that all countries work together on cyber security. Canada works on cyber security issues in concert with its allies, such as the United States, the UK, Australia and New Zealand. We are also working with international organizations such as Interpol, NATO, the Organization of American States and the Organization for Security and Cooperation in Europe.

Branch	NS
Subject	Cyber Security Strategy
Questions	Reporter is looking at the issue of cyber attacks on water treatment plants and is wondering what is being done from a Canadian perspective. Has there been any studies done/alarm bells raised on this issue in Canada?
s.19(1)	
Reporter and Outlet	[redacted] The Toronto Star
Actions Taken	No existing entries.
Draft Response	
Approvals	Mike de Jong, Suky Wong, Robert Dick, Lisa, SD, MIke also consulted with EC MR and PCO
Final Response	The security and resilience of the cyber systems that support Canada's critical infrastructure, including our water treatment plants, is essential to our economic prosperity, our quality of life and our national and personal security. This is why partnering with critical infrastructure sectors is a key component of Canada's Cyber Security Strategy, launched in October 2010. The second pillar of the Strategy - partnering to secure vital cyber systems outside the Federal Government - is meant to complement the National Strategy and Action Plan for Critical Infrastructure. This Strategy reflects the Government's commitment to protect critical infrastructure, including water treatment plants, from cyber attacks and other disruptions. In collaboration with other federal partners, Public Safety Canada is working on cyber security issues with critical infrastructure sectors, as well as with provinces, territories and other key stakeholders. Public Safety Canada and Environment Canada are also actively working with our partners in the water sector, including the Canadian Water and

Wastewater Association, to protect our drinking water systems from all-hazards (e.g. terrorist attacks, natural disasters, cyber attacks). This includes providing briefings on process control system security and participating in cyber security exercises.
On a day to day basis, Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) works with critical infrastructure providers to prevent and mitigate cyber incidents to enhance the resilience of Canada's critical infrastructure. In particular, the CCIRC coordinates cyber incident response with critical infrastructure sectors, such as dissemination of cyber awareness products, notifying critical infrastructure stakeholders of compromised systems, and conducting analysis of malicious software and websites.

Branch	NS
Subject	Anonymous - cyber attack on oilsands
Questions	Hello, I am writing a story this week based on government memos showing that the hacker group Anonymous in July 2011 targeted Canada's energy industry because of objections to developing Alberta's oil sands. The documents were obtained through access to information law requests, and contain memos from the DFAIT, RCMP, Public Safety department and Communications Security Establishment Canada and the Integrated Terrorism Assessment Centre. The memos warn governments and corporations to guard against cyber-attacks from Anonymous. For example: ``The Canadian law enforcement and security intelligence community have noted a growing radicalized environmentalist faction who is opposed to Canada's energy sector," the RCMP's report said. ``Corporate security officers should verify that security testing has been performed on public facing web servers and mail servers." Can you comment on: What kind of threat does the Anonymous hacker group pose to Canada's energy industry today? Has your agency warned energy companies about the risk of a cyber attack from Anonymous? Thank you, s.19(1) Bloomberg News Ottawa
Reporter and Outlet	Bloomberg News Ottawa
Actions Taken	No existing entries.
Draft Response	
Approvals	CI and Cyber policy Consulted: CSIS, NRCan, RCMP, CSEC and EC Julie
Final Response	While we do not comment on specific threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them. The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents. The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Branch NS

Subject Cyber Security Strategy

Final Response

1. Memo to minister from DM on cyber security (File name PS ATIP cyberthreats May 12):
- Mr. Baker says in his letter that the threat environment is ``likely worsening'' and beginning to impact economic prosperity through loss of IP. Is this still the department's position?
The Government of Canada remains concerned about threats to cyber security and is working to mitigate the risks by implementing Canada's Cyber Security Strategy.
As part of the first pillar of the Strategy, "securing government systems," the Government has created Shared Services Canada. This means that Government will consolidate its email systems, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.
Under the second pillar of the Strategy, the Government of Canada is reaching out to other levels of government, the private sector and critical infrastructure sectors to secure vital systems outside the Government. The Canadian Cyber Incident Response Centre (CCIRC) works directly with the owners of vital systems on how to deal with particular cyber threats. They are on the frontline in protecting our critical networks. Also, the Government is engaging key players, such as bringing together senior executives from the telecommunications industry in the Canadian Security Telecommunications Advisory Council, which also addresses cyber security issues.
The third pillar of the Strategy is reaching out to Canadians, to raise public awareness to help Canadians protect themselves and their families against online threats. For instance, the Government has instituted the Get Cyber Safe campaign and getcybersafe.ca website, as well as setting up the national Spam Centre for unsolicited and often fraud-related email.
- In the second paragraph of the memo, is he referring to cyber threats to Canada or cyber threats in general?
Cyber threats in general.
- Based on this document and the following, I'm confused about who coordinates cyber incident response. Is it CSC or CCIRC within PS? If their roles are different, how are they different?
Responsibility between CSEC and CCIRC for coordinating a response to cyber incidents depends on what types of networks are at risk. In the event of a cyber incident that impacts federal government networks, CSEC leads the response to the threat and works with other federal partners to resolve the situation. In this way, CSEC supports the first pillar of Canada's Cyber Security Strategy to secure government systems.
CCIRC coordinates the federal response to major cyber incidents that occur outside of Government networks. CCIRC regularly analyzes emerging cyber risks across Canada and provides advice to the private sector and other stakeholders on how to deal with particular cyber threats. CCIRC's role therefore supports the second pillar of Canada's Cyber Security Strategy to secure systems outside of Government.
- The second page refers to ``critical infrastructure sectors.'' Which sectors does that include?
Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.
The National Strategy for Critical Infrastructure identifies the following ten critical infrastructure sectors:
- Health
- Food
- Finance
- Water
- Information and Communication Technology
- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

2. Various documents prepared by CCIRC (File name CCIRC ATIP May 12)
- The deck on pgs 1-16 says 22 FTEs, with 14 staffed. How many full-time employees does CCIRC currently have?
CCIRC has staffed all 22 FTEs.

- Pg. 5 says there were 9 requests to shut down malicious systems last year. What does that mean? Are those requests by CCIRC to shut down systems, or requests of CCIRC to shut down systems? Which systems?
Malicious systems are often reported to CCIRC or observed by CCIRC directly. When CCIRC becomes aware of potential malicious code, it brings it to the attention of the internet service providers (ISPs) or webhosts affected. By making ISPs and others webhosts aware of the malicious content, those hosts are able to evaluate whether it contravenes their terms of service agreements and shut down the malicious systems accordingly. We do not comment on which systems.

- Pg. 6 says CCRIC is facing a number of challenges, including aging lab tech and difficulty recruiting qualified staff. How are these issues being addressed?
CCIRC is strengthening its capacity to effectively coordinate the national response to cyber security incidents. CCIRC has successfully recruited the additional staff needed and is modernizing its cyber security lab.

- Pgs. 57-8 refers to the future threat of attacks by Anonymous. What action was taken in response to this warning?
We do not comment on measures taken to address security threats. That said, the Government takes such threats seriously and has measures in place to address them.
- Pgs 64-6 includes a request to change CCRIC's mandate. Was the mandate changed as requested?
Canada's Cyber Security Strategy focused CCIRC's activities on vital systems outside of federal governments. The process of formalizing CCIRC's mandate is underway.

Subject

Cyber Threat

Questions

Looking for an interview /general information on DNSChanger malaware.

Draft Response

Answer to question 1 plus general info on the issue

- In November 2011, Canadian law enforcement and cyber security officials collaborated with national and international partners in their efforts to shut down a network of Domain Name System (DNS) servers controlled by cyber criminals. The network had been used to distribute a malware known as DNSChanger.
- The Canadian Cyber Incident Response Centre (CCIRC) monitored the network shutdown to ensure that it did not have a negative impact in Canada, particularly on the critical infrastructure sector.
- CCIRC has information posted on its webpage to help people find out if they have been infected by DNSChanger and how they can fix the problem. The information is available at the Public Safety Canada web site: http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-002-eng.aspx
- CCIRC worked with Canadian internet service providers to help them notify any of their subscribers who may have been infected by the malicious software and collaborated with the Canadian Internet Registration Authority (CIRA) on a web-based tool to detect whether Internet users are infected by the DNSChanger malware. This tool is hosted by CIRA at: http://www.dns-ok.ca
- CCIRC is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of national critical infrastructure against cyber incidents.
- General information for Canadians to protect themselves online is available at Get Cyber Safe (http://www.getcybersafe.gc.ca/index-eng.aspx)

Answer to question 2

- Government of Canada IT security personnel are aware of DNSChanger and have taken the necessary measures to protect against it.

Approvals

Final Response

s.19(1)

Good day [redacted]
Thank you for your information request regarding the DNSChanger malaware. To give you some context, in November 2011, Canadian law enforcement and cyber security officials collaborated with

national and international partners in their efforts to shut down a network of Domain Name System (DNS) servers controlled by cyber criminals. The network had been used to distribute a malware known as DNSChanger.
The Canadian Cyber Incident Response Centre (CCIRC) monitored the network shutdown to ensure that it did not have a negative impact in Canada, particularly on the critical infrastructure sector.
CCIRC has information posted on its webpage to help people find out if they have been infected by DNSChanger and how they can fix the problem. The information is available at the Public Safety Canada web site: http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-002-eng.aspx
CCIRC worked with Canadian internet service providers to help them notify any of their subscribers who may have been infected by the malicious software and collaborated with the Canadian Internet Registration Authority (CIRA) on a web-based tool to detect whether Internet users are infected by the DNSChanger malware. This tool is hosted by CIRA at: http://www.dns-ok.ca. CCIRC is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of national critical infrastructure against cyber incidents.
General information for Canadians to protect themselves online is available at Get Cyber Safe (http://www.getcybersafe.gc.ca/index-eng.aspx)

Branch

NS

Subject

Cyber

Questions

He is doing a three-part series for le Téléjournal regarding cyberwarfare. The first episode will be a 101 on cyberwarfare, second episode will focus on Canada`s position on this topic and finally, the last episode will provide an example of a cyber attack.

The reporter will be in the US this week to work on this piece and will be back on January 30th and would be available to interview the Minister between January 31st and February 3rd.

1) What is this new kind of threats mean for Canada?

2) Who could be interrested (wich coutries) to attack Canada?

3) What kind of attacks have we faced so far?

4) What is the gouvernement doing to make sure that our informations are kept in a safe way (wich organisations -groups-centres-ministries are working on that topic)?

5) Are we working with the american governement to develop an international defense?

6) How much money is the Canadian government spending on cyberwar?

Draft Response

***1) What do these new kinds of threats mean for Canada? Who would be interested (which countries) in attacking* Canada? What kind of attacks have we faced so far?**
First, the notion of "cyber-attacks" is frequently misunderstood. Despite speculation about the futuristic cyber warfare and cyber arms races, we have seen very few instances of this in the real world.
In Canada, we prefer to talk about cyber security because the real threats that we see every day are the use of cyberspace to facilitate crime. Criminals are taking advantage of the communications opportunities of the internet to steal identities, traffic in stolen data, and spread criminal material like child pornography. Sometimes it is led by organized crime; sometimes these crimes are perpetrated by individuals who are seeking thrills, pursuing a political agenda, or are trying to achieve notoriety or fame. As has been reported in the media, corporations and foreign governments use cyber space as a way to conduct espionage, such as to steal trade secrets and research. A U.S. Senator recently described these activities as "the biggest transfer of wealth through theft and piracy in the history of mankind."
Technology itself not responsible for these problems – the internet has had tremendous benefits. This is a case of criminals deliberately misusing and abusing the networks on which we rely. We need to remember that these crimes

don't just "happen." These threats exist because educated and skilled people invest huge effort to construct the software to do something illegal and then, quite deliberately, commit crimes for their personal gain.
These are the types of attacks we are seeing every day. So, while some commentators focus on largely hypothetical situations around cyber warfare, these issues are frankly far removed from what really affects people from day-to-day. The Government is committed to first addressing cyber threats that are most pressing for the country.

2) What is the government doing to make sure that our information is kept safe (which organizations -groups-centres-ministries are working on that topic)?

In October 2010 the Government of Canada released *Canada's Cyber Security Strategy*. The Strategy is founded on the idea of partnerships because, ultimately, the only way to improve our cyber security is by working together, both inside and outside government.
The first pillar of the Strategy is "Securing Government Systems" and the creation of Shared Services Canada is a great example of how we are moving to better protect Government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline the electronic network. In essence, this means that we will better know how our networks connect to the broader world, and be better able to protect them. Not only will this make our networks more secure, it will also be more efficient and improve services to Canadians.
The Government is also reaching out to other levels of government and to the private sector to ensure that critical pieces of our national infrastructure – such telecommunications networks, the financial sector, power grids and others vital systems – are getting the information they need to protect themselves and keep their systems secure. For example, the Canadian Cyber Incident Response Centre (CCIRC) monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with particular cyber threats.
Another important element of the Strategy is *Get Cyber Safe,* the Government of Canada's national public awareness initiative to help Canadians protect themselves and their families against a wide range of online threats.

3) Are we working with the American government to develop an international defense?

Cyber threats don't stop at borders.
Indeed the international nature of cyber activities has been a significant complication for the global community in effectively addressing these types of threats. It is important that all countries work together in the area of cyber security.
Because we are neighbors and our economies and infrastructure are so connected, we work closely with the United States.
With the release of the Perimeter Security and Economic Competitiveness Action Plan in December, Canada and the United States committed to enhancing our already strong bilateral cyber security cooperation to better protect vital government and critical digital infrastructure and increase both countries' ability to respond jointly and effectively to cyber incidents. Coordination between Canadian and U.S. cyber-security operations centers will be improved and allow for both our countries to better prevent and respond to cyber incidents.
The Government of Canada works closely with its national and international partners. At the United Nations, within NATO and the Organization of American States, at the Organization for Security and Co-operation in Europe and the G-8 and at so many other venues, we are hearing cyber security raised as a concern, and Canada is stepping forward to help be part of the solution.

4) How much money is the Canadian government spending on cyber war?

Canada's Cyber Security Strategy builds on existing programs and activities – our diplomatic efforts, our law enforcement and intelligence agencies, our connections to industry and academe.
Beyond the significant existing capability the Government already has for cyber security, we committed to investing $90 million over five years when we launched Canada's Cyber Security Strategy in 2010. We also began investing $18 million per year ongoing in cyber security to protect the security and economic prosperity of our digital infrastructure, as highlighted in the Government's 2010 Speech from the Throne.

Slack, Jessica

From: Swift, Andrew
Sent: September-20-12 11:27 AM
To: Slack, Jessica
Subject: Fw: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"
Attachments: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Sorry about that, didn't notice there was an attachment!

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Julie Gagnon [mailto:julie.gagnon@rcmp-grc.gc.ca]
Sent: Thursday, September 20, 2012 10:43 AM
To: Swift, Andrew
Cc: Greg Cox <Greg.Cox@rcmp-grc.gc.ca>; Marc Richer <Marc.Richer@rcmp-grc.gc.ca>
Subject: Fw: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Andrew,

Would this not be a request more for your shop than for RCMP?

Julie
Sgt. Julie Gagnon
RCMP National Communication Services / Services nationaux de communication de la GRC Sent from my wireless device
Depuis mon sans fil

Malik, Zarah

From: [redacted] <assistant@[redacted]> s.19(1)
Sent: Thursday, September 20, 2012 10:40 AM
To: Julie Gagnon
Subject: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Hello-

My name is [redacted] personal assistant to [redacted] a freelance journalist writing for SC Magazine.

[redacted] is writing an article regarding "How Safe Are Canada's Energy Companies?" [redacted] requested me to contact RCMP and ask if [redacted] could have a telephone interview with a view to quoting someone in the article.

The research deadline for the article is 1 October 2012. [redacted] must conduct all of [redacted] interviews by the close of play that day and preferably sooner if possible. [redacted] cannot conduct interviews after this deadline.

At the foot of this email is a brief for your review. [redacted] is eager to talk with you, and would be delighted if you were able to take part.

It would be hugely helpful if you could let me know as early as possible that you received this email, and whether you are interested, as [redacted] has to plan [redacted] interviewees in advance. If I do not hear from you in the next couple of days, I will call you. If I still cannot reach you, I will assume that you have declined and will advise [redacted] to pursue an alternative interviewee on [redacted] target list.

You are one of the first on our list of potential interviewees, so if you are unable or unwilling to take part, I would very much appreciate a response declining the opportunity ASAP. This helps me enormously when keeping [redacted] up to date on the status of potential interviews.

Some interviewees and their PR representatives have asked for a backgrounder of [redacted] before deciding on an interview, so I like to provide this up front when making initial requests. [redacted] web site is at [redacted] and you can see examples of his work there.

[redacted] is eager to include you in the finished article. I look forward to hearing from you to schedule a mutually convenient time.

Article Brief:

Publication: SC Magazine

Deadline: 1 October 2012

Energy is one of Canada's primary exports, and one of its most contentious issues. The Canadian tar sands have huge amounts of oil embedded in them, but extraction is a thorny issue, with many environmental worries. Consequently, Canadian energy companies have been the target of many threats from activist groups including Anonymous. With issues like the Enbridge pipeline gathering public attention, things are becoming increasingly tense, and the Canadian government has issued warnings to key stakeholders about these threats. How much of a threat is cyberactivism to Canadian oil, gas and other energy firms? To what extent does this threat move beyond simple web site defacement into

data breach territory, and potential attacks on SCADA systems? How secure are energy companies' networks and control infrastructures?

--
Best regards,

s.19(1)

Personal Assistant to

Follow on Twitter: http://twitter.com/

Slack, Jessica

From: Matz, Mark
Sent: September-27-12 2:29 PM
To: DeJong, Michael; Slack, Jessica; Wong, Suki
Cc: Filipps, Lisa; Duval, Jean Paul; Carta, John; Willey, Chris
Subject: Re: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

NCSD is fine with this message.

From: DeJong, Michael
Sent: Thursday, September 27, 2012 01:34 PM
To: Slack, Jessica; Matz, Mark; Wong, Suki
Cc: Filipps, Lisa; Duval, Jean Paul; Carta, John; Willey, Chris
Subject: RE: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Hi Jessica – we've added one line below - thx

From: Slack, Jessica
Sent: September-27-12 10:16 AM
To: Matz, Mark; DeJong, Michael; Wong, Suki
Cc: Filipps, Lisa; Duval, Jean Paul; Carta, John; Willey, Chris
Subject: FW: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Hi there,

See request we have received below – reporter initially went to RCMP and they directed him here.
We would propose declining the interview request and responding along the lines of the below.
Could you please advise by the end of the day if you are ok with this or have anything to add?
Let me know if you have any questions.
Many thanks,
Jessica

PROPOSED RESPONSE:
While we do not comment on specific or potential threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them. The Government also works in partnership with critical infrastructure sectors, including the energy sector, to identify and address risks and threats facing Canada's vital assets and systems.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Reporter's Name [redacted] s.19(1)

edia Outlet	SC Magazine
all Date	9/20/2012 2:00 PM
elephone	
mail address	assistant@
eadline	9/26/2012 12:00 AM
atus	Consulting
anch	NS
bject	CI / Cyberactivism
estions	Article brief:

Publication: SC Magazine
Deadline: 1 October 2012
Energy is one of Canada's primary exports, and one of its most contentious issues. The Canadian tar sands have huge amounts of oil embedded in them, but extraction is a thorny issue, with many environmental worries. Consequently, Canadian energy companies have been the target of many threats from activist groups including Anonymous. With issues like the Enbridge pipeline gathering public attention, things are becoming increasingly tense, and the Canadian government has issued warnings to key stakeholders about these threats. How much of a threat is cyberactivism to Canadian oil, gas and other energy firms? To what extent does this threat move beyond simple web site defacement into data breach territory, and potential attacks on SCADA systems? How secure are energy companies' networks and control infrastructures?

****

is writing an article regarding "How Safe Are Canada's Energy Companies?" requested me to contact RCMP and ask if could have a telephone interview with a view to quoting someone in the article.

The research deadline for the article is 1 October 2012. must conduct all of interviews by the close of play that day and preferably sooner if possible. cannot conduct interviews after this deadline.

At the foot of this email is a brief for your review. is eager to talk with you, and would be delighted if you were able to take part.

It would be hugely helpful if you could let me know as early as possible that you received this email, and whether you are interested, as has to plan interviewees in advance. If I do not hear from you in the next couple of days, I will call you. If I still cannot reach you, I will assume that you have declined and will advise to pursue an alternative interviewee on target list.

You are one of the first on our list of potential interviewees, so if you are unable or unwilling to take part, I would very much appreciate a response declining the opportunity ASAP. This helps me enormously when keeping up to date on the status of potential interviews.

Some interviewees and their PR representatives have asked for a backgrounder of before deciding on an interview, so I like to provide this up front when making initial requests.

web site is at and you can see examples of work there.

is eager to include you in the finished article. I look forward to hearing from you to schedule a mutually convenient time.

porter and Outlet	- SC Magazine
tions Taken	No existing entries.

Slack, Jessica

From: Swift, Andrew
Sent: September-27-12 2:56 PM
To: Slack, Jessica
Cc: Filipps, Lisa; Duval, Jean Paul
Subject: Re: FOR APPROVAL: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Approved, thx.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica
Sent: Thursday, September 27, 2012 02:33 PM
To: Swift, Andrew
Cc: Filipps, Lisa; Duval, Jean Paul
Subject: FOR APPROVAL: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Andrew- you may recall this request went to RCMP and RCMP referred it here. Reporter's assistant just came to us yesterday.

Here is proposed response. Approved by CI and NCSD.

FYI, I checked with NRCan to see if they had this request. They didn't. I advise them that the reporter may contact them next and said I would flip our response for their information.
Jessica

PROPOSED RESPONSE:

We respectfully decline your interview request.

While we do not comment on specific or potential threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them. The Government also works in partnership with critical infrastructure sectors, including the energy sector, to identify and address risks and threats facing Canada's vital assets and systems.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Reporter's Name	[redacted]
Media Outlet	SC Magazine
Call Date	9/20/2012 2:00 PM
Telephone	[redacted]
E-mail address	assistant@[redacted]
Deadline	9/26/2012 12:00 AM
Status	Consulting
Branch	NS
Subject	CI / Cyberactivism
Questions	Article brief:

Publication: SC Magazine
Deadline: 1 October 2012
Energy is one of Canada's primary exports, and one of its most contentious issues. The Canadian tar sands have huge amounts of oil embedded in them, but extraction is a thorny issue, with many environmental worries. Consequently, Canadian energy companies have been the target of many threats from activist groups including Anonymous. With issues like the Enbridge pipeline gathering public attention, things are becoming increasingly tense, and the Canadian government has issued warnings to key stakeholders about these threats. How much of a threat is cyberactivism to Canadian oil, gas and other energy firms? To what extent does this threat move beyond simple web site defacement into data breach territory, and potential attacks on SCADA systems? How secure are energy companies' networks and control infrastructures?

****

[redacted] is writing an article regarding "How Safe Are Canada's Energy Companies?" He requested me to contact RCMP and ask if [redacted] ould have a telephone interview with a view to quoting someone in the article.

The research deadline for the article is 1 October 2012. [redacted] must conduct all of [redacted] interviews by the close of play that day and preferably sooner if possible. He cannot conduct interviews after this deadline.

At the foot of this email is a brief for your review. [redacted] is eager to talk with you, and would be delighted if you were able to take part.

It would be hugely helpful if you could let me know as early as possible that you received this email, and whether you are interested, as [redacted] has to plan [redacted] interviewees in advance. If I do not hear from you in the next couple of days, I will call you. If I still cannot reach you, I will assume that you have declined and will advise [redacted] to pursue an alternative interviewee on [redacted] target list.

You are one of the first on our list of potential interviewees, so if you are unable or unwilling to take part, I would very much appreciate a response declining the opportunity ASAP. This helps me enormously when keeping [redacted] up to date on the status of potential interviews.

Some interviewees and their PR representatives have asked for a backgrounder of [redacted] before deciding on an interview, so I like to provide this up front when making initial requests. [redacted] web site is at [redacted] and you can see examples of [redacted] work there.

[redacted] is eager to include you in the finished article. I look forward to hearing from you to schedule a mutually convenient time.

Reporter and Outlet	[redacted] - SC Magazine

tions Taken

No existing entries.

Slack, Jessica

From: Tomlinson, Jamie
Sent: September-27-12 3:09 PM
To: Slack, Jessica; Salewski, Shawn; Dubé, Rosanne
Cc: Swift, Andrew; Filipps, Lisa; Duval, Jean Paul
Subject: Re: FOR APPROVAL: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Approved

From: Slack, Jessica
Sent: Thursday, September 27, 2012 03:04 PM
To: Tomlinson, Jamie; Salewski, Shawn; Dubé, Rosanne
Cc: Swift, Andrew; Filipps, Lisa; Duval, Jean Paul
Subject: FOR APPROVAL: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Hi Jamie,

For approval please. This has been approved by CI Policy, NCSD, Lisa and Andrew.
We will share with NRCan for their info.
Jessica

PROPOSED RESPONSE:

We respectfully decline your interview request.

While we do not comment on specific or potential threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them. The Government also works in partnership with critical infrastructure sectors, including the energy sector, to identify and address risks and threats facing Canada's vital assets and systems.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Reporter's Name	[redacted]	
Media Outlet	SC Magazine	s.19(1)
Call Date	9/20/2012 2:00 PM	
Telephone	[redacted]	
E-mail address	assistant@[redacted]	
Deadline	9/26/2012 12:00 AM	

Status	Consulting
Branch	NS
Subject	CI / Cyberactivism
Questions	Article brief: Publication: SC Magazine Deadline: 1 October 2012 Energy is one of Canada's primary exports, and one of its most contentious issues. The Canadian tar sands have huge amounts of oil embedded in them, but extraction is a thorny issue, with many environmental worries. Consequently, Canadian energy companies have been the target of many threats from activist groups including Anonymous. With issues like the Enbridge pipeline gathering public attention, things are becoming increasingly tense, and the Canadian government has issued warnings to key stakeholders about these threats. How much of a threat is cyberactivism to Canadian oil, gas and other energy firms? To what extent does this threat move beyond simple web site defacement into data breach territory, and potential attacks on SCADA systems? How secure are energy companies' networks and control infrastructures? ********** [redacted] is writing an article regarding "How Safe Are Canada's Energy Companies?" [redacted] requested me to contact RCMP and ask if [redacted] could have a telephone interview with a view to quoting someone in the article. The research deadline for the article is 1 October 2012. [redacted] must conduct all of [redacted] interviews by the close of play that day and preferably sooner if possible. [redacted] cannot conduct interviews after this deadline. At the foot of this email is a brief for your review. [redacted] is eager to talk with you, and would be delighted if you were able to take part. s.19(1) It would be hugely helpful if you could let me know as early as possible that you received this email, and whether you are interested, as [redacted] has to plan [redacted] interviewees in advance. If I do not hear from you in the next couple of days, I will call you. If I still cannot reach you, I will assume that you have declined and will advise [redacted] to pursue an alternative interviewee on [redacted] target list. You are one of the first on our list of potential interviewees, so if you are unable or unwilling to take part, I would very much appreciate a response declining the opportunity ASAP. This helps me enormously when keeping [redacted] up to date on the status of potential interviews. Some interviewees and their PR representatives have asked for a backgrounder of [redacted] before deciding on an interview, so I like to provide this up front when making initial requests. [redacted] [redacted] web site is at [redacted] and you can see examples of [redacted] work there. [redacted] is eager to include you in the finished article. I look forward to hearing from you to schedule a mutually convenient time.
Reporter and Outlet	[redacted] - SC Magazine
Actions Taken	No existing entries.

Duval, Jean Paul

From: PS Media Relations / Relations médias SP
Sent: Friday, September 28, 2012 10:41 AM
To: [redacted]
Subject: RE: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Good day [redacted]

We respectfully decline your interview request.

While we do not comment on specific or potential threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them. The Government also works in partnership with critical infrastructure sectors, including the energy sector, to identify and address risks and threats facing Canada's vital assets and systems.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

The CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Kind regards,

Jean Paul Duval
Spokesperson / Porte-parole
Media Relations / Relations avec les médias
Public Safety Canada / Sécurité publique Canada
613-991-0657
media@ps-sp.gc.ca

From: [redacted] [mailto:assistant@[redacted]
Sent: Wednesday, September 26, 2012 4:52 PM
To: PS Media Relations / Relations médias SP
Subject: PR Interview Request - SC Magazine "How Safe Are Canada's Energy Companies"

Hello-

My name is [redacted] personal assistant to [redacted] a freelance journalist writing for SC Magazine.

[redacted] is writing an article regarding "How Safe Are Canada's Energy Companies?" [redacted] requested me to contact Public Safety Canada and ask if [redacted] could have a telephone interview with a view to quoting someone in the article.

The research deadline for the article is 1 October 2012. [redacted] must conduct all of [redacted] interviews by the close of play that day and preferably sooner if possible. [redacted] cannot conduct interviews after this deadline.

At the foot of this email is a brief for your review. [redacted] is eager to talk with you, and would be delighted if you were

able to take part.

It would be hugely helpful if you could let me know as early as possible that you received this email, and whether you are interested, as has to plan interviewees in advance. If I do not hear from you in the next couple of days, I will call you. If I still cannot reach you, I will assume that you have declined and will advise to pursue an alternative interviewee on target list.

You are one of the first on our list of potential interviewees, so if you are unable or unwilling to take part, I would very much appreciate a response declining the opportunity ASAP. This helps me enormously when keeping up to date on the status of potential interviews.

Some interviewees and their PR representatives have asked for a backgrounder of before deciding on an interview, so I like to provide this up front when making initial requests.

web site is at www.itjournalist.com and you can see examples of work there.

is eager to include you in the finished article. I look forward to hearing from you to schedule a mutually convenient time.

Article Brief:

Publication: SC Magazine

Deadline: 1 October 2012

Energy is one of Canada's primary exports, and one of its most contentious issues. The Canadian tar sands have huge amounts of oil embedded in them, but extraction is a thorny issue, with many environmental worries. Consequently, Canadian energy companies have been the target of many threats from activist groups including Anonymous. With issues like the Enbridge pipeline gathering public attention, things are becoming increasingly tense, and the Canadian government has issued warnings to key stakeholders about these threats. How much of a threat is cyberactivism to Canadian oil, gas and other energy firms? To what extent does this threat move beyond simple web site defacement into data breach territory, and potential attacks on SCADA systems? How secure are energy companies' networks and control infrastructures?

--
Best regards,

Personal Assistant to

Follow on Twitter: http://twitter.com/

Pages 513 to / à 514
are duplicates of
sont des duplicatas des
pages 516 to / à 517

Swift, Andrew

From: Filipps, Lisa
Sent: Thursday, October 25, 2012 1:57 PM
To: Champoux, Martin
Cc: Swift, Andrew
Subject: FW: Information Note IN12-002: Anonymous DDoS activity against GC

Categories: ATI PRINT

Martin – can you work up some holding lines (we do not comment on security related matters, that said, we are working with partners to ensure vital government systems are safe...etc!)

Would be great if we could share something out with departments tomorrow morning. We could forward the lines along with the CCIRC notification.

Thanks!

From: Swift, Andrew
Sent: Thursday, October 25, 2012 1:54 PM
To: Filipps, Lisa
Cc: Champoux, Martin
Subject: RE: Information Note IN12-002: Anonymous DDoS activity against GC

Thanks. Is this not worth flagging to our core cyber fed depts. group and developing suggested holding lines? If a planned attack that we are aware of is not worthy, what would be?

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Filipps, Lisa
Sent: Thursday, October 25, 2012 1:28 PM
To: Swift, Andrew
Cc: Champoux, Martin
Subject: FW: Information Note IN12-002: Anonymous DDoS activity against GC
Importance: High

Andrew – I briefed Stéphanie on this a little bit yesterday although I wasn't aware that it was Anonymous or that there was a scheduled operation date. Martin did let me know that the service providers are managing the issue and that users in departments shouldn't notice anything.

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 1:24 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
==========

[redacted]

To report any outages or suspicious network activities that require mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@tpsgc-pwgsc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Champoux, Martin

From: Champoux, Martin
Sent: Thursday, October 25, 2012 4:03 PM
To: Slack, Jessica
Subject: FW: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 3:08 PM
To: CTEC
Subject: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: UNCLASSIFIED

La version française suit.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 1:

We have corrected the e-mail address for SSC to RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca

[redacted]

French version is now attached and reflects this update.
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

[redacted]

SUGGESTED ACTION
==========

[redacted]

To report any outages or suspicious network activities that require mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contain information which may have been collected from external sources for which GC CTEC cannot verify the accuracy and integrity. GC CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

==========
CECM-GC – Note d'information IN12-002
Date : 25 octobre 2012
==========

==========

Update 1:

Voici la bonne adresse de courriel de SPC : RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca.

[redacted]

Vous trouverez ci-joint la version française qui reflète ce changement.

==========

==========

Anonymous – Attaque par déni de service distribué visant le GC

==========

PUBLIC

======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

ÉVALUATION

==========

[redacted]

MESURES RECOMMANDÉES

==========

[redacted]

Pour signaler toute interruption de service ou activité réseau suspecte aux fins d'atténuation, veuillez communiquer avec les deux entités suivantes :

- l'agent de service du Centre de protection de l'information (CPI) de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;

- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse cst.gc.ca.

==========

Le présent message et ses pièces jointes contiennent des renseignements pouvant provenir de sources externes et dont le CECM-GC ne peut pas vérifier l'exactitude ni l'intégrité. Le CECM-GC ne sera pas responsable des conséquences négatives résultant de l'utilisation de ces renseignements.

Les liens vers les sites Web sur lesquels le gouvernement du Canada n'exerce aucun contrôle sont fournis aux utilisateurs pour des raisons de commodité seulement. Le GC n'est pas responsable de l'exactitude, de l'actualité ni de la fiabilité du contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites ou leur contenu.

Note aux lecteurs
==========
Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Austria, Jamela

From: Matz, Mark
Sent: Thursday, October 25, 2012 10:57 PM
To: Champoux, Martin
Cc: Hatfield, Adam; Labelle, Sébastien; Anderson, Windy; Weir, Sarah; Fortunato, Stephanie; Filipps, Lisa; Slack, Jessica; Duval, Jean Paul; Austria, Jamela
Subject: Re: FOR APPROVAL Media Lines on Anonymous

These are good - approved!

Thanks - mark

From: Champoux, Martin
Sent: Thursday, October 25, 2012 04:00 PM
To: Matz, Mark
Cc: Hatfield, Adam; Labelle, Sébastien; Anderson, Windy; Weir, Sarah; Fortunato, Stephanie; Filipps, Lisa; Slack, Jessica; Duval, Jean Paul; Austria, Jamela
Subject: FOR APPROVAL Media Lines on Anonymous

Mark

As you know CCIRC sent out a Cyber Notification yesterday followed by one from CTEC today on Anonymous' plan for DDOS attacks on government websites. Since Anonymous has a habit of publicizing its activities we have prepared anticipatory media lines **for your approval**. Thanks

Martin

Media Lines

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy. Furthermore we are investing an additional $155 million in cyber security.

Austria, Jamela

From: Austria, Jamela
Sent: Thursday, October 25, 2012 4:06 PM
To: Carta, John; Willey, Chris
Subject: FW: FOR APPROVAL Media Lines on Anonymous

FYI:

From: Champoux, Martin
Sent: Thursday, October 25, 2012 4:00 PM
To: Matz, Mark
Cc: Hatfield, Adam; Labelle, Sébastien; Anderson, Windy; Weir, Sarah; Fortunato, Stephanie; Filipps, Lisa; Slack, Jessica; Duval, Jean Paul; Austria, Jamela
Subject: FOR APPROVAL Media Lines on Anonymous

Mark

As you know CCIRC sent out a Cyber Notification yesterday followed by one from CTEC today on Anonymous' plan for DDOS attacks on government websites. Since Anonymous has a habit of publicizing its activities we have prepared anticipatory media lines **for your approval**. Thanks

Martin

Media Lines

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy. Furthermore we are investing an additional $155 million in cyber security.

Pages 524 to / à 526
are duplicates of
sont des duplicatas des
pages 536 to / à 538

Pages 527 to / à 529

are duplicates of

sont des duplicatas des

pages 536 to / à 538

Dubé, Rosanne

From: Dubé, Rosanne
Sent: Friday, October 26, 2012 11:48 AM
To: Salewski, Shawn; Bue, Richard
Subject: RE: FOR APPROVAL Media Lines on Anonymous

Printed

Rosanne Dubé
Administrative Officer | Agente administrative
Office of the Director General, Communications | Bureau de la Directrice générale, Communications
Public Safety Canada | Sécurité publique Canada
Ottawa, Canada K1A 0P8
Telephone | Téléphone 613 949-4485 / Facsimile | Télécopieur 613 993-7062

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

October is Cyber Security Awareness Month

Octobre est le Mois de la sensibilisation à la cybersécurité

For information on how to stay safe online, please visit GETCYBERSAFE.CA

Pour des renseignements sur la façon de vous protéger en ligne, veuillez consulter PENSEZCYBERSECURITE.CA

From: Slack, Jessica
Sent: Friday, October 26, 2012 11:40 AM
To: Durand, Stéphanie; Bue, Richard; Salewski, Shawn; Dubé, Rosanne
Cc: Swift, Andrew; Champoux, Martin; Wilson, Barbara; Duval, Jean Paul; Carta, John; Austria, Jamela
Subject: FOR APPROVAL Media Lines on Anonymous

Hi Stéphanie,

CCIRC and CTEC have sent out notifications regarding Anonymous' plan for Distributed Denial of Service attacks on government websites. CTEC notice is below for further context.

We pulled together a few responsive lines anticipatorily. Please advise if you approve and we will move to MO for their awareness and approval.

We have consulted with Mark Matz in NCSD and Lisa and Andrew have approved.

Many thanks,
Jessica

Media Lines

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 3:08 PM
To: CTEC
Subject: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: UNCLASSIFIED

La version française suit.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 1:

We have corrected the e-mail address for SSC to RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca

[redacted]

French version is now attached and reflects this update.
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
==========

To report any outages or suspicious network activities that require mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contain information which may have been collected from external sources for which GC CTEC cannot verify the accuracy and integrity. GC CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Pages 533 to / à 535
are duplicates of
sont des duplicatas des
pages 536 to / à 538

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Friday, October 26, 2012 11:58 AM
To: Swift, Andrew; Slack, Jessica; Bue, Richard; Salewski, Shawn; Dubé, Rosanne
Cc: Champoux, Martin; Wilson, Barbara; Duval, Jean Paul; Carta, John; Austria, Jamela
Subject: RE: FOR APPROVAL Media Lines on Anonymous

Thx – I signed off on lines.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Swift, Andrew
Sent: Friday, October 26, 2012 11:42 AM
To: Slack, Jessica; Durand, Stéphanie; Bue, Richard; Salewski, Shawn; Dubé, Rosanne
Cc: Champoux, Martin; Wilson, Barbara; Duval, Jean Paul; Carta, John; Austria, Jamela
Subject: Re: FOR APPROVAL Media Lines on Anonymous

Shared Services has also asked for our lines.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica
Sent: Friday, October 26, 2012 11:39 AM
To: Durand, Stéphanie; Bue, Richard; Salewski, Shawn; Dubé, Rosanne
Cc: Swift, Andrew; Champoux, Martin; Wilson, Barbara; Duval, Jean Paul; Carta, John; Austria, Jamela
Subject: FOR APPROVAL Media Lines on Anonymous

Hi Stéphanie,

CCIRC and CTEC have sent out notifications regarding Anonymous' plan for Distributed Denial of Service attacks on government websites. CTEC notice is below for further context.

We pulled together a few responsive lines anticipatorily. Please advise if you approve and we will move to MO for their awareness and approval.

We have consulted with Mark Matz in NCSD and Lisa and Andrew have approved.

Many thanks,
Jessica

Media Lines

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 3:08 PM
To: CTEC
Subject: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: UNCLASSIFIED

La version française suit.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 1:

We have corrected the e-mail address for SSC to RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca

[redacted]

French version is now attached and reflects this update.
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
==========

[redacted]

To report any outages or suspicious network activities that require mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contain information which may have been collected from external sources for which GC CTEC cannot verify the accuracy and integrity. GC CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Page 539

is a duplicate of

est un duplicata de la

page 546

Pages 540 to / à 541

are duplicates of

sont des duplicatas des

pages 553 to / à 554

Page 542

is a duplicate of

est un duplicata de la

page 546

Pages 543 to / à 544

are duplicates of

sont des duplicatas des

pages 553 to / à 554

Swift, Andrew

From: Williams, Christopher <Christopher.Williams@pco-bcp.gc.ca>
Sent: Friday, October 26, 2012 3:02 PM
To: Swift, Andrew; Slack, Jessica; Thibouthot, AkimIsabelle
Cc: Wilson, Barbara; Durand, Stéphanie
Subject: Re: FOR APPROVAL - anticipatory media lines on Anonymous' attacks on GOC websites

Categories: ATI PRINT

Hi Andrew,

Good to go with your message. We can confirm PS is the lead and the protocol should be to send calls your way.

Without knowing who is affected, it is tough to know what other depts to target. What I suggest is to stick to list you note, include me and I will fan it out to my analyst colleagues to share with their depts.

Thanks!

From: Swift, Andrew [mailto:Andrew.Swift@ps-sp.gc.ca]
Sent: Friday, October 26, 2012 02:53 PM
To: Williams, Christopher; Slack, Jessica <Jessica.Slack@ps-sp.gc.ca>; Thibouthot, Akim Isabelle
Cc: Wilson, Barbara <Barbara.Wilson@ps-sp.gc.ca>; Durand, Stéphanie <Stephanie.Durand@ps-sp.gc.ca>
Subject: RE: FOR APPROVAL - anticipatory media lines on Anonymous' attacks on GOC websites

Chris,
As discussed, we will prepare a note to PWGSC, TBS, CSEC, CSIS, RCMP, and any others you recommend, with the media relations protocol should this issue arise over the weekend.
Can you confirm that the agreed upon lead is PS? We'll have the note ready to go.
Thx.
Andrew

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Williams, Christopher [mailto:Christopher.Williams@pco-bcp.gc.ca]
Sent: Friday, October 26, 2012 2:25 PM
To: Slack, Jessica; Thibouthot, AkimIsabelle
Cc: Swift, Andrew; Wilson, Barbara
Subject: RE: FOR APPROVAL - anticipatory media lines on Anonymous' attacks on GOC websites

Thanks. We understand that some depts. may already be experiencing some difficulties in relation to the threat. Have you heard anything?

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: Friday, October 26, 2012 1:31 PM
To: Williams, Christopher; Thibouthot, Akim Isabelle
Cc: Swift, Andrew; Wilson, Barbara
Subject: FW: FOR APPROVAL - anticipatory media lines on Anonymous' attacks on GOC websites

FYI...we will share with CSEC and SSC and advise if we get any calls...
Let us know if there are any concerns.

From: Carmichael, Julie
Sent: October-26-12 1:28 PM
To: Slack, Jessica; Mueller, Mike; Johnson, Mark; McGrath, Andrew
Cc: Swift, Andrew; Durand, Stéphanie; Carta, John; Austria, Jamela; Wilson, Barbara; Champoux, Martin
Subject: Re: FOR APPROVAL - anticipatory media lines on Anonymous' attacks on GOC websites

Approved

Julie Carmichael
Director of Communications
Office of the Minister of Public Safety

From: Slack, Jessica
Sent: Friday, October 26, 2012 01:10 PM
To: Carmichael, Julie; Mueller, Mike; Johnson, Mark; McGrath, Andrew
Cc: Swift, Andrew; Durand, Stéphanie; Carta, John; Austria, Jamela; Wilson, Barbara; Champoux, Martin
Subject: FOR APPROVAL - anticipatory media lines on Anonymous' attacks on GOC websites

Hi Julie,

CCIRC and CTEC have sent out notifications regarding Anonymous' plan for Distributed Denial of Service attacks on government websites. CTEC notice is below for further context.

We pulled together a few responsive lines anticipatorily. We have not yet received calls or seen media coverage, however Shared Services has requested our lines so please advise if you are ok with the following and we will share.

We will of course flag calls if we get them.

Many thanks,
Jessica

Media Lines

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

Pages 547 to / à 548

are duplicates of

sont des duplicatas des

pages 553 to / à 554

Slack, Jessica

From: Slack, Jessica
Sent: October-26-12 4:25 PM
To: Swift, Andrew
Subject: RE: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2

Ok thanks. I don't get these so I didn't realize there was an update!
The note is good to go? I will include MR contact info and CC you and Chris.

-----Original Message-----
From: Swift, Andrew
Sent: October-26-12 4:24 PM
To: Slack, Jessica
Subject: FW: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2
Importance: High

Use this note from CTEC instead.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques Communications Directorate | Direction générale des communications Public Safety Canada | Sécurité publique Canada Telephone | Téléphone : 613-991-3549 Fax | Télécopieur : 613-954-2000 Email | Courriel : Andrew.Swift@ps-sp.gc.ca

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, October 26, 2012 4:23 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 2: 26 October 2012
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
================

[redacted]

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both :

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Wilson, Barbara

From: Wilson, Barbara
Sent: Friday, October 26, 2012 4:28 PM
To: Slack, Jessica
Subject: FW: FOR APPROVAL - anticipatory media lines on Anonymous' attacks on GOC websites

Whichever way you wish Jess – if you want to send it out, just cc me. If you want me to do it, send me the list.

Barbara Wilson
Senior Communications Advisor
Issues management and media relations
Conseillère principale en communications
Gestion des enjeux et relations avec les médias
Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue W/ 269, avenue Laurier ouest
Ottawa, (ON) K1P 0P8
(613) 944-4920
barbara.wilson@ps-sp.gc.ca

From: Swift, Andrew
Sent: Friday, October 26, 2012 4:27 PM
To: Slack, Jessica
Cc: Champoux, Martin; Wilson, Barbara
Subject: RE: FOR APPROVAL - anticipatory media lines on Anonymous' attacks on GOC websites

Minor changes. Please send it out to media relations contacts.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica
Sent: Friday, October 26, 2012 3:52 PM
To: Swift, Andrew
Cc: Champoux, Martin; Wilson, Barbara
Subject: FW: FOR APPROVAL - anticipatory media lines on Anonymous' attacks on GOC websites

Andrew- suggested note. Let me know if it works and if you are sending or if you want me or Barb to send on behalf of MR.
I will whip up a dist list in the meantime...

Colleagues,

Further to the note below (issued by CTEC yesterday) regarding Anonymous' plan for Distributed Denial of Service attacks on government websites, we wanted to touch base regarding the media relations protocol in advance of the weekend.

Direction (DELETE: from PCO) at this time is that all departments should send any calls they receive to Public Safety for response (media@ps-sp.gc.ca / 613-991-0657).

The approved media lines are below for your information.

Please do not hesitate to get in touch should you have any questions. We will be in touch next week.

Regards,

Media Lines

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 3:08 PM
To: CTEC
Subject: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: UNCLASSIFIED

La version française suit.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 1:

We have corrected the e-mail address for SSC to RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca

French version is now attached and reflects this update.
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
==========

[redacted]

To report any outages or suspicious network activities that require mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to

cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Swift, Andrew

From: Swift, Andrew
Sent: Friday, October 26, 2012 4:34 PM
To: Durand, Stéphanie
Subject: FW: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Categories: ATI PRINT

FYI

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica **On Behalf Of** PS Media Relations / Relations médias SP
Sent: Friday, October 26, 2012 4:33 PM
To: [redacted]@cse-cst.gc.ca; [redacted]@cse-cst.gc.ca; julie.gagnon@rcmp-grc.gc.ca; [redacted] Theresa.Knowles@tbs-sct.gc.ca; TBS Media / Média SCT; mylene.dupere@tpsgc-pwgsc.gc.ca; ted.francis@ssc-spc.gc.ca; sebastien.bois@tpsgc-pwgsc.gc.ca; Isabelle.Scott@cra-arc.gc.ca
Cc: Champoux, Martin; Wilson, Barbara; Swift, Andrew; Williams, Christpher; Duval, Jean Paul; Carta, John
Subject: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Colleagues,

Further to the note below (issued by CTEC) regarding Anonymous' plan for Distributed Denial of Service attacks on government websites, we wanted to touch base regarding the media relations protocol in advance of the weekend.

Direction at this time is that all departments should send any calls they receive to Public Safety for response (our contact info: media@ps-sp.gc.ca / 613-991-0657)

The approved media lines are below for your information.

Please do not hesitate to get in touch should you have any questions.

We will be in touch further next week.

Many thanks,

Jessica

Media Lines

Pages 557 to / à 558

are duplicates of

sont des duplicatas des

pages 566 to / à 567

Pages 559 to / à 561
are duplicates of
sont des duplicatas des
pages 562 to / à 564

Durand, Stéphanie

From: Salewski, Shawn
Sent: Friday, October 26, 2012 4:49 PM
To: Carta, John; Swift, Andrew
Cc: Durand, Stéphanie
Subject: FW: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2

Importance: High

FYI - as per email Stephanie just sent via John Carta

-----Original Message-----
From: Anderson, Windy
Sent: Friday, October 26, 2012 4:40 PM
To: Durand, Stéphanie
Subject: Fw: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2
Importance: High

Fyi

----- Original Message -----
From:
Sent: Friday, October 26, 2012 04:34 PM
To: Anderson, Windy
Cc: * CyberIH; Beaudoin, Luc; Clow, Patrick; Bendelier, Kenneth
Subject: FW: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2

Updated IN from CTEC. Essentially states who to contact...

\\\\\

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both :

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

\\\\\

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, October 26, 2012 4:23 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 2: 26 October 2012
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
==========

[redacted]

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both :

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Carta, John

From: Salewski, Shawn on behalf of Durand, Stéphanie
Sent: October-26-12 4:51 PM
To: Carta, John
Subject: FW: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

FYI for Stephanie

From: Swift, Andrew
Sent: Friday, October 26, 2012 4:34 PM
To: Durand, Stéphanie
Subject: FW: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

FYI

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica **On Behalf Of** PS Media Relations / Relations médias SP
Sent: Friday, October 26, 2012 4:33 PM
To: [redacted]@cse-cst.gc.ca; [redacted]@cse-cst.gc.ca; julie.gagnon@rcmp-grc.gc.ca; [redacted] Theresa.Knowles@tbs-sct.gc.ca; TBS Media / Média SCT; mylene.dupere@tpsgc-pwgsc.gc.ca; ted.francis@ssc-spc.gc.ca; sebastien.bois@tpsgc-pwgsc.gc.ca; Isabelle.Scott@cra-arc.gc.ca
Cc: Champoux, Martin; Wilson, Barbara; Swift, Andrew; Williams, Christpher; Duval, Jean Paul; Carta, John
Subject: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Colleagues,

Further to the note below (issued by CTEC) regarding Anonymous' plan for Distributed Denial of Service attacks on government websites, we wanted to touch base regarding the media relations protocol in advance of the weekend.

Direction at this time is that all departments should send any calls they receive to Public Safety for response (our contact info: media@ps-sp.gc.ca / 613-991-0657)

The approved media lines are below for your information.

Please do not hesitate to get in touch should you have any questions.

We will be in touch further next week.

Many thanks,

Jessica

Media Lines

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, October 26, 2012 4:23 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 2: 26 October 2012
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

[redacted]

SUGGESTED ACTION
==========

[redacted]

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both :

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Swift, Andrew

From: Carta, John
Sent: Friday, October 26, 2012 4:55 PM
To: Swift, Andrew
Cc: Salewski, Shawn
Subject: Re: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Categories: ATI PRINT

Super, thanks.
Steph

From: Swift, Andrew
Sent: Friday, October 26, 2012 04:54 PM
To: Carta, John
Cc: Salewski, Shawn
Subject: RE: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Yes, it was PCO who confirmed the protocol and I spoke to Julie about it.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Carta, John
Sent: Friday, October 26, 2012 4:53 PM
To: Swift, Andrew
Cc: Salewski, Shawn
Subject: Fw: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Steph here.
Had you checked with Min Off and PCO?

From: PS Media Relations / Relations médias SP
Sent: Friday, October 26, 2012 04:33 PM
To: @cse-cst.gc.ca <@cse-cst.gc.ca>; @cse-cst.gc.ca @cse-cst.gc.ca>; julie.gagnon@rcmp-grc.gc.ca <julie.gagnon@rcmp-grc.gc.ca>; ; Theresa.Knowles@tbs-sct.gc.ca <Theresa.Knowles@tbs-sct.gc.ca>; TBS Media / Média SCT <media@tbs-sct.gc.ca>; mylene.dupere@tpsgc-pwgsc.gc.ca <mylene.dupere@tpsgc-pwgsc.gc.ca>; ted.francis@ssc-spc.gc.ca <ted.francis@ssc-spc.gc.ca>; sebastien.bois@tpsgc-pwgsc.gc.ca <sebastien.bois@tpsgc-pwgsc.gc.ca>; Isabelle.Scott@cra-arc.gc.ca <Isabelle.Scott@cra-arc.gc.ca>
Cc: Champoux, Martin; Wilson, Barbara; Swift, Andrew; Williams, Christpher; Duval, Jean Paul; Carta, John
Subject: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Colleagues,

Pages 570 to / à 572

are duplicates of

sont des duplicatas des

pages 613 to / à 615

Champoux, Martin

From: Champoux, Martin
Sent: Monday, October 29, 2012 8:57 AM
To: Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: FW: Information Note IN12-002: Anonymous DDoS activity against GC - Update 4

Importance: High

FYI

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Sunday, October 28, 2012 6:57 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 4
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 28 October 2012
==========

==========
Update 4: 28 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
==========

[redacted]

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:

- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca.

Slack, Jessica

From: Slack, Jessica
Sent: October-29-12 10:35 AM
To: Champoux, Martin
Subject: RE: Media lines - DDoS/ Anonymous

Martin, will let you weigh in on that as appropriate...

From: Scott, Isabelle [mailto:Isabelle.Scott@cra-arc.gc.ca]
Sent: October-29-12 10:31 AM
To: Slack, Jessica; Champoux, Martin
Subject: RE: Media lines - DDoS/ Anonymous

Hi,

As discussed Friday, do you know the likelihood of the govt. websites going down because of Anonymous' attack?

Isabelle

Isabelle Scott

Issues and Program Communications Manager | Gestionnaire d'enjeux et de la communication des programmes
Communications Directorate | Direction des communications
Public Affairs Branch | Direction générale des affaires publiques
Canada Revenue Agency | Agence du revenu du Canada
555 MacKenzie Ottawa ON K1A 0L5
Isabelle.Scott@cra-arc.gc.ca
Telephone | Téléphone 613-948-7872
Facsimile | Télécopieur 613-954-5456
Government of Canada | Gouvernement du Canada

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: October 26, 2012 2:32 PM
To: ted.francis@ssc-spc.gc.ca; Scott, Isabelle; [redacted]@cse-cst.gc.ca; [redacted]@cse-cst.gc.ca
Cc: Filipps, Lisa; Champoux, Martin; Wilson, Barbara; Duval, Jean Paul
Subject: Media lines - DDoS/ Anonymous

Colleagues,

Below are our MO approved lines.

Grateful if you could advise of any media calls you may receive.

Many thanks,
Jessica

Jessica Slack
Media Relations
613-949-4288

Page 577

is a duplicate of

est un duplicata de la

page 553

Page 578

is a duplicate of

est un duplicata de la

page 555

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Monday, October 29, 2012 11:11 AM
To: Swift, Andrew
Subject: RE: CYBER NOTIFICATION-12-014-1 – LOW IMPACT SEVERITY – MEDIA INTEREST– Distributed Denial-of-Service Attacks Targeting Government Entities (UPDATE One)

Thx

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Swift, Andrew
Sent: Monday, October 29, 2012 11:06 AM
To: Durand, Stéphanie
Subject: RE: CYBER NOTIFICATION-12-014-1 – LOW IMPACT SEVERITY – MEDIA INTEREST– Distributed Denial-of-Service Attacks Targeting Government Entities (UPDATE One)

Thx. You, Martin, Lisa and I get them as well when they are sent to the GOC (today @ 10:32 a.m.)

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Durand, Stéphanie
Sent: Monday, October 29, 2012 11:01 AM
To: Dick, Robert; Wong, Suki; Gordon, Robert; Swift, Andrew
Subject: Re: CYBER NOTIFICATION-12-014-1 – LOW IMPACT SEVERITY – MEDIA INTEREST– Distributed Denial-of-Service Attacks Targeting Government Entities (UPDATE One)

Thanks.
Andrew: fyi

From: Dick, Robert
Sent: Monday, October 29, 2012 10:36 AM
To: Wong, Suki; Durand, Stéphanie; Gordon, Robert

Subject: Fw: CYBER NOTIFICATION-12-014-1 – LOW IMPACT SEVERITY – MEDIA INTEREST– Distributed Denial-of-Service Attacks Targeting Government Entities (UPDATE One)

From: Klassen, Nathan
Sent: Monday, October 29, 2012 10:24 AM
To: Dick, Robert; Matz, Mark; Hatfield, Adam; Labelle, Sébastien; Anderson, Windy; Gordon, Robert
Cc: Bendelier, Kenneth; Proulx, Véronique; Pacha, Tomasz; Beaudoin, Luc; Clow, Patrick; Fortunato, Stephanie; Proulx, Véronique
Subject: CYBER NOTIFICATION-12-014-1 – LOW IMPACT SEVERITY – MEDIA INTEREST– Distributed Denial-of-Service Attacks Targeting Government Entities (UPDATE One)

CYBER NOTIFICATION – INCIDENT

Note: Updates / Changes in **BOLD** text

Incident Number: CNT-12-014-**1** – LOW IMPACT SEVERITY – MEDIA INTEREST

Description of Incident: CCIRC has become aware of distributed denial-of-service (DDoS) attacks that are currently targeting municipal, provincial, and federal government entities.

Sources of reporting: Trusted partners and open sources.

Current actions: CCIRC has directly notified its affected partners, and is collaborating with federal and non-federal partners to further assess the situation. CCIRC will continue to monitor and if necessary, will release further products. CCIRC's DDoS mitigation guidelines are available on its website.

Initial analysis / assessment:

-
- Partners at the federal level have already reported these attacks.
- According to open source reports, it is possible that these attacks may also target Canadian political entities at various levels,
- CCIRC is aware, through open source reports, that Anonymous has been promoting two operations, named *#opf***harper* and *#oppartycrasher*, which call for DDoS attacks against government targets, beginning on November 3, 2012.
- **Shared Services Canada is the lead on this incident and the Canadian Security Establishment is providing coordination support. CCIRC will continue to monitor the situation and will inform its affected partners if necessary.**

Disclaimer:

This notification is only for distribution within Public Safety Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Nate Klassen & Gregg Murphy (991-6052 & 991-3579)
Approved by: Ken Bendelier (993-5042)

s.16(2)

Champoux, Martin

From: Champoux, Martin
Sent: Monday, October 29, 2012 10:20 PM
To: Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Fw: Update 5: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Fyi

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Monday, October 29, 2012 04:27 PM
To: CTEC <CTEC@CSE-CST.GC.CA>
Subject: Update 5: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 29 October 2012
==========

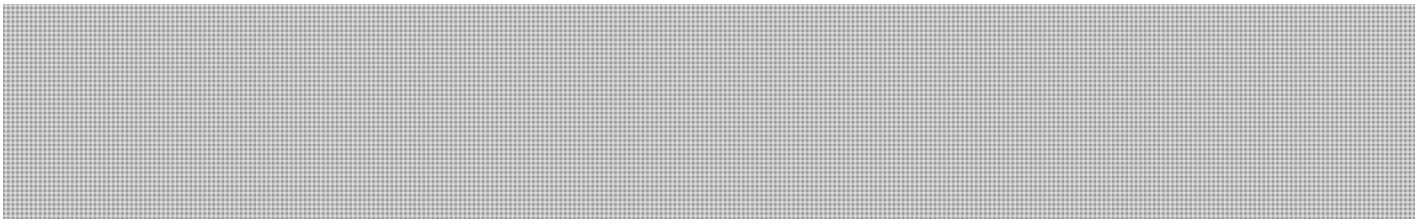
==========
Update 5: 29 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========



[redacted]

SUGGESTED ACTION
==========

[redacted]

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:

- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca.

Slack, Jessica

From: [redacted]@CSE-CST.GC.CA>
Sent: October-30-12 11:26 AM
To: Slack, Jessica
Cc: Duval, Jean Paul; Wilson, Barbara
Subject: RE: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Classification: UNCLASSIFIED

sorry. It should have been [redacted]

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: October 30, 2012 10:54 AM
To: [redacted]
Cc: Duval, Jean Paul; Wilson, Barbara
Subject: FW: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS
Importance: High

Can you double-check the phone number you gave us please?

From: [redacted]
Sent: Tuesday, October 30, 2012 10:15:41 AM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject: FW: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Classification: UNCLASSIFIED

Hello,

We received a call yesterday on our media line (actually the same gentleman called three times). [redacted] and so did not get the call.

His name is [redacted] (?)
Radio 147 (?) or 48
[redacted]

He wants to discuss Anonymous and the recent attacks DDoS on GoC departments.

As per instructions below, I have not called him back. Please call him asap. His third voice-mail from about at 1 p.m. yesterday was very unhappy.

Thank you.

[redacted]
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada
Ottawa, Canada K1G 3Z4
[redacted]@cse-cst.gc.ca

Pages 586 to / à 588
are duplicates of
sont des duplicatas des
pages 613 to / à 615

Austria, Jamela

From: Slack, Jessica
Sent: Tuesday, October 30, 2012 11:52 AM
To: Matz, Mark
Cc: Fortunato, Stephanie; Wilson, Barbara; Champoux, Martin; Duval, Jean Paul; Anderson, Windy; Austria, Jamela; Carta, John; Willey, Chris; Weir, Sarah; Dick, Robert; Hatfield, Adam
Subject: FYI: MEDIA CALL ON ANONYMOUS

Hi Mark,

The call below was referred to us by CSEC. We are having the lines that were approved translated now with a view to responding asap this afternoon.

Jessica

RESPONSE:

The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

Reporter's Name	[redacted]
Media Outlet	104.7 FM Gatineau
Call Date	10/30/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	10/30/2012 3:00 PM
Status	Consulting
Branch	
Subject	Cyber attacks
Questions	J'ai entendu que Anonymous tente d'infiltrer le réseau du Gouvenment du Canada avec une campagne d'attaques du 3-15 nov. Selon un courriel qui circule dans divers départements du gouvernement fédéral. Comment est-ce que le Gouvernement se prépare? Que faites vous? Entrevue de 4-6 mins (pré-enregistré ou en direct)

Slack, Jessica

From: Swift, Andrew
Sent: October-30-12 12:02 PM
To: Slack, Jessica
Cc: Champoux, Martin; Wilson, Barbara; Duval, Jean Paul
Subject: Re: FYI: MEDIA CALL ON ANONYMOUS

Agreed, thx.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: Slack, Jessica
Sent: Tuesday, October 30, 2012 11:56 AM
To: Swift, Andrew
Cc: Champoux, Martin; Wilson, Barbara; Duval, Jean Paul
Subject: FW: FYI: MEDIA CALL ON ANONYMOUS

Hi Andrew- for approval please. We have sent these lines to translation, but assume we are ok to proceed with Jamie and Julie's approval in the meantime?

I sent NCSD a heads-up and cc'ed [redacted] and co at Secure Tech a note for their awareness.
Once Julie approves, will send to PCO as FYI...

The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

Reporter's Name	[redacted]
Media Outlet	104.7 FM Gatineau
Call Date	10/30/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	10/30/2012 3:00 PM
Status	Consulting
Branch	
Subject	Cyber attacks

Questions

J'ai entendu que Anonymous tente d'infiltrer le réseau du Gouvenment du Canada avec une campagne d'attaques du 3-15 nov. Selon un courriel qui circule dans divers départements du gouvernement fédéral.

Comment est-ce que le Gouvernement se prépare?
Que faites vous?

Entrevue de 4-6 mins (pré-enregistré ou en direct)

Slack, Jessica

From: Duval, Jean Paul
Sent: October-30-12 12:04 PM
To: Slack, Jessica
Subject: FW: ML - Translation request
Attachments: 30 octobre_FREN_PS-SP-#714645-1-ML - Cyber Attack.doc

From: Abboud, Helene
Sent: Tuesday, October 30, 2012 12:03 PM
To: Translation (COMMS) / Traduction (COMMS)
Cc: Duval, Jean Paul
Subject: RE: ML - Translation request

From: Translation (COMMS) / Traduction (COMMS)
Sent: October-30-12 11:40 AM
To: Abboud, Helene; McDonald, Andrea; Langlais-Gagne, Vanessa
Subject: FW: ML - Translation request

From: Duval, Jean Paul
Sent: Tuesday, October 30, 2012 11:39:37 AM (UTC-05:00) Eastern Time (US & Canada)
To: * Translation (COMMS) / Traduction (COMMS)
Cc: Wilson, Barbara; Slack, Jessica; Champoux, Martin
Subject: ML - Translation request

Translation team,

Please find attached two media lines which require translation (65 words) before 1pm. Please advise if there are any issues with this request.

Many thanks,
JP

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

Cyber attacks

Media Lines/Infocapsules

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

- Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

- Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

Pierre Tr...del

Bue, Richard

From: Tomlinson, Jamie
Sent: October-30-12 12:13 PM
To: Slack, Jessica; Salewski, Shawn; Bue, Richard; Dubé, Rosanne
Cc: Swift, Andrew; Wilson, Barbara; Duval, Jean Paul
Subject: RE: FOR APPROVAL MEDIA CALL ON ANONYMOUS DDoS attacks

Approved.

thanks

From: Slack, Jessica
Sent: October-30-12 12:07 PM
To: Tomlinson, Jamie; Salewski, Shawn; Bue, Richard; Dubé, Rosanne
Cc: Swift, Andrew; Wilson, Barbara; Duval, Jean Paul
Subject: FOR APPROVAL MEDIA CALL ON ANONYMOUS DDoS attacks

Hi Jamie,

For approval please. We will decline interview and provide the following lines that NCSD approved last Friday in anticipation of calls.
I have advised NCSD and those at Secure Tech that we received the call...

With your ok, I will go to MO.
Jessica

PROPOSED RESPONSE
The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

TRANSLATION:
Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

Reporter's Name	[redacted]
Media Outlet	104.7 FM Gatineau
Call Date	10/30/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	10/30/2012 3:00 PM

Status	Consulting
Branch	
Subject	Cyber attacks
Questions	J'ai entendu que Anonymous tente d'infiltrer le réseau du Gouvenment du Canada avec une campagne d'attaques du 3-15 nov. Selon un courriel qui circule dans divers départements du gouvernement fédéral. Comment est-ce que le Gouvernement se prépare? Que faites vous? Entrevue de 4-6 mins (pré-enregistré ou en direct)

Slack, Jessica

From: Williams, Christopher <Christopher.Williams@pco-bcp.gc.ca>
Sent: October-30-12 12:36 PM
To: Slack, Jessica
Cc: Swift, Andrew; Duval, Jean Paul; Wilson, Barbara
Subject: Re: FOR APPROVAL: MEDIA CALL ON ANONYMOUS DDoS ATTACKS

None - thanks for flagging!

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: Tuesday, October 30, 2012 12:27 PM
To: Williams, Christopher
Cc: Swift, Andrew <Andrew.Swift@ps-sp.gc.ca>; Duval, Jean Paul <JeanPaul.Duval@ps-sp.gc.ca>; Wilson, Barbara <Barbara.Wilson@ps-sp.gc.ca>
Subject: FW: FOR APPROVAL: MEDIA CALL ON ANONYMOUS DDoS ATTACKS

Chris-see below. Any concerns?

From: Carmichael, Julie
Sent: October-30-12 12:27 PM
To: Slack, Jessica; Mueller, Mike; Johnson, Mark; McGrath, Andrew
Cc: Swift, Andrew; Duval, Jean Paul; Champoux, Martin; Carta, John; Tomlinson, Jamie; Wilson, Barbara
Subject: RE: FOR APPROVAL: MEDIA CALL ON ANONYMOUS DDoS ATTACKS

approved

From: Slack, Jessica
Sent: October-30-12 12:23 PM
To: Carmichael, Julie; Mueller, Mike; Johnson, Mark; McGrath, Andrew
Cc: Swift, Andrew; Duval, Jean Paul; Champoux, Martin; Carta, John; Tomlinson, Jamie; Wilson, Barbara
Subject: FOR APPROVAL: MEDIA CALL ON ANONYMOUS DDoS ATTACKS

Hi Julie-we have a call on the Anonymous DDoS attacks. We will decline interview and respond with the lines below (approved by you Friday)

Please advise if you approve.
Jessica

PROPOSED RESPONSE
The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

TRANSLATION:
Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

Reporter's Name	
Media Outlet	104.7 FM Gatineau
Call Date	10/30/2012 12:00 PM
Telephone	
E-mail address	
Deadline	10/30/2012 3:00 PM
Status	Consulting
Branch	
Subject	Cyber attacks
Questions	J'ai entendu que Anonymous tente d'infiltrer le réseau du Gouvenment du Canada avec une campagne d'attaques du 3-15 nov. Selon un courriel qui circule dans divers départements du gouvernement fédéral. Comment est-ce que le Gouvernement se prépare? Que faites vous? Entrevue de 4-6 mins (pré-enregistré ou en direct)

Duval, Jean Paul

From: Duval, Jean Paul
Sent: Tuesday, October 30, 2012 12:40 PM
To: ted.francis@ssc-spc.gc.ca
Cc: Wilson, Barbara; Slack, Jessica
Subject: FYI - Media Call: Anonymous DDoS Attacks

Ted,

FYI - The CSE flipped us a call they received on the Anonymous DDoS attacks. We will respond with the French lines below.

Regards,
JP

PROPOSED RESPONSE
The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

TRANSLATION:
Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

Reporter's Name	[redacted]
Media Outlet	104.7 FM Gatineau
Call Date	10/30/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	10/30/2012 3:00 PM
Status	Consulting
Branch	
Subject	Cyber attacks
Questions	J'ai entendu que Anonymous tente d'infiltrer le réseau du Gouvenment du Canada avec une campagne d'attaques du 3-15 nov. Selon un courriel qui circule dans divers départements du gouvernement fédéral. Comment est-ce que le Gouvernement se prépare? Que faites vous? Entrevue de 4-6 mins (pré-enregistré ou en direct)

Pages 600 to / à 602

are duplicates

sont des duplicatas

Slack, Jessica

From: Saul, Dawolu <Dawolu.Saul@cnsc-ccsn.gc.ca>
Sent: October-30-12 1:14 PM
To: Duval, Jean Paul
Cc: Slack, Jessica; Wilson, Barbara
Subject: RE: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Thank JP. [redacted] and nice chatting with you too. Thank you very much for sharing, and if possible can we be included on the list, if there are any future mail-outs please? We often get overlooked, when these things go down.

Thanks,
D.

Dawolu Saul
Senior Communications Project Officer | Agent principal de projets en communications
Strategic Communications Directorate | Direction des communications stratégiques
Regulatory Affairs Branch | Direction générale des affaires réglementaires
Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire
280, rue Slater Street
Ottawa, Canada K1A 0R5
dawolu.saul@cnsc-ccsn.gc.ca
Telephone | Téléphone : 613-947-3712
Blackberry : [redacted]
Facsimile | Télécopieur : 613-995-5086

From: Duval, Jean Paul [mailto:JeanPaul.Duval@ps-sp.gc.ca]
Sent: Tuesday, October 30, 2012 1:07 PM
To: Saul, Dawolu
Cc: Slack, Jessica; Wilson, Barbara
Subject: FW: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Dawolu,

Glad to have had the chance to chat with you today. As promised, here is the media relations protocol for questions on Anonymous DDoS attacks.

Please feel free to call or email with any questions you may have.

Kind regards,
JP

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

From: Slack, Jessica **On Behalf Of** PS Media Relations / Relations médias SP
Sent: Friday, October 26, 2012 4:33 PM

To: [redacted]@cse-cst.gc.ca; [redacted]@cse-cst.gc.ca; julie.gagnon@rcmp-grc.gc.ca; [redacted] Theresa.Knowles@tbs-sct.gc.ca; TBS Media / Média SCT; mylene.dupere@tpsgc-pwgsc.gc.ca; ted.francis@ssc-spc.gc.ca; sebastien.bois@tpsgc-pwgsc.gc.ca; Isabelle.Scott@cra-arc.gc.ca
Cc: Champoux, Martin; Wilson, Barbara; Swift, Andrew; Williams, Christpher; Duval, Jean Paul; Carta, John
Subject: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Colleagues,

Further to the note below (issued by CTEC) regarding Anonymous' plan for Distributed Denial of Service attacks on government websites, we wanted to touch base regarding the media relations protocol in advance of the weekend.

Direction at this time is that all departments should send any calls they receive to Public Safety for response (our contact info: media@ps-sp.gc.ca / 613-991-0657)

The approved media lines are below for your information.

Please do not hesitate to get in touch should you have any questions.

We will be in touch further next week.

Many thanks,

Jessica

Media Lines

EN

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.
- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

FR

- Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.
- Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

****

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, October 26, 2012 4:23 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

s.16(2)

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 2: 26 October 2012
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
==========

[redacted]

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both :

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contain information which may have been collected from external sources for which GC CTEC cannot verify the accuracy and integrity. GC CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

addressee. Access, copying, or re-use of the e-mail or any information contained therein by any other person is not authorized. If you are not the intended recipient, please notify us immediately by returning the e-mail to the originator.

Ce message est strictement réservé à l'usage du destinataire indiqué. Si vous n'êtes pas le destinataire de ce message, la consultation ou la reproduction même partielle de ce message et des renseignements qu'il contient est non autorisée. Si ce message vous a été transmis par erreur, veuillez en informer l'expéditeur en lui retournant ce message immédiatement.
****

Wilson, Barbara

From: Wilson, Barbara
Sent: Tuesday, October 30, 2012 1:16 PM
To: Slack, Jessica
Subject: FW: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Info – see below...

Barbara Wilson
Senior Communications Advisor
Issues management and media relations
Conseillère principale en communications
Gestion des enjeux et relations avec les médias
Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue W/ 269, avenue Laurier ouest
Ottawa, (ON) K1P 0P8
(613) 944-4920
barbara.wilson@ps-sp.gc.ca

From: [redacted]@CSE-CST.GC.CA]
Sent: Tuesday, October 30, 2012 1:15 PM
To: Swift, Andrew
Cc: Wilson, Barbara; Champoux, Martin; Plamondon, Jean J.
Subject: RE: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Classification: UNCLASSIFIED

Andrew,

I apologize for this delay, and you're absolutely right, this should never happen.

Since [redacted] departure and becoming a new department, we have been trying to cover many bases. But help is finally on the way. [redacted] recently joined our team as a media relations officer. He's unfortunately on training right now but will be back as of November 6. He will be joined by another new employee in late January. I am hopeful that with two media relations officers on board, such issues will not happen again. In the meantime, we'll have clearer guidelines in place for checking the media line.

I should also let you know that [redacted] I will be replaced by [redacted] as of November 5.

[redacted]
Communications Security Establishment Canada/
Centre de sécurité des télécommunications Canada
[redacted]

From: Swift, Andrew [mailto:Andrew.Swift@ps-sp.gc.ca]
Sent: October 30, 2012 11:24 AM
To: [redacted]
Cc: Wilson, Barbara; Champoux, Martin

Pages 609 to / à 611
are duplicates of
sont des duplicatas des
pages 613 to / à 615

s.15(1) - Subv
s.19(1)

s.15(1) - Def

Champoux, Martin

From: Champoux, Martin
Sent: Tuesday, October 30, 2012 1:18 PM
To: Slack, Jessica; Duval, Jean Paul
Subject: FW: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

FYI

From: [redacted] [mailto: [redacted] @CSE-CST.GC.CA]
Sent: Tuesday, October 30, 2012 1:15 PM
To: Swift, Andrew
Cc: Wilson, Barbara; Champoux, Martin; Plamondon, Jean J.
Subject: RE: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Classification: UNCLASSIFIED

Andrew,

I apologize for this delay, and you're absolutely right, this should never happen.

Since [redacted] departure and becoming a new department, we have been trying to cover many bases. But help is finally on the way. [redacted] recently joined our team as a media relations officer. He's unfortunately on training right now but will be back as of November 6. He will be joined by another new employee in late January. I am hopeful that with two media relations officers on board, such issues will not happen again. In the meantime, we'll have clearer guidelines in place for checking the media line.

I should also let you know that [redacted] I will be replaced by [redacted] as of November 5.

[redacted]
Communications Security Establishment Canada/
Centre de sécurité des télécommunications Canada
[redacted]

From: Swift, Andrew [mailto:Andrew.Swift@ps-sp.gc.ca]
Sent: October 30, 2012 11:24 AM
To: [redacted]
Cc: Wilson, Barbara; Champoux, Martin
Subject: FW: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS
Importance: High

[redacted]
While we appreciate getting these forwarded to our attention and follow up, the delay in getting the call to us and the lack of detail doesn't make our work any easier.
Appreciate if you can follow up.
Happy to discuss further if you would like.
Thanks,

s.15(1) - Subv
s.19(1)
s.15(1) - Def

Andrew

Andrew Swift
Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: PS Media Relations / Relations médias SP
Sent: Tuesday, October 30, 2012 10:16 AM
To: Filipps, Lisa; Slack, Jessica; Swift, Andrew; Swift, Andrew; Picard, Josée; Manning, Kerri; Wilson, Barbara; Champoux, Martin; Van Criekingen, Jane; Duval, Jean Paul
Subject: FW: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS
Importance: High

From:
Sent: Tuesday, October 30, 2012 10:15:41 AM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject: FW: CALL FROM RADIO STATION - MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Classification: UNCLASSIFIED

Hello,
We received a call yesterday on our media line (actually the same gentleman called three times). and so did not get the call.
His name (?)
Radio 147 (?) or 48

wants to discuss Anonymous and the recent attacks DDoS on GoC departments.
As per instructions below, I have not called back. Please call asap. third voice-mail from about at 1 p.m. yesterday
Thank you.

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada
Ottawa, Canada K1G 3Z4
@cse-cst.gc.ca
Telephone | Téléphone
Fax | Télécopieur 613-991-7691
Government of Canada | Gouvernement du Canada

From:
Sent: October 26, 2012 4:42 PM
To: Plamondon, Jean J.;
Cc: c2_media_relations-dl
Subject: FW: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Classification: UNCLASSIFIED

FYI - Public Safety Media Relations plan for DDoS is below.

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca] **On Behalf Of** PS Media Relations / Relations médias SP
Sent: October 26, 2012 4:33 PM
To: julie.gagnon@rcmp-grc.gc.ca; Theresa.Knowles@tbs-sct.gc.ca; TBS Media / Média SCT; mylene.dupere@tpsgc-pwgsc.gc.ca; ted.francis@ssc-spc.gc.ca; sebastien.bois@tpsgc-pwgsc.gc.ca; Isabelle.Scott@cra-arc.gc.ca

Cc: Champoux, Martin; Wilson, Barbara; Swift, Andrew; Williams, Christpher; Duval, Jean Paul; Carta, John
Subject: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Colleagues,
Further to the note below (issued by CTEC) regarding Anonymous' plan for Distributed Denial of Service attacks on government websites, we wanted to touch base regarding the media relations protocol in advance of the weekend.

Direction at this time is that all departments should send any calls they receive to Public Safety for response (our contact info: media@ps-sp.gc.ca / 613-991-0657)
The approved media lines are below for your information.
Please do not hesitate to get in touch should you have any questions.
We will be in touch further next week.
Many thanks,

Jessica

Media Lines

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.
- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, October 26, 2012 4:23 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2
Importance: High
Classification: UNCLASSIFIED
La version française suivra.

==========

GC CTEC - Information Note IN12-002
Date: 25 October 2012

==========

==========

Update 2: 26 October 2012

==========

==========

Anonymous DDOS activity against GC

==========

AUDIENCE

========

This Information Note is intended for IT professionals and managers within the federal government.
ASSESSMENT

==========

[redacted]

[redacted]

SUGGESTED ACTION

==========

[redacted]

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both :
- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

NOTICE:

This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contain information which may have been collected from external sources for which GC CTEC cannot verify the accuracy and integrity. GC CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers

==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Slack, Jessica

From: Slack, Jessica
Sent: October-30-12 2:35 PM
To: Swift, Andrew
Cc: Salewski, Shawn; Wilson, Barbara
Subject: RE: DDOS Threat - communications engaged?

Sensitivity: Confidential

Mais oui.

From: Swift, Andrew
Sent: October-30-12 2:34 PM
To: Slack, Jessica
Cc: Salewski, Shawn; Wilson, Barbara
Subject: FW: DDOS Threat - communications engaged?
Sensitivity: Confidential

Jessica,
See below. CBSA has questions on DDoS & Anonymous. Can you get in touch and share the lines and comms protocol?
Thx.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Salewski, Shawn
Sent: Tuesday, October 30, 2012 1:31 PM
To: 'Sutton, Sean'
Cc: Le Breton, Gilles; Swift, Andrew
Subject: RE: DDOS Threat - communications engaged?
Sensitivity: Confidential

Contact Andrew Swift – he is our Director of Public Affairs.

Shawn

From: Sutton, Sean [mailto:Sean.Sutton@cbsa-asfc.gc.ca]
Sent: Tuesday, October 30, 2012 1:20 PM
To: Salewski, Shawn
Cc: Le Breton, Gilles
Subject: FW: DDOS Threat - communications engaged?
Sensitivity: Confidential

Hi Shawn, do you have a contact that could help me with this? We're looking to see if PS or SSC or CRA might have already created lines on the Anonymous Denial of Service threat.

Thanks,

Sean

From: Le Breton, Gilles
Sent: October 30, 2012 12:47 PM
To: Sutton, Sean
Subject: RE: DDOS Threat - communications engaged?
Sensitivity: Confidential

Yeah, to you and Scott. Is he in? [redacted] Let's hat when I get back.

Gilles

From: Sutton, Sean
Sent: October 30, 2012 12:31 PM
To: Le Breton, Gilles
Subject: RE: DDOS Threat - communications engaged?
Sensitivity: Confidential

Did you send this to me?

From: Le Breton, Gilles
Sent: October 30, 2012 12:31 PM
To: Sutton, Sean
Cc: MacIntosh, ScottM
Subject: FW: DDOS Threat - communications engaged?
Sensitivity: Confidential

Have you had a chance to look into this?

If not, please come see me.

Gilles

From: Stokes, Mark
Sent: October 30, 2012 10:49 AM
To: Le Breton, Gilles
Cc: Hawkins, Keren; CBSA-ASFC_Comms_Coordination; MacKillop, Ken
Subject: FW: DDOS Threat - communications engaged?
Sensitivity: Confidential

Gilles – another one for you. This is in respect of the Anonymous denial of service attack (Nov 3-13). We are part of a bigger target, so I'm wondering whether SSC, or CRA, or PS for that matter, is working on comms products. There is a BN which I can share as info. Would you mind looking into this?
Thanks
Mark

From: Stokes, Mark
Sent: October 30, 2012 10:44 AM
To: Banks, Carol

Subject: RE: DDOS Threat - communications engaged?
Sensitivity: Confidential

That's fine Carol – I was just wondering whether in the course of the contacts with SSC, calls or otherwise, the issue of communications had come up.

Given the nature and scope of the threat/disruption, there is often a Whole-of-Government approach to these things.

We will follow up on the comms channels through SSC et al..

From: Banks, Carol
Sent: October 30, 2012 10:39 AM
To: Stokes, Mark
Subject: DDOS Threat - communications engaged?
Sensitivity: Confidential

Mark,

As per your question on the conference call this morning, I am being told that both you and Ken have been engaged in terms of receiving a heads-up in case media lines needed to be prepared for questions to CBSA.

What other involvement do you guys require? Let me know and I can assist in making that happen...

Merci et bonne journée!

Carol A. Banks

Director - IT Quality Management | Directrice de la gestion de la qualité de la TI
Infrastructure Services Directorate | Direction des services d'infrastructure
Information, Science and Technology Branch | Direction générale de l'information, des sciences et de la technologie
Canada Border Services Agency | Agence des services frontaliers du Canada
2323 Riverside Drive Ottawa ON K1A 0L8 | 2323 chemin Riverside Ottawa ON K1A 0L8
carol.banks@cbsa-asfc.gc.ca
Telephone | Téléphone 613-941-5909 / Facsimile | Télécopieur 613-941-5551 / Cellular | Cellulaire [redacted]
Government of Canada | Gouvernement du Canada

Slack, Jessica

From: Slack, Jessica
Sent: October-30-12 3:50 PM
To: 'McDonald, Jessica'
Subject: RE: Comms approach and MLs: DDoS activity against GC

Jessica, at this point, yes – everything should come here and be flagged here...That may change depending on how the issues progresses...
We will also ensure CBSA is included if/when the media relations protocol changes.
Give me a call if you have any questions...
613-949-4288

From: McDonald, Jessica [mailto:Jessica.McDonald@cbsa-asfc.gc.ca]
Sent: October-30-12 3:35 PM
To: Slack, Jessica
Subject: RE: Comms approach and MLs: DDoS activity against GC

Hey ☺ hope things are going well with you. I saw the note to Pat and Esme, thanks, so PS is taking all calls, even those specifically on "loss of service and attacks"? Mark specifically asked about that scenario.

Thanks!

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: October 30, 2012 3:33 PM
To: McDonald, Jessica
Subject: RE: Comms approach and MLs: DDoS activity against GC

Hey, lady! You can let Mark know that I sent a note to Patrizia and Esme...yes, PS is taking calls at this point..will forward you what I sent them.

From: McDonald, Jessica [mailto:Jessica.McDonald@cbsa-asfc.gc.ca]
Sent: October-30-12 3:30 PM
To: Slack, Jessica
Subject: FW: Comms approach and MLs: DDoS activity against GC

Hello!

Our professional paths meet again ☺ Quick question – will PS take calls in the wake of any attacks/loss of service, or would it be CSE?

Thanks!
Jessica

From: Stokes, Mark
Sent: October 30, 2012 3:27 PM
To: McDonald, Jessica
Subject: Re: Comms approach and MLs: DDoS activity against GC

Jessica -- will PS take calls in the wake of any attack/loss of service?
Thanks

Mark

Sent from my BlackBerry handheld.
Envoyé à partir de mon BlackBerry.

From: McDonald, Jessica
Sent: Tuesday, October 30, 2012 03:14 PM
To: Stokes, Mark
Cc: Giolti, Patrizia; Le Breton, Gilles; Sutton, Sean; MacIntosh, ScottM
Subject: Comms approach and MLs: DDoS activity against GC

Hi Mark,

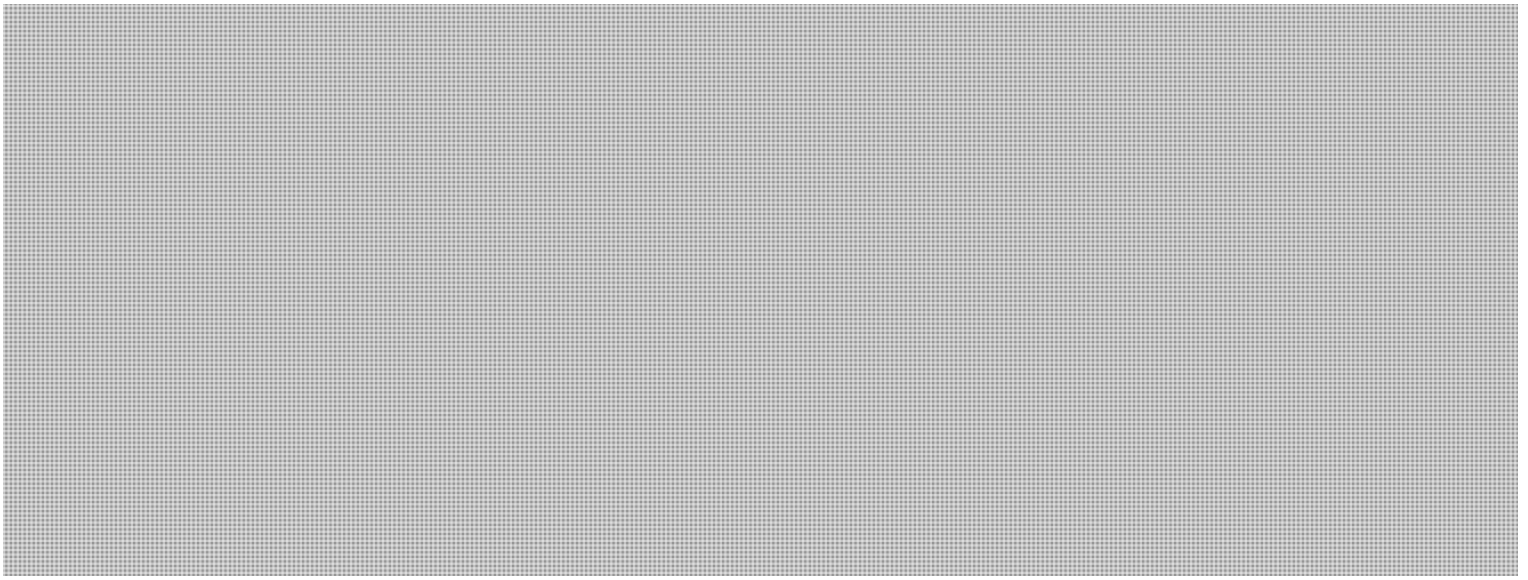
Following up to your request, please find below Comms approach, media lines and background information on the cyber threat – DDoS activity against GC / Anonymous.

For media enquiries, Public Safety Canada is the lead at this point, so any calls about these DDoS attacks should be forwarded to media@ps-sp.gc.ca or 613-991-0657.

For your information, below are the media lines being shared:

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.
- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

Background information:



Suggested action:

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:

- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

Thank you,

Jessica McDonald
Communications Officer | Agente des communications
Corporate Affairs | Direction générale des services intégrés
Communications Directorate | Direction des communications
Canada Border Services Agency | Agence des services frontaliers du Canada
Protection – Service – Integrity
Jessica.mcdonald@cbsa-asfc.gc.ca
Telephone | Téléphone 613-952-2812

Duval, Jean Paul

From: Duval, Jean Paul
Sent: Tuesday, October 30, 2012 5:00 PM
To: * Media Monitoring / Suivi des médias; Austria, Jamela; Baulne, Lucie; Bernas, Angie; Boucher, Patrick; Bourdeau, Anne; Burton, Meredith; Carmichael, Julie; CBSA Media Relations; Champoux, Martin; CSC Media Relations; Csversko, Christine; Cyr, Lynne; Daoust, Normand; Derek Cefaloni; Douglas, Caroline; Durand, Stéphanie; Duval, Jean Paul; Eke, Darren; Filipps, Lisa; Issues / Enjeux; jane mcdonald; Johnson, Mark; jspassov; julie gagnon; Lambert, Louise; Leclair, Natalie; Leclerc, Carole; Marc Richer; marie cocking; Mark Prieur; McAteer, Julie; McDonald, Andrea; McGrath, Andrew; McRae, Marley; Mueller, Mike; [redacted] Nadine Archambault; Panthaky, Jasmine; Paulson, Erika; Picard, Josée; Salewski, Shawn; Sergeant Greg Cox; Slack, Jessica; Swift, Andrew; Taillefer, Lucie; Thibouthot, AkimIsabelle; Tomlinson, Jamie; Van Criekingen, Jane; Veilleux, Martine; Verret, Scott; Willey, Chris; Williams, Christpher; Wilson, Barbara
Subject: Daily Media Report / Rapport média quotidien
Attachments: image001.jpg

For your information, we received 3 new media calls on Tuesday, October 30 // Pour votre information, nous avons reçu 3 appels des médias ce mardi le 30 octobre.

New

Reporter's Name	[redacted]
Media Outlet	Newsletter - TD Bank
Call Date	10/30/2012 3:00 PM
Telephone	[redacted]
E-mail address	
Deadline	11/2/2012 11:00 AM
Status	Consulting
Branch	EM
Subject	Winter Power Outage
Questions	As per our conversation earlier today, I write The Smart Life — an e-newsletter that goes out to more than 1 million subscribers (in English and French) who are all TD Insurance clients. Every issue contains four consumer interest pieces that give tips for the average Canadian. For the December 2012 issue, we're including a story tentatively titled "Winter power outages — what to do, what not to do" and I'm hoping someone from Public Safety will be available for an interview. Of course, I will provide a link to GetPrepared.ca -- specifically http://www.getprepared.gc.ca/cnt/hzd/pwrtgs-eng.aspx — which contains relevant information for readers who want to know more. Here's more information about the story, interview process and publication: General article key points to cover (suggestions only): - Simple tips for being prepared for a power outage - What to do when the power goes off - What to do when you must leave your home for more than 24 hours - What to do when you get home and turn the power back on Interview Since the article is only 600-700 words, a 15- or 20-minute phone call is all I need. Due to deadlines, I would like to interview someone this week.

As discussed, while I would prefer to interview someone, it is possible to use another process.

I can also conduct the interview over email OR can go ahead and write the story based on information found at Get Prepared's "Power outages" sections, attribute them to Public Safety Canada and then have you or another member of the media team approve of the information given.

Approval process
Once I write the story and it goes through my editor, I will email it back to you and your spokesperson (if one is used) for changes or approval. (Normally, I can give about a 24-hour review period.) If you do have changes, they will be made but may be altered to fit our style/tone.

Back issues of The Smart Life
You can access back issues by clicking on one of the following links:

May 2012:
http://enewsletter.thesmartlife.ca/T/OFSYS/SM2/2/S/F/3742/2028474/Hgi1jods.html

February 2012:
http://enewsletter.thesmartlife.ca/T/OFSYS/SM2/2/S/F/3742/1020522/wWJuaNeD.html

November 2011:
http://thesmartlife.clientcontact.ca/1201/email.php?version=tdmm&lang=en&s=1&associationid=laurentiar

Many thanks and I look forward to your reply!

Reporter's Name	[redacted]
Media Outlet	104.7 FM Gatineau
Call Date	10/30/2012 12:00 PM
Telephone	[redacted]
E-mail address	
Deadline	10/30/2012 3:00 PM
Status	Final
Subject	Cyber attacks
Questions	J'ai entendu que Anonymous tente d'infiltrer le réseau du Gouvenment du Canada avec une campagne d'attaques du 3-15 nov. Selon un courriel qui circule dans divers départements du gouvernement fédéral. Comment est-ce que le Gouvernement se prépare? Que faites vous? Entrevue de 4-6 mins (pré-enregistré ou en direct)
Final Response	Je regrette de vous annoncer que nous ne pourrons pas accommoder votre requête pour une entrevue aujourd'hui. J'aimerais toutefois souligner que le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes. Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.
Reporter's Name	[redacted]
Media Outlet	Freelance (National Post)
Call Date	10/30/2012 6:00 PM

Telephone	[redacted]
E-mail address	[redacted]@gmail.com
Status	Final
Subject	Cyber Bullying
Questions	- Does Public Safety Canada consider the case of Amanda Todd was cyber bullying. What is the government doing to police the internet with regards to bullying. - When does cyber bullying become a crime? - Is Public Safety Canada aware of the web site "Is anyone up?" and/or similar sites (Daily Capper, Blogg tv, 4 Chan) which publish "revenge porn" or nude photographs against the will or unbeknownst to the individuals, while providing direct links to their facebook profiles.
Reporter and Outlet	[redacted] - Freelance (National Post)
Approvals	MO
Final Response	Further to your request, I am able to provide you with the following information regarding federal action to combat bullying. The Government of Canada takes the issue of bullying very seriously and a number of departments and agencies provide anti-bullying programs and information, including Public Health Agency of Canada, the RCMP and Public Safety Canada. Within the department of Public Safety, the National Crime Prevention Centre (NCPC) has produced a series of documents related to bullying. Most of these documents are available on the Department's website at: www.publicsafety.gc.ca. These documents provide information on bullying in Canada, promising practices in preventing bullying, and examples of bullying projects previously funded by the NCPC. Here are more specific links: llying prevention in schools: Executive summary - http://www.publicsafety.gc.ca/res/cp/res/bully_exec-eng.aspx search publication – bullying prevention in schools - http://www.publicsafety.gc.ca/res/cp/res/bully-eng.aspx llying Prevention: Nature and Extent of Bullying in Canada - http://www.publicsafety.gc.ca/res/cp/res/2008-bp-01-eng.aspx pporting the Successful Implementation of the National Crime Prevention Strategy - http://www.publicsafety.gc.ca/res/cp/res/ssincps-amosnpc-eng.aspx Through Health Canada, the Government invests significantly in initiatives that promote awareness and crack down on bullying through online initiatives, programs and resources that assist youth, parents, and educators combat bullying in their communities. We created the Walk Away, Ignore, Talk it Out, and Seek help initiative (WITS) which teaches children to make positive choices when faced with bullying, cyber-bulling, peer victimization and conflict. The RCMP operates a website, DEAL.org, which offers resources to youth, parents, and educators on bullying and cyber-bullying. The Government has invested to expand Cybertip.ca's capacity to address self and peer exploitation. If you have not already done so, you may wish to contact the RCMP (www.rcmp-grc.gc.ca) for additional information. The Public Health Agency of Canada also has information on

bullying at: http://www.phac-aspc.gc.ca/hp-ps/dca-dea/stages-etapes/ado/bullied-intimide-eng.php.

s.19(1)

Closed

Reporter's Name	[redacted]
Media Outlet	CBC News (Winnipeg)
Call Date	10/29/2012 12:00 PM
Telephone	[redacted]
E-mail address	[redacted]@cbc.ca
Status	Final
Branch	CSP
Subject	Band Constable Program
Questions	Is there any way to confirm that this year the certification lapsed for band constables in Lac Brochet? They tell me they lost keys to the RCMP detention facility because it was discovered there last band constable no longer was certified. Was his name Martin Veuillot? Can you confirm how many of the first nation communities in Manitoba's North do not have band constables? That's the focus of my report. • How often does a band constable need to be recertified? • How much does the original certification cost? How long does it take? • How much does the recertification cost? How long does that take? • Who/what government agency trains/certifies band constables?
Reporter and Outlet	[redacted] CBC News (Winnipeg)
Actions Taken	No existing entries.
Final Response	In response to your questions, we would like to underscore the objective of the Band Constable Program (BCP) which is to enforce laws within band jurisdiction which do not fall within the purview of the provincial police service, and to supplement police forces at the local level. As such, Band Constables are to enforce band by-laws of a civil nature and areas of local concern outside the purview of the RCMP or provincial police. Band Constables must refer to the RCMP or provincial police cases involving Criminal Code offences or other offences under federal or provincial legislation. Questions as to the identity of the designated Band Constable can be addressed to the respective Chief and/or Band Council as they designate and manage their own Band Constables. In some cases the Province may choose to appoint certain Band Constables as 'special constables' to give them more authority, such as arrest and detention. Questions on these Provincially appointed "special constables" should be directed to the Province or to the Chief or Council of the respective Band. As mentioned in our previous response, of the 63 First Nation communities across Manitoba, 29 do not have Band Constable agreements with Public Safety Canada. If you are looking for the number of "special constables", please refer your questions to the Province of Manitoba.

s.19(1)

Reporter's Name	[redacted]
Media Outlet	Carleton University
Call Date	10/29/2012 4:00 PM
Telephone	[redacted]
E-mail address	[redacted]@cmail.carleton.ca
Deadline	10/31/2012 12:00 PM
Status	Final
Subject	Police Officers Recruitment Fund (PORF)
Questions	I'm [redacted] at Carleton University working on a story about the end of the Police Officers Recruitment Fund, and I was wondering if I could get a bi information. In particular, I am writing about how some First Nations communities, which previously had their own police force now returning to OPP to provide police. I was wondering i could provide some information about a couple things. 1. Of the initial $156 million put into the program in Onta much of this went to First Nations communities? 2. How much did each community receive? If it was broke unevenly, which communities received the most? 3. Related to number 2, how was the funding broken dow how was the need of each community decided. 4. Has Public Safety received any updates or information the loss of local police forces as a result of the cuts in the program? Thanks for the information. Please feel free to email me, me a call at [redacted]
Final Response	Thank you for your questions. I can confirm that in 2 Police Officers Recruitment Fund allocated $400 mil over five years to the provinces and territories to re 2,500 police officers across the country. (Please see http://www.publicsafety.gc.ca/media/nr/2008/nr20 2-eng.aspx). Under the fund, Ontario received a one-time payme $156 million. The funding period runs from 2008-09 2012-13 and the withdrawal and distribution of fun responsibility of each province and territory. For mo information please visit http://www.fin.gc.ca/fedpr eng.asp. Provinces and territories are in the best po decide how to direct the federal funding in ways tha their respective policing priorities and public safety keeping with the terms of the Fund.

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

Octobre est le Mois de la sensibilisation à la cybersécurité

October is Cyber Security Awareness Month

Pour des renseignements sur la façon de vous protéger en ligne, veuillez consulter

PENSEZCYBERSECURITE.CA

For information on how to stay safe online, please visit

GETCYBERSAFE.CA

Slack, Jessica

From: Swift, Andrew
Sent: October-30-12 5:31 PM
To: Duval, Jean Paul; Slack, Jessica
Cc: Wilson, Barbara; Champoux, Martin
Subject: FW: FYI - EXCLUSIF: Anonymous veut attaquer le gouvernement fédéral

FYI

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: COMDO
Sent: Tuesday, October 30, 2012 5:26 PM
To: GOC-COG
Cc: * Media Monitoring / Suivi des médias
Subject: FYI - EXCLUSIF: Anonymous veut attaquer le gouvernement fédéral

EXCLUSIF: Anonymous veut attaquer le gouvernement fédéral
Le 29 octobre, 2012
98,5 FM

Le groupe de pirates informatiques et d'activistes Anonymous a le gouvernement fédéral dans sa mire.

Selon nos informations, pas moins de 44 ministères ont vu leurs défenses numériques testées par des cyberpirates.

Depuis 9h30 lundi matin, nous attendons des retours d'appels effectués auprès du Centre de la sécurité des télécommunications du Canada.

On s'attend à ce que les pirates informatiques d'Anonymous mènent une attaque d'envergure contre le gouvernement du Canada entre le 3 et le 15 novembre prochain.

Lien

Champoux, Martin

From: Champoux, Martin
Sent: Tuesday, October 30, 2012 10:17 PM
To: Wilson, Barbara
Subject: Fw: Update 6: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

----- Original Message -----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, October 30, 2012 05:29 PM
To: CTEC <CTEC@CSE-CST.GC.CA>
Subject: Update 6: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 30 October 2012
==========

==========
Update 6: 30 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

[redacted]

SUGGESTED ACTION
==========

[redacted]

Departments should implement the mitigation advice in GCCF12-008: DDoS campaign against the GC.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca.

Champoux, Martin

From: Champoux, Martin
Sent: Tuesday, October 30, 2012 10:22 PM
To: Anderson, Windy; Beaudoin, Luc; Bendelier, Kenneth; Dick, Robert; Matz, Mark; Hatfield, Adam; Labelle, Sébastien
Cc: Carta, John
Subject: Fw: FYI - EXCLUSIF: Anonymous veut attaquer le gouvernement fédéral

FYI

From: COMDO
Sent: Tuesday, October 30, 2012 05:26 PM
To: GOC-COG
Cc: * Media Monitoring / Suivi des médias
Subject: FYI - EXCLUSIF: Anonymous veut attaquer le gouvernement fédéral

EXCLUSIF: Anonymous veut attaquer le gouvernement fédéral
Le 29 octobre, 2012
98,5 FM

Le groupe de pirates informatiques et d'activistes Anonymous a le gouvernement fédéral dans sa mire.

Selon nos informations, pas moins de 44 ministères ont vu leurs défenses numériques testées par des cyberpirates.

Depuis 9h30 lundi matin, nous attendons des retours d'appels effectués auprès du Centre de la sécurité des télécommunications du Canada.

On s'attend à ce que les pirates informatiques d'Anonymous mènent une attaque d'envergure contre le gouvernement du Canada entre le 3 et le 15 novembre prochain.

Lien

Austria, Jamela

From: Slack, Jessica
Sent: Wednesday, October 31, 2012 9:13 AM
To: Austria, Jamela; Filipps, Lisa; Duval, Jean Paul; Champoux, Martin
Cc: Willey, Chris; Carta, John
Subject: RE: Question: Denial of service MLs

These are the lines, but if departments receive calls the direction is that they be sent here for response...until further notice anyway.
Jessica

Lines:
The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

TRANSLATION:
Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

-----Original Message-----
From: Austria, Jamela
Sent: October-31-12 8:38 AM
To: Filipps, Lisa; Slack, Jessica; Duval, Jean Paul; Champoux, Martin
Cc: Willey, Chris; Carta, John
Subject: Question: Denial of service MLs

Hello!

Please see request below from TBS Comms - would we have lines to this effect?

I'm not sure if the version I was cc'ed on is the right one.

Thanks!
j

----- Original Message -----
From: Le Gras, Gilbert [mailto:Gilbert.LeGras@tbs-sct.gc.ca]
Sent: Wednesday, October 31, 2012 08:34 AM
To: Austria, Jamela
Cc: Dussault, Nathalie <Nathalie.Dussault@tbs-sct.gc.ca>
Subject: Denial of service

Hi Jamela,
Could you share your denial of service media lines with us, please?
Thank you.
Gilbert

Durand, Stéphanie

From: Boucher, Pierre <Pierre.Boucher@tbs-sct.gc.ca>
Sent: Wednesday, October 31, 2012 9:59 AM
To: Durand, Stéphanie; Dick, Robert; Gordon, Robert; Swift, Andrew
Subject: Re: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Thanks. Pierre
Pierre Boucher
Deputy Chief Information Officer of the government of Canada | Co-dirigeant principal de l'information du gouvernement du Canada
Chief Information Officer Branch | Direction du dirigeant principal de l'information
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Pierre.Boucher@tbs-sct.gc.ca
Telephone | Téléphone 613-957-8990 / Facsimile | Télécopieur 613-952-8536 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

From: Durand, Stéphanie [mailto:Stephanie.Durand@ps-sp.gc.ca]
Sent: Wednesday, October 31, 2012 09:46 AM
To: Boucher, Pierre; Dick, Robert <Robert.Dick@ps-sp.gc.ca>; Gordon, Robert: PS-SP; Swift, Andrew: PS-SP
Subject: Re: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

We will be following up on the public comms side and connect with TBS, CSEC and SSC Comms. We'll also connect with MO and PCO on this. We'll share and consult with you as messaging is developed.

Andrew: pls handle.

Thanks.

From: Boucher, Pierre [mailto:Pierre.Boucher@tbs-sct.gc.ca]
Sent: Wednesday, October 31, 2012 09:43 AM
To: Dick, Robert; Gordon, Robert
Cc: Durand, Stéphanie
Subject: Re: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Hi,

I had a discussion on this very topic yesterday with SSC. I don't think the internal communication (to program ADMs and DMs) is well covered. My sense is this is related to the fact that before SSC, CIOs were in the middle of the action and they could brief up within their departments. This is not happening right now as they are outside the loop.

For now, CIOB will issue updates to DMs until the situation calms down. We will do a postmortem after and make necessary changes to the IMP to address that.

I want to make sure however that you are on top of the public comms side. Is it safe to assume you are handling that?

Pages 636 to / à 638

are duplicates of

sont des duplicatas des

pages 640 to / à 642

Durand, Stéphanie

From: Swift, Andrew
Sent: Wednesday, October 31, 2012 10:02 AM
To: Durand, Stéphanie; 'Pierre.Boucher@tbs-sct.gc.ca'; Dick, Robert; Gordon, Robert
Subject: RE: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

The following lines were approved by PS MO and PCO late last week on this issue. The current media relations protocol (shared with TBS, SSC, CSEC, CSIS, RCMP and PWGSC comms) is for all calls on the matter to go to PS.

The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Durand, Stéphanie
Sent: Wednesday, October 31, 2012 9:46 AM
To: 'Pierre.Boucher@tbs-sct.gc.ca'; Dick, Robert; Gordon, Robert; Swift, Andrew
Subject: Re: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

We will be following up on the public comms side and connect with TBS, CSEC and SSC Comms. We'll also connect with MO and PCO on this. We'll share and consult with you as messaging is developed.

Andrew: pls handle.

Thanks.

From: Boucher, Pierre [mailto:Pierre.Boucher@tbs-sct.gc.ca]
Sent: Wednesday, October 31, 2012 09:43 AM
To: Dick, Robert; Gordon, Robert
Cc: Durand, Stéphanie

Subject: Re: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Hi,

I had a discussion on this very topic yesterday with SSC. I don't think the internal communication (to program ADMs and DMs) is well covered. My sense is this is related to the fact that before SSC, CIOs were in the middle of the action and they could brief up within their departments. This is not happening right now as they are outside the loop.

For now, CIOB will issue updates to DMs until the situation calms down. We will do a postmortem after and make necessary changes to the IMP to address that.

I want to make sure however that you are on top of the public comms side. Is it safe to assume you are handling that?

Thanks. Pierre.
Pierre Boucher
Deputy Chief Information Officer of the government of Canada | Co-dirigeant principal de l'information du gouvernement du Canada
Chief Information Officer Branch | Direction du dirigeant principal de l'information
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Pierre.Boucher@tbs-sct.gc.ca
Telephone | Téléphone 613-957-8990 / Facsimile | Télécopieur 613-952-8536 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

From: Dick, Robert [mailto:Robert.Dick@ps-sp.gc.ca]
Sent: Wednesday, October 31, 2012 09:36 AM
To: Boucher, Pierre; Gordon, Robert: PS-SP
Cc: Durand, Stephanie: PS-SP
Subject: Re: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Thanks, Pierre.

We're receiving a formal update every night from CSEC on this specific issue and CCIRC and CSEC are in constant touch on it given impacts on sites outside Government as well.

I do think, however, that we can use this issue as a case study to discuss as a community whether we have our mechanisms right for briefing up to higher levels of comms and policy leadership, and for determining when we manage an issue up through the apparatus as just a Government vs a national issue.

Robert

From: Boucher, Pierre [mailto:Pierre.Boucher@tbs-sct.gc.ca]
Sent: Wednesday, October 31, 2012 09:10 AM
To: Dick, Robert; Gordon, Robert
Subject: Fw: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Hi, just want to make sure you are on this. See reference below to the Anonymous attack. Have you got all the communications info you need to respond to media inquiries? Thanks. Pierre.
Pierre Boucher
Deputy Chief Information Officer of the government of Canada | Co-dirigeant principal de l'information du

gouvernement du Canada
Chief Information Officer Branch | Direction du dirigeant principal de l'information
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Pierre.Boucher@tbs-sct.gc.ca
Telephone | Téléphone 613-957-8990 / Facsimile | Télécopieur 613-952-8536 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

From: PSMediaCentre/CentredesmediasdeSP [mailto:PSMediaCentre/CentredesmediasdeSP@ps-sp.gc.ca]
Sent: Wednesday, October 31, 2012 08:31 AM
To: Cyber Security / Sécurité cybernétique <CyberSecurity@ps-sp.gc.ca>
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
October 31, 2012 / le 31 octobre 2012

Print Media / Médias imprimés

Canadians don't think in 'diabolical way'
Cyber attacks are skyrocketing primarily because average Canadians do not take computer security seriously enough, experts told an Ottawa security conference Tuesday. Ottawa Citizen, A4

Everyone's a soldier in cyber-war: Wallin
Canadians and the federal government don't want more regulations over how we use our mobile and Internet-connected devices all in the name of cyber-security, a high-profile Tory senator says. Montreal Gazette, A9

Online Media / Médias en ligne

FBI cybersecurity shift draws skepticism from experts
The FBI has changed its cybersecurity strategy to place greater emphasis on identifying the criminals behind attacks, a shift that some experts say won't make a dent in hacking operations. CSO

DHS eyes kindergarten for next generation of cybersecurity pros
The Department of Homeland Security (DHS), struggling to find enough cybersecurity talent to meet its needs, says it is going to groom the next generation of cybersecurity pros starting in kindergarten. CSO

EXCLUSIF: Anonymous veut attaquer le gouvernement fédéral
Le groupe de pirates informatiques et d'activistes Anonymous a le gouvernement fédéral dans sa mire. Selon nos informations, pas moins de 44 ministères ont vu leurs défenses numériques testées par des cyberpirates. On s'attend à ce que les pirates informatiques d'Anonymous mènent une attaque d'envergure contre le gouvernement du Canada entre le 3 et le 15 novembre prochain. 98,5 FM

Privacy issues online evolving too fast for regulation, Google tells MPs
Search engine giant Google says it feels no need for governments to regulate online privacy policies. A policy manager for the company's Canadian operations told a House of Commons committee that it would be difficult to determine default positions for the policies. And Colin McKay says that's because the online world is evolving too quickly to set regulations in stone that would endure. Canadian Press

Stratsec research reveals potential alarm for cloud security
A new piece of research from security providers Stratsec has inferred that some cloud providers are unable to block malicious attacks, which could lead to cyber hackers being able to infiltrate systems in a botnet-styled attack. Cloud Tech News

ZeroAccess infects 2,2 million homes

About 2.2 million home networks worldwide were infected with the ZeroAccess botnet in the third quarter of 2012, according to the Kindsight Security Labs quarterly Malware Report. In the United States alone, approximately 685,000 users are infected, at a rate of one in 125 home networks. Infosecurity

Cybersecurity legislation mired as executive order looms
The 112th Congress is in a virtual state of paralysis after having balked at several opportunities to pass comprehensive cybersecurity legislation. Senate Majority Leader Harry Reid expressed hope recently that progress could be made during the post-election lame duck session, but experts familiar with the legislative process believe the chances of that happening are slim at best. Tech Target

India to invest $ 200 mn to build Cybersecurity infra
Cybersecurity is more more a murmur in bureaucratic corridors. With the recent rumor-mongering in the Cyberspace during Assam violence and plethora of blasphemous content, the Indian government is readying a robust Cybersecurity policy. The government is investing US$ 200 million to build Cybersecurity infrastructure over a period of four years, Sathyanarayana informed. CIOL News Reports

Malicious spam hits Indian users of Skype
A "malicious spam" has hit the internet-based audio-video communicator 'Skype' in the Indian cyberspace and anti-hacking sleuths have asked users to remain alert and cautious. The Hindu

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Austria, Jamela

From: Austria, Jamela
Sent: Wednesday, October 31, 2012 10:16 AM
To: Gilbert LeGras; 'Nathalie.Dussault@tbs-sct.gc.ca'
Cc: Carta, John; Slack, Jessica; Willey, Chris; Champoux, Martin; Filipps, Lisa
Subject: Re: Denial of service

Good morning,

As requested, please find pasted below the media lines. I understand that the current media relations protocol is to refer all calls to Public Safety.

I have cc'ed my media relations colleagues above in case you have any questions. Please feel free to contact any of us.

Merci,
Jamela

Lines:
The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

TRANSLATION:
Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

----- Original Message -----
From: Le Gras, Gilbert [mailto:Gilbert.LeGras@tbs-sct.gc.ca]
Sent: Wednesday, October 31, 2012 08:34 AM
To: Austria, Jamela
Cc: Dussault, Nathalie <Nathalie.Dussault@tbs-sct.gc.ca>
Subject: Denial of service

Hi Jamela,
Could you share your denial of service media lines with us, please?
Thank you.
Gilbert

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Wednesday, October 31, 2012 10:40 AM
To: Swift, Andrew
Subject: RE: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Thx – tough to keep track during meeting.
Robert Dick is here...

From: Swift, Andrew
Sent: Wednesday, October 31, 2012 8:38 AM
To: Durand, Stéphanie
Subject: RE: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

I did, responded at 10:02.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Durand, Stéphanie
Sent: Wednesday, October 31, 2012 10:38 AM
To: Swift, Andrew
Subject: RE: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Need to ensure that loop is closed with those on e-mail with Robert Dick.
Thx

From: Swift, Andrew
Sent: Wednesday, October 31, 2012 8:31 AM
To: Durand, Stéphanie
Subject: FW: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

FYI, We've shared the small story on the DDoS attacks with partners below and re-confirmed the media relations protocol.
Andrew

From: Slack, Jessica On Behalf Of PS Media Relations / Relations médias SP
Sent: Wednesday, October 31, 2012 10:15:03 AM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP; [redacted]@cse-cst.gc.ca'; [redacted]@cse-cst.gc.ca'; 'julie.gagnon@rcmp-grc.gc.ca'; [redacted]; 'Theresa.Knowles@tbs-sct.gc.ca'; 'TBS Media / Média SCT'; 'mylene.dupere@tpsgc-pwgsc.gc.ca'; 'ted.francis@ssc-spc.gc.ca'; 'sebastien.bois@tpsgc-pwgsc.gc.ca'; Isabelle.Scott@cra-arc.gc.ca; Saul, Dawolu; Bailey, Esme; Giolti, Patrizia
Cc: Champoux, Martin; Wilson, Barbara; Swift, Andrew; Williams, Christpher; Duval, Jean Paul; Carta, John
Subject: RE: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Colleagues,

Just an update - only media interest we have seen so far is from a radio station in the Outaouais . Online story is below for your information. Initial call went to CSE and it was forwarded to us and we responded yesterday afternoon with the lines below.

We have not noted any other media coverage or received any other calls.

As promised, we will advise if direction on media relations protocol changes. In the meantime, please do send any calls may receive our way.

Many thanks,
Jessica

EXCLUSIF: Anonymous veut attaquer le gouvernement fédéral
Le 29 octobre, 2012
98,5 FM

Le groupe de pirates informatiques et d'activistes Anonymous a le gouvernement fédéral dans sa mire.

Selon nos informations, pas moins de 44 ministères ont vu leurs défenses numériques testées par des cyberpirates.

Depuis 9h30 lundi matin, nous attendons des retours d'appels effectués auprès du Centre de la sécurité des télécommunications du Canada.

On s'attend à ce que les pirates informatiques d'Anonymous mènent une attaque d'envergure contre le gouvernement du Canada entre le 3 et le 15 novembre prochain.

Lien

From: Slack, Jessica **On Behalf Of** PS Media Relations / Relations médias SP
Sent: October-26-12 4:33 PM
To: @cse-cst.gc.ca; @cse-cst.gc.ca; julie.gagnon@rcmp-grc.gc.ca; Theresa.Knowles@tbs-sct.gc.ca; TBS Media / Media SCT; mylene.dupere@tpsgc-pwgsc.gc.ca; ted.francis@ssc-spc.gc.ca; sebastien.bois@tpsgc-pwgsc.gc.ca; Isabelle.Scott@cra-arc.gc.ca
Cc: Champoux, Martin; Wilson, Barbara; Swift, Andrew (Andrew.Swift@ps-sp.gc.ca); Williams, Christpher; Duval, Jean Paul; Carta, John
Subject: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Colleagues,

Further to the note below (issued by CTEC) regarding Anonymous' plan for Distributed Denial of Service attacks on government websites, we wanted to touch base regarding the media relations protocol in advance of the weekend.

Direction at this time is that all departments should send any calls they receive to Public Safety for response (our contact info: media@ps-sp.gc.ca / 613-991-0657)

The approved media lines are below for your information.

Please do not hesitate to get in touch should you have any questions.

We will be in touch further next week.

Many thanks,

Pages 646 to / à 647

are duplicates of

sont des duplicatas des

pages 614 to / à 615

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Wilson, Barbara

From: Swift, Andrew
Sent: Friday, November 02, 2012 9:51 AM
To: Slack, Jessica
Cc: Wilson, Barbara; Champoux, Martin
Subject: FW: Media lines>Cyber-attack

FYI

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Swift, Andrew
Sent: Friday, November 02, 2012 9:50 AM
To: 'Thibouthot, Akim Isabelle'; Stephanie.Hebert@tbs-sct.gc.ca; Stephan.Belanger@ic.gc.ca
Cc: Durand, Stéphanie; Williams, Christpher
Subject: RE: Media lines>Cyber-attack

Hi everyone,

The following lines were approved by PS MO and PCO late last week on this issue.

The current media relations protocol is for all calls on the matter to go to PS (613-991-0657 / media@ps-sp.gc.ca).

Andrew

The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Thibouthot, Akim Isabelle [mailto:AkimIsabelle.Thibouthot@pco-bcp.gc.ca]
Sent: Friday, November 02, 2012 9:46 AM
To: Stephanie.Hebert@tbs-sct.gc.ca; Stephan.Belanger@ic.gc.ca
Cc: Durand, Stéphanie; Williams, Christpher; Swift, Andrew
Subject: Re: Media lines>Cyber-attack

Yes, PS is coordinating.

From: Hébert, Stephanie [mailto:Stephanie.Hebert@tbs-sct.gc.ca]
Sent: Friday, November 02, 2012 09:41 AM
To: Belanger, Stephan: IC.IC <Stephan.Belanger@ic.gc.ca>
Cc: Thibouthot, Akim Isabelle; Durand, Stephanie: PS-SP <stephanie.durand@ps-sp.gc.ca>
Subject: Re: Media lines>Cyber-attack

My understanding is that Public Safety is the lead on external communications on GC cyber issues.

I have copied Akim and Stephanie so they can assist.

From: Stephan.Belanger@ic.gc.ca [mailto:Stephan.Belanger@ic.gc.ca]
Sent: Friday, November 02, 2012 09:35 AM
To: Hébert, Stephanie
Subject: Media lines>Cyber-attack

Hi Stephanie,

Hope all is well with you!

Just wondering if there are any media lines re: the DDOS cyber attack.

Should depts field enquries or fwd them on to a central body.

Thanks v much.

S

Stephan Belanger
Senior Director | Directeur principal
Communications Branch | Direction générale des communications
Industry Canada | Industrie Canada
stephan.belanger@ic.gc.ca
Telephone | Téléphone 613-943-7081
Facsimile | Télécopieur 613-954-6436
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada
bb [redacted] s.19(1)

Slack, Jessica

From: Slack, Jessica
Sent: November-02-12 1:06 PM
To: Swift, Andrew (Andrew.Swift@ps-sp.gc.ca)
Cc: Duval, Jean Paul
Subject: FW: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

fyi

From: [redacted]@CSE-CST.GC.CA]
Sent: November-02-12 12:29 PM
To: Champoux, Martin; Filipps, Lisa; Slack, Jessica
Cc: [redacted]; ted.francis@ssc-spc.gc.ca; Plamondon, Jean J.; [redacted]
Subject: FW: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Classification: UNCLASSIFIED

Hi,

I just checked in with our CTEC guys for a status report. So far, the DDoS effects remain "petty" or small (as you may well already know). The goup has posted its intent to create DDoS' from noon until 6 over the weekend and from 6 to 10 Tuesday to Friday. CTEC will continue to monitor Saturday/Sunday, perhaps bunking with SSC.

I will check our media line over the weekend and if there is anything, I will of course send details to media@ps-sp.gc.ca.

regards,

[redacted]

[redacted]
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada
Ottawa, Canada K1G 3Z4
[redacted]@cse-cst.gc.ca
Telephone | Téléphone [redacted]
Fax | Télécopieur 613-991-7691
Government of Canada | Gouvernement du Canada

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca] **On Behalf Of** PS Media Relations / Relations médias SP
Sent: October 31, 2012 10:15 AM
To: PS Media Relations / Relations médias SP; [redacted] 'julie.gagnon@rcmp-grc.gc.ca'; [redacted] 'Theresa.Knowles@tbs-sct.gc.ca'; 'TBS Media / Média SCT'; 'mylene.dupere@tpsgc-pwgsc.gc.ca'; 'ted.francis@ssc-spc.gc.ca'; 'sebastien.bois@tpsgc-pwgsc.gc.ca'; Isabelle.Scott@cra-arc.gc.ca; Saul, Dawolu; Bailey, Esme; Giolti, Patrizia
Cc: Champoux, Martin; Wilson, Barbara; Swift, Andrew; Williams, Christpher; Duval, Jean Paul; Carta, John
Subject: RE: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS

Colleagues,

Just an update - only media interest we have seen so far is from a radio station in the Outaouais . Online story is below for your information. Initial call went to CSE and it was forwarded to us and we responded yesterday afternoon with the lines below.
We have not noted any other media coverage or received any other calls.
As promised, we will advise if direction on media relations protocol changes. In the meantime, please do send any calls may receive our way.

Many thanks,
Jessica

EXCLUSIF: Anonymous veut attaquer le gouvernement fédéral
Le 29 octobre, 2012
98,5 FM
Le groupe de pirates informatiques et d'activistes Anonymous a le gouvernement fédéral dans sa mire.
Selon nos informations, pas moins de 44 ministères ont vu leurs défenses numériques testées par des cyberpirates.
Depuis 9h30 lundi matin, nous attendons des retours d'appels effectués auprès du Centre de la sécurité des télécommunications du Canada.
On s'attend à ce que les pirates informatiques d'Anonymous mènent une attaque d'envergure contre le gouvernement du Canada entre le 3 et le 15 novembre prochain.
Lien

From: Slack, Jessica **On Behalf Of** PS Media Relations / Relations médias SP
Sent: October-26-12 4:33 PM
To: [redacted]@cse-cst.gc.ca; [redacted]@cse-cst.gc.ca; julie.gagnon@rcmp-grc.gc.ca; [redacted] Theresa.Knowles@tbs-sct.gc.ca; TBS Media / Média SCT; mylene.dupere@tpsgc-pwgsc.gc.ca; ted.francis@ssc-spc.gc.ca; sebastien.bois@tpsgc-pwgsc.gc.ca; Isabelle.Scott@cra-arc.gc.ca
Cc: Champoux, Martin; Wilson, Barbara; Swift, Andrew (Andrew.Swift@ps-sp.gc.ca); Williams, Christpher; Duval, Jean Paul; Carta, John
Subject: MEDIA RELATIONS PROTOCOL RE ANONYMOUS DDoS ATTACKS
Colleagues,
Further to the note below (issued by CTEC) regarding Anonymous' plan for Distributed Denial of Service attacks on government websites, we wanted to touch base regarding the media relations protocol in advance of the weekend.

Direction at this time is that all departments should send any calls they receive to Public Safety for response (our contact info: media@ps-sp.gc.ca / 613-991-0657)
The approved media lines are below for your information.
Please do not hesitate to get in touch should you have any questions.
We will be in touch further next week.
Many thanks,

Jessica

Media Lines

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.
- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, October 26, 2012 4:23 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2
Importance: High
Classification: UNCLASSIFIED

La version française suivra.

==========

s.16(2)

GC CTEC - Information Note IN12-002
Date: 25 October 2012

==========

==========

Update 2: 26 October 2012

==========

==========

Anonymous DDOS activity against GC

==========

AUDIENCE

========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT

==========

[redacted]

SUGGESTED ACTION

==========

[redacted]

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both :
- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Pages 656 to / à 657

are duplicates of

sont des duplicatas des

pages 665 to / à 666

Page 658
is a duplicate of
est un duplicata de la
page 707

Page 659
is a duplicate of
est un duplicata de la
page 706

Pages 660 to / à 664

are duplicates of

sont des duplicatas des

pages 701 to / à 705

Swift, Andrew

From: Swift, Andrew
Sent: Saturday, November 03, 2012 9:26 AM
To: COMDO; Miller, Kevin
Subject: Re: CE12-003863 [#OpPartyCrasher Anonymous DDoS]

Categories: ATI PRINT

Thanks Karolina. I will follow up.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: COMDO
Sent: Saturday, November 03, 2012 07:46 AM
To: Swift, Andrew; Miller, Kevin
Subject: FW: CE12-003863 [#OpPartyCrasher Anonymous DDoS]

Good morning,

[redacted] http://pastebay.net/ [redacted]

[redacted]
http://www.pastebay.net/ [redacted]

The minister's website is currently up and running. I will flag any updates to you.

Thanks,

Karolina

-----Original Message-----
From: Beaudoin, Luc
Sent: November 3, 2012 4:19 AM
To: COMDO
Cc: Champoux, Martin; Anderson, Windy; CYBERDO
Subject: Fw: CE12-003863 [#OpPartyCrasher Anonymous DDoS]

FYI. This is not impacting any vital systems, but from a comms perspective, you may want to inform our public affairs staff.

Please do not pass on , or make public that DND reported this to us, nor that we contacted the site admin.

Luc

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----
From: CYBERDO
Sent: Saturday, November 03, 2012 02:29 AM
To: Beaudoin, Luc; Anderson, Windy
Cc: CYBERDO
Subject: CE12-003863 [#OpPartyCrasher Anonymous DDoS]

Hello Luc, Wendy,

[redacted]

Received the info from DND.

[redacted]

Slack, Jessica

From: Durand, Stéphanie
Sent: November-03-12 1:46 PM
To: Swift, Andrew
Cc: Tomlinson, Jamie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul; Carta, John
Subject: Re: DDoS media call - Le Droit

Thanks - yes, pls consult with Robert and Suki. Thx

----- Original Message -----
From: Swift, Andrew
Sent: Saturday, November 03, 2012 01:43 PM
To: Durand, Stéphanie
Cc: Tomlinson, Jamie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul; Carta, John
Subject: DDoS media call - Le Droit

Stephanie,
We've received a media call on DDoS.

While the reporter doesn't identify the source of the threat, we do identify that one has been made by Anonymous in our lines which we used for the only other call we received earlier this week. Do you want me to send to Robert Dick and Suki first before sending to the MO?
Andrew

-The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

-While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

-Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

-Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.
Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: PS Media Relations / Relations médias SP

Sent: Saturday, November 03, 2012 12:45 PM
To: Filipps, Lisa; Slack, Jessica; Swift, Andrew; Swift, Andrew; Picard, Josée; Manning, Kerri; Wilson, Barbara; Champoux, Martin; Van Criekingen, Jane; Duval, Jean Paul
Subject: FW:

From:
Sent: November-03-12 12:45:37 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject:

Several directors of the government of Canada have received emails regarding a possible cyberattack on govt websites for the period ranging from Nov 2 to 15 2012. According to that message, the level of alert is at High.

Here are my questions:
When has the govt learned of this,
What actions are taken to protect the Internet infrastructure of the GoC, Were does the threat come from, Etc.

Regards,

Journaliste - LeDroit

Durand, Stéphanie

From: Boudreau, Paul <Paul.Boudreau@tbs-sct.gc.ca>
Sent: Saturday, November 03, 2012 2:15 PM
To: Durand, Stéphanie
Subject: Re: Information Note IN12-002: Anonymous Distributed Denial of Service (DDOS) activity against the Government of Canada (GC) / Note d'information IN12-002: Attaques par déni de service distribuées (« DDOS ») d'Anonymous contre le gouvernement du Canada (G

My pleasure.

Paul
This message was sent via my BlackBerry handheld device.

From: Durand, Stéphanie [mailto:Stephanie.Durand@ps-sp.gc.ca]
Sent: Saturday, November 03, 2012 02:12 PM
To: Boudreau, Paul
Subject: Re: Information Note IN12-002: Anonymous Distributed Denial of Service (DDOS) activity against the Government of Canada (GC) / Note d'information IN12-002: Attaques par déni de service distribuées (« DDOS ») d'Anonymous contre le gouvernement du Canada (G

Thanks for copying me. This will be helpful going forward.

From: Boudreau, Paul [mailto:Paul.Boudreau@tbs-sct.gc.ca]
Sent: Saturday, November 03, 2012 02:00 PM
To: 'craig.oldham@opscen.gc.ca' <'craig.oldham@opscen.gc.ca'>; D'Iorio, Colleen <Colleen.Diorio@tbs-sct.gc.ca>; Parson, Stephane <Stephane.Parson@tbs-sct.gc.ca>; 'stan.burke@rcmp-grc.gc.ca' <'stan.burke@rcmp-grc.gc.ca'>; 'Eric.Belzile@ssc-spc.gc.ca' <Eric.Belzile@ssc-spc.gc.ca>; 'Rod.Lander@forces.gc.ca' <'Rod.Lander@forces.gc.ca'>; @cse-cst.gc.ca' <@cse-cst.gc.ca>; Hebert, Brigitte: PWGSC.TPSGC <brigitte.hebert@tpsgc-pwgsc.gc.ca>; 'patrice.nadeau@ssc-spc.gc.ca' <'patrice.nadeau@ssc-spc.gc.ca'>; 'robert.dick@ps-sp.gc.ca' <'robert.dick@ps-sp.gc.ca'>; 'tony.pickett@rcmp-grc.gc.ca' <'tony.pickett@rcmp-grc.gc.ca'>; @cse-cst.gc.ca' <@cse-cst.gc.ca'>; Durand, Stéphanie
Subject: Re: Information Note IN12-002: Anonymous Distributed Denial of Service (DDOS) activity against the Government of Canada (GC) / Note d'information IN12-002: Attaques par déni de service distribuées (« DDOS ») d'Anonymous contre le gouvernement du Canada (G

For your information.

Paul
This message was sent via my BlackBerry handheld device.

From: Boudreau, Paul
Sent: Saturday, November 03, 2012 01:59 PM
To: 'craig.oldham@opscen.gc.ca' <'craig.oldham@opscen.gc.ca'>; D'Iorio, Colleen; Parson, Stephane; 'stan.burke@rcmp-grc.gc.ca' <'stan.burke@rcmp-grc.gc.ca'>; Eric.Belzile@ssc-spc.gc.ca' <Eric.Belzile@ssc-spc.gc.ca>; 'Rod.Lander@forces.gc.ca' <'Rod.Lander@forces.gc.ca'>; @cse-cst.gc.ca' @cse-cst.gc.ca>; 'Brigitte.Hebert@tpsgc-pwgsc.gc.ca' <Brigitte.Hebert@tpsgc-pwgsc.gc.ca>; 'patrice.nadeau@ssc-spc.gc.ca' <'patrice.nadeau@ssc-spc.gc.ca'>; 'robert.dick@ps-sp.gc.ca' <'robert.dick@ps-sp.gc.ca'>; 'tony.pickett@rcmp-grc.gc.ca' <'tony.pickett@rcmp-grc.gc.ca'>
Subject: Fw: Information Note IN12-002: Anonymous Distributed Denial of Service (DDOS) activity against the

Government of Canada (GC) / Note d'information IN12-002: Attaques par déni de service distribuées (« DDOS ») d'Anonymous contre le gouvernement du Canada (G

This message was sent via my BlackBerry handheld device.

From: D'Iorio, Colleen
Sent: Saturday, November 03, 2012 09:09 AM
To: Boudreau, Paul
Cc: Parson, Stephane
Subject: Fw: Information Note IN12-002: Anonymous Distributed Denial of Service (DDOS) activity against the Government of Canada (GC) / Note d'information IN12-002: Attaques par déni de service distribuées (« DDOS ») d'Anonymous contre le gouvernement du Canada (G

Paul -

This is the note that Corinne sent yesterday. Would you please forward to the MT dist list?

Thanks,

C.

From: O'Neill, Elaine
Sent: Friday, November 02, 2012 05:33 PM
To: D'Iorio, Colleen
Subject: FW: Information Note IN12-002: Anonymous Distributed Denial of Service (DDOS) activity against the Government of Canada (GC) / Note d'information IN12-002: Attaques par déni de service distribuées (« DDOS ») d'Anonymous contre le gouvernement du Canada (G

FYI...

Thank you

Elaine O'Neill

Executive Assistant and Issues Manager | Adjointe exécutive et gestionnaire des enjeux

Office of the Chief Information Officer | Bureau de la Dirigeante principale de l'information

Chief Information Officer Branch | Direction du dirigeant principal de l'information

Treasury Board of Canada, Secretariat | Secrétariat du Conseil du Trésor du Canada

L'Esplanade Laurier – Room: 07154, 7th Floor, 140 O'Connor Street | L'Esplanade Laurier – Salle: 07154, 7e Étage, 140, rue O'Connor

Ottawa, Ontario, Canada K1A 0R5

Elaine.O'Neill@tbs-sct.gc.ca

Telephone | Téléphone 613-957-9681 / Facsimile | Télécopieur 613-952-8536 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

From: Charette, Corinne
Sent: November 2, 2012 5:22 PM
Subject: Information Note IN12-002: Anonymous Distributed Denial of Service (DDOS) activity against the Government of Canada (GC) / Note d'information IN12-002: Attaques par déni de service distribuées (« DDOS ») d'Anonymous contre le gouvernement du Canada (GC)

Background

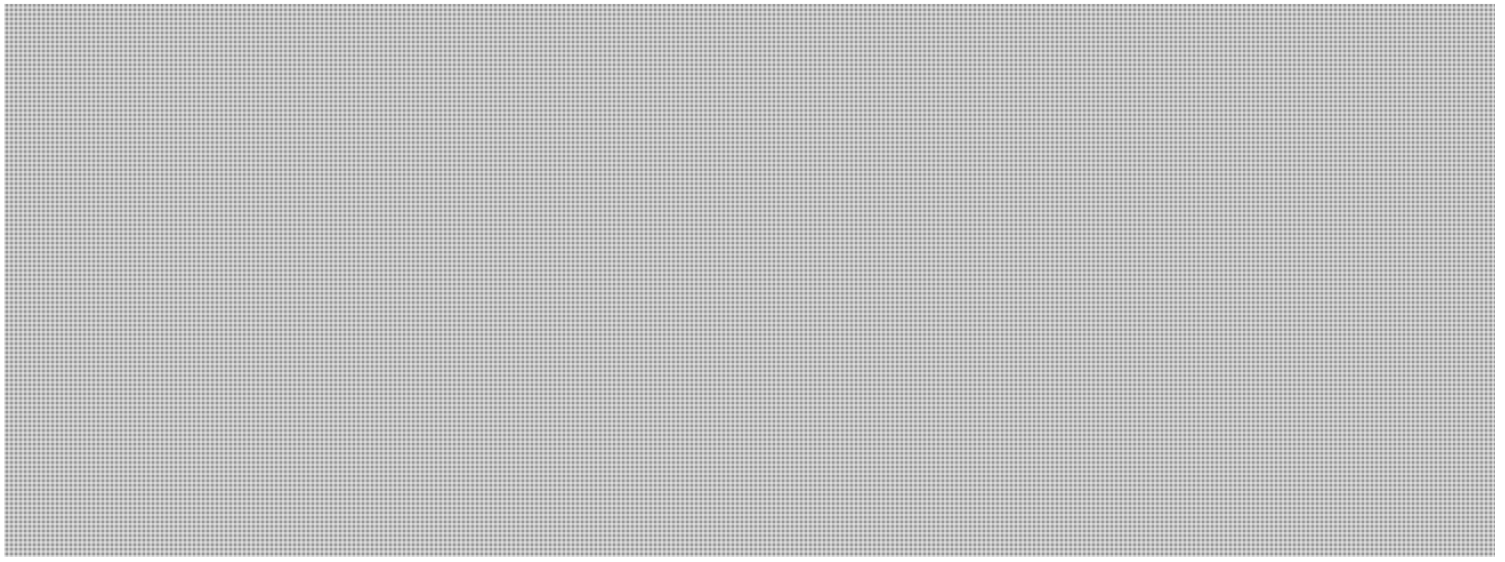
As reported by the Secretary of the Treasury Board at the Deputy Heads' breakfast on October 31st, the Communications Security Establishment Canada (CSEC) identified that a Distributed Denial of Service (DDoS) operation against the Government of Canada may be imminent. This possible attack has the potential to cause online service disruptions.

Current information indicates that this operation is scheduled to run from November 3, 2012 to November 15, 2012.

Current Status

As of November 2nd, there are continuing reports that activity potentially related to this attack has been identified on some Government of Canada networks. The level of activity may vary over the next few days.

Mitigation strategies



Media relations

Public Safety Canada is identified as the media relations lead on this issue. If your organizations receive media enquiries, please refer them to:

Public Safety Canada

s.15(1) - Subv

Media Relations

T: 613-991-0657

E: media@ps-sp.gc.ca

Corinne Charette
Chief Information Officer of the Government of Canada | Dirigeant principal de l'information du gouvernement du canada
Chief Information Officer | Dirigeante principale de l'information
Chief Information Officer Branch | Direction du dirigeant principal de l'information
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Corinne.Charette@tbs-sct.gc.ca

Telephone | Téléphone 613-957-7070 / Facsimile | Télécopieur 613-952-8536 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

Contexte

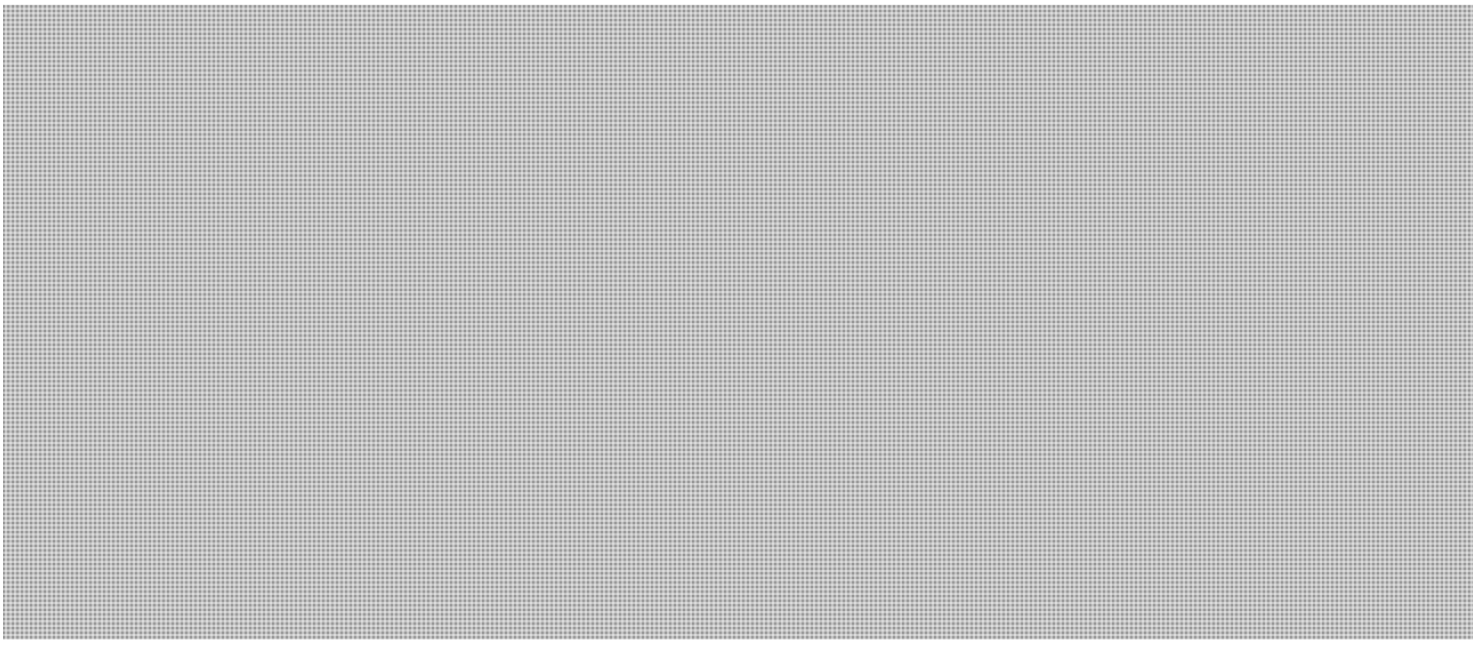
Comme l'a indiqué la secrétaire du Conseil du Trésor lors du Déjeuner des sous-ministres le 31 octobre dernier, le Centre de la sécurité des télécommunications Canada (CSTC) a découvert qu'une attaque de déni de service distribué (DDoS) contre le gouvernement du Canada pourrait être imminente. Cette attaque potentielle pourrait provoquer une interruption des services en ligne.

D'après les renseignements dont nous disposons à l'heure actuelle, cette attaque devrait avoir lieu entre le 3 et le 15 novembre 2012.

État actuel de la situation

En date du 2 novembre, on a signalé à plusieurs reprises des activités sur certains des réseaux du gouvernement du Canada qui pourraient avoir un lien avec cette attaque. Le niveau d'activité pourrait varier au cours des quelques prochains jours.

Stratégies d'atténuation



s.15(1) - Subv

Relations avec les médias

Sécurité publique Canada est responsable des relations avec les médias dans ce dossier. Si votre organisation reçoit des demandes de renseignements des médias, veuillez les acheminer vers :

Relations avec les médias
Sécurité publique Canada
613-991-0657

media@ps-sp.gc.ca

Corinne Charette
Chief Information Officer of the Government of Canada | Dirigeant principal de l'information du gouvernement du canada
Chief Information Officer | Dirigeante principale de l'information
Chief Information Officer Branch | Direction du dirigeant principal de l'information
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Corinne.Charette@tbs-sct.gc.ca

Telephone | Téléphone 613-957-7070 / Facsimile | Télécopieur 613-952-8536 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

Slack, Jessica

From: Wong, Suki
Sent: November-03-12 2:28 PM
To: Dick, Robert; Swift, Andrew
Cc: Durand, Stéphanie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Agree

----- Original Message -----
From: Dick, Robert
Sent: Saturday, November 03, 2012 02:24 PM
To: Swift, Andrew; Wong, Suki
Cc: Durand, Stéphanie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

That works, though you may wish to refer simply to the Strategy rather than specify pillar 1 (it doesn't seem to add much except length).

----- Original Message -----
From: Swift, Andrew
Sent: Saturday, November 03, 2012 01:52 PM
To: Dick, Robert; Wong, Suki
Cc: Durand, Stéphanie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: FOR REVIEW: DDoS media call - Le Droit

Robert and Suki,
See enquiry below. The reporter asks about the source of our threat, which is identified in our lines. Any objections to our previously approved media lines? We would seek MO and PCO approval, and would advise partners.

-The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

-While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

-Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

-Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

Andrew

Andrew Swift

Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: PS Media Relations / Relations médias SP
Sent: Saturday, November 03, 2012 12:45 PM
To: Filipps, Lisa; Slack, Jessica; Swift, Andrew; Swift, Andrew; Picard, Josée; Manning, Kerri; Wilson, Barbara; Champoux, Martin; Van Criekingen, Jane; Duval, Jean Paul
Subject: FW:

From: [redacted]
Sent: November-03-12 12:45:37 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject:

Several directors of the government of Canada have received emails regarding a possible cyberattack on govt websites for the period ranging from Nov 2 to 15 2012. According to that message, the level of alert is at High.

Here are my questions:
When has the govt learned of this,
What actions are taken to protect the Internet infrastructure of the GoC, Were does the threat come from, Etc.

Regards,

[redacted]
Journaliste [redacted] - LeDroit
[redacted]

Slack, Jessica

From: Swift, Andrew
Sent: November-03-12 2:35 PM
To: Dick, Robert; Wong, Suki
Cc: Durand, Stéphanie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Thx, I have advised MO. Will keep you posted.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Dick, Robert
Sent: Saturday, November 03, 2012 02:32 PM
To: Swift, Andrew; Wong, Suki
Cc: Durand, Stéphanie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

If we've not done so before, I wouldn't here. It's not such much for reasons of secrecy, as of lending profile and credibility to a so-called group. Why not just say "the GoC is aware of calls to undertake DDoS..."

In effect, wherever something is attributed to "Anonymous" it may as well read "someone or unidentified people"...

----- Original Message -----
From: Swift, Andrew
Sent: Saturday, November 03, 2012 02:28 PM
To: Dick, Robert; Wong, Suki
Cc: Durand, Stéphanie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Ok, so it would read:

"...significant action to protect its own IT systems as part of Canada's Cyber Security Strategy."

Any concerns about identifying the source of the threat? I noticed that the CIO message circulated yesterday (where it looks like the reporter is getting his info) makes no reference to Anonymous.

Andrew
Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549

Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Dick, Robert
Sent: Saturday, November 03, 2012 02:24 PM
To: Swift, Andrew; Wong, Suki
Cc: Durand, Stéphanie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

That works, though you may wish to refer simply to the Strategy rather than specify pillar 1 (it doesn't seem to add much except length).

----- Original Message -----
From: Swift, Andrew
Sent: Saturday, November 03, 2012 01:52 PM
To: Dick, Robert; Wong, Suki
Cc: Durand, Stéphanie; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: FOR REVIEW: DDoS media call - Le Droit

Robert and Suki,
See enquiry below. The reporter asks about the source of our threat, which is identified in our lines. Any objections to our previously approved media lines? We would seek MO and PCO approval, and would advise partners.

-The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

-While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

****

-Le gouvernement du Canada est conscient des menaces d'Anonymous d'organiser des attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.

-Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

Andrew

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: PS Media Relations / Relations médias SP
Sent: Saturday, November 03, 2012 12:45 PM

To: Filipps, Lisa; Slack, Jessica; Swift, Andrew; Swift, Andrew; Picard, Josée; Manning, Kerri; Wilson, Barbara; Champoux, Martin; Van Criekingen, Jane; Duval, Jean Paul
Subject: FW:

From: [redacted]
Sent: November-03-12 12:45:37 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject:

Several directors of the government of Canada have received emails regarding a possible cyberattack on govt websites for the period ranging from Nov 2 to 15 2012. According to that message, the level of alert is at High.

Here are my questions:
When has the govt learned of this,
What actions are taken to protect the Internet infrastructure of the GoC, Were does the threat come from, Etc.

Regards,

[redacted]
Journaliste [redacted] LeDroit
[redacted]

Austria, Jamela

From: Carta, John
Sent: Saturday, November 03, 2012 3:16 PM
To: Austria, Jamela; Willey, Chris
Subject: Fw: FOR REVIEW: DDoS media call - Le Droit

Fyi

----- Original Message -----
From: Swift, Andrew
Sent: Saturday, November 03, 2012 02:34 PM
To: Carmichael, Julie; Johnson, Mark; Mueller, Mike; McGrath, Andrew
Cc: Durand, Stéphanie; Wilson, Barbara; Duval, Jean Paul; Slack, Jessica; Carta, John
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Julie,
I should add, let me know whether you think we should identify Anonymous as the source of the threat or if we should just refer to the threat itself.
Andrew

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Swift, Andrew
Sent: Saturday, November 03, 2012 02:32 PM
To: Carmichael, Julie; Johnson, Mark; Mueller, Mike; McGrath, Andrew
Cc: Durand, Stéphanie; Wilson, Barbara; Duval, Jean Paul; Slack, Jessica; Carta, John
Subject: FOR REVIEW: DDoS media call - Le Droit

Julie,
See enquiry below from Le Droit about the DDoS threat/attack.
The following previously approved lines were reviewed again this afternoon by Robert Dick (DG, Cyber Security). Once approved, we would notify PCO and other partners of the enquiry and the response.
Andrew

-The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

-While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as part of Canada's Cyber Security Strategy.

Andrew Swift
Director, Public Affairs

Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: PS Media Relations / Relations médias SP
Sent: Saturday, November 03, 2012 12:45 PM
To: Filipps, Lisa; Slack, Jessica; Swift, Andrew; Swift, Andrew; Picard, Josée; Manning, Kerri; Wilson, Barbara; Champoux, Martin; Van Criekingen, Jane; Duval, Jean Paul
Subject: FW:

From: [redacted]
Sent: November-03-12 12:45:37 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject:

Several directors of the government of Canada have received emails regarding a possible cyberattack on govt websites for the period ranging from Nov 2 to 15 2012. According to that message, the level of alert is at High.

Here are my questions:
When has the govt learned of this,
What actions are taken to protect the Internet infrastructure of the GoC, Were does the threat come from, Etc.

Regards,

[redacted]
Journaliste [redacted] LeDroit

Page 681

is a duplicate of

est un duplicata de la

page 684

Page 682

is a duplicate of

est un duplicata de la

page 689

Page 683

is a duplicate of

est un duplicata de la

page 691

Duval, Jean Paul

From: Duval, Jean Paul
Sent: Saturday, November 03, 2012 3:30 PM
To: Swift, Andrew; Slack, Jessica
Cc: Wilson, Barbara
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Sure, I'm on it!

----- Original Message -----
From: Swift, Andrew
Sent: Saturday, November 03, 2012 03:28 PM
To: Duval, Jean Paul; Slack, Jessica
Cc: Wilson, Barbara
Subject: Fw: FOR REVIEW: DDoS media call - Le Droit

JP,
Can you deliver the update lines to the reporter below?
Andrew

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Williams, Christopher [mailto:Christopher.Williams@pco-bcp.gc.ca]
Sent: Saturday, November 03, 2012 03:27 PM
To: Swift, Andrew; Thibouthot, AkimIsabelle
Cc: Durand, Stéphanie; Carta, John; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Works for me Andrew, no concerns. Thanks.

----- Original Message -----
From: Swift, Andrew [mailto:Andrew.Swift@ps-sp.gc.ca]
Sent: Saturday, November 03, 2012 03:25 PM
To: Williams, Christopher; Thibouthot, Akim Isabelle
Cc: Durand, Stéphanie <Stephanie.Durand@ps-sp.gc.ca>; Carta, John <John.Carta@ps-sp.gc.ca>; Wilson, Barbara <Barbara.Wilson@ps-sp.gc.ca>; Slack, Jessica <Jessica.Slack@ps-sp.gc.ca>; Duval, Jean Paul <JeanPaul.Duval@ps-sp.gc.ca>
Subject: Fw: FOR REVIEW: DDoS media call - Le Droit

Chris,
See below, we've had a call on DDoS. MO recommends we change bullets to remove reference to "Anonymous". We will advise partners of the call, once approved.

Pages 685 to / à 687

are duplicates of

sont des duplicatas des

pages 689 to / à 691

Slack, Jessica

From: Williams, Christopher <Christopher.Williams@pco-bcp.gc.ca>
Sent: November-03-12 3:33 PM
To: Swift, Andrew; Thibouthot, AkimIsabelle
Cc: Durand, Stéphanie; Carta, John; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Thanks. I've briefed up on my end.

----- Original Message -----
From: Swift, Andrew [mailto:Andrew.Swift@ps-sp.gc.ca]
Sent: Saturday, November 03, 2012 03:32 PM
To: Williams, Christopher; Thibouthot, Akim Isabelle
Cc: Durand, Stéphanie <Stephanie.Durand@ps-sp.gc.ca>; Carta, John <John.Carta@ps-sp.gc.ca>; Wilson, Barbara <Barbara.Wilson@ps-sp.gc.ca>; Slack, Jessica <Jessica.Slack@ps-sp.gc.ca>; Duval, Jean Paul <JeanPaul.Duval@ps-sp.gc.ca>
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Thanks Chris. JP will respond now. I will advise TBS, SSC, CSEC, RCMP, CSIS.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Williams, Christopher [mailto:Christopher.Williams@pco-bcp.gc.ca]
Sent: Saturday, November 03, 2012 03:27 PM
To: Swift, Andrew; Thibouthot, AkimIsabelle
Cc: Durand, Stéphanie; Carta, John; Wilson, Barbara; Slack, Jessica; Duval, Jean Paul
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Works for me Andrew, no concerns. Thanks.

----- Original Message -----
From: Swift, Andrew [mailto:Andrew.Swift@ps-sp.gc.ca]
Sent: Saturday, November 03, 2012 03:25 PM
To: Williams, Christopher; Thibouthot, Akim Isabelle
Cc: Durand, Stéphanie <Stephanie.Durand@ps-sp.gc.ca>; Carta, John <John.Carta@ps-sp.gc.ca>; Wilson, Barbara <Barbara.Wilson@ps-sp.gc.ca>; Slack, Jessica <Jessica.Slack@ps-sp.gc.ca>; Duval, Jean Paul <JeanPaul.Duval@ps-sp.gc.ca>
Subject: Fw: FOR REVIEW: DDoS media call - Le Droit

Chris,

See below, we've had a call on DDoS. MO recommends we change bullets to remove reference to "Anonymous". We will advise partners of the call, once approved.

-The Government of Canada is aware of the threat to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

-While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as part of Canada's Cyber Security Strategy.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Carmichael, Julie
Sent: Saturday, November 03, 2012 03:22 PM
To: Swift, Andrew; Johnson, Mark; Mueller, Mike; McGrath, Andrew
Cc: Durand, Stéphanie; Wilson, Barbara; Duval, Jean Paul; Slack, Jessica; Carta, John
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Please removed reference to Anonymous.

Otherwise good

Julie Carmichael
Director of Communications
Office of the Minister of Public Safety

----- Original Message -----
From: Swift, Andrew
Sent: Saturday, November 03, 2012 02:34 PM
To: Carmichael, Julie; Johnson, Mark; Mueller, Mike; McGrath, Andrew
Cc: Durand, Stéphanie; Wilson, Barbara; Duval, Jean Paul; Slack, Jessica; Carta, John
Subject: Re: FOR REVIEW: DDoS media call - Le Droit

Julie,
I should add, let me know whether you think we should identify Anonymous as the source of the threat or if we should just refer to the threat itself.
Andrew

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----

From: Swift, Andrew
Sent: Saturday, November 03, 2012 02:32 PM
To: Carmichael, Julie; Johnson, Mark; Mueller, Mike; McGrath, Andrew
Cc: Durand, Stéphanie; Wilson, Barbara; Duval, Jean Paul; Slack, Jessica; Carta, John
Subject: FOR REVIEW: DDoS media call - Le Droit

Julie,
See enquiry below from Le Droit about the DDoS threat/attack.
The following previously approved lines were reviewed again this afternoon by Robert Dick (DG, Cyber Security). Once approved, we would notify PCO and other partners of the enquiry and the response.
Andrew

-The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

-While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as part of Canada's Cyber Security Strategy.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: PS Media Relations / Relations médias SP
Sent: Saturday, November 03, 2012 12:45 PM
To: Filipps, Lisa; Slack, Jessica; Swift, Andrew; Swift, Andrew; Picard, Josée; Manning, Kerri; Wilson, Barbara; Champoux, Martin; Van Criekingen, Jane; Duval, Jean Paul
Subject: FW:

s.19(1)

From: [redacted]
Sent: November-03-12 12:45:37 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject:

Several directors of the government of Canada have received emails regarding a possible cyberattack on govt websites for the period ranging from Nov 2 to 15 2012. According to that message, the level of alert is at High.

Here are my questions:
When has the govt learned of this,
What actions are taken to protect the Internet infrastructure of the GoC, Were does the threat come from, Etc.

Regards,

s.19(1)

[redacted] Journaliste [redacted] LeDroit

Champoux, Martin

From: Champoux, Martin
Sent: Saturday, November 03, 2012 4:33 PM
To: Swift, Andrew
Subject: Fw: Update 10: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Just double checking but you get these don't you?

----- Original Message -----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Saturday, November 03, 2012 04:16 PM
To: CTEC <CTEC@CSE-CST.GC.CA>
Subject: Update 10: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 10: 3 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC.

ASSESSMENT

==========

[redacted]

SUGGESTED ACTION

==========

GC-CTEC and SSC will have staff in place this weekend, during the announced attack times, monitoring the situation and providing general mitigation advice including new or updated Cyber Flashes as required. Information note updates will be released as required in order to inform the GC of any changes of attack schedule as well as any trending in DDoS activity observed.

Departments should implement the mitigation advice in above listed Cyber Flashes as well as any other Cyber Flashes that are released.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contain information which may have been collected from external sources for which GC-CTEC cannot verify the accuracy and integrity. GC-CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Saturday, November 03, 2012 7:52 PM
To: Swift, Andrew
Subject: Re: FYI - Twitter: Second target

Thx

From: Swift, Andrew
Sent: Saturday, November 03, 2012 06:50 PM
To: Durand, Stéphanie
Subject: Fw: FYI - Twitter: Second target

FYI

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: COMDO
Sent: Saturday, November 03, 2012 06:08 PM
To: Swift, Andrew; Miller, Kevin
Cc: CYBERDO; GOC-COG
Subject: FYI - Twitter: Second target

TxANONxH 5:59pm via web
Great job everyone! commencing Day 1 #OpPartyCrasher target 2 will be up at midnight.

Durand, Stéphanie

From: Swift, Andrew
Sent: Saturday, November 03, 2012 11:29 PM
To: Durand, Stéphanie
Subject: Fw: (UPDATED) - FYI - Twitter: Second target

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: COMDO
Sent: Saturday, November 03, 2012 09:49 PM
To: COMDO; Swift, Andrew; Miller, Kevin
Cc: CYBERDO; GOC-COG
Subject: (UPDATED) - FYI - Twitter: Second target

Appears to be Minister Flaherty.

Portion below taken from Pastebay (after portion below, message continues with various URLs):

http://www.pastebay.net/ s.16(2)

First off, Great job on day 1. We claim victory over www.victoews.com
it was Tango Down for a total of 4 hours today. (StopWatch :P)
(That is combined times between on/off)

Keep up the twitter campaign and the open letter email

Tweet – Dear @pmharper, We warned you before, #ExpectUs. You should have listened
#STOPHarper #OpPartyCrasher

Tweet – Dear @pmharper, We are here to stop the #Globalization of #Canada
#STOPHarper #OpPartyCrasher

Tweet – Dear @pmharper, We have come to crash your #Capitalist party.
#STOPHarper #OpPartyCrasher

Tweet – Dear @pmharper, We put you in power, and we will take you out. #STOPHarper
#OpPartyCrasher

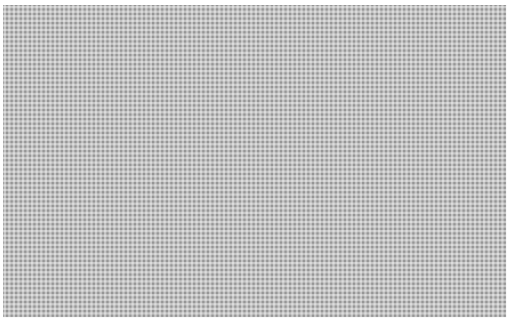
Tweet – Dear @pmharper, #Canada isn't yours to do with as you please. #STOPHarper
#OpPartyCrasher

Make your own as well...

Jim Flaherty,

You continue to approve massive budget cuts, and massive corporate subsidies. The recently released budget is harmful not only to

our native Canadians, but to every Canadian, to the environment. We have warned you and the CPC before about your heinous objectives,
and you failed to comply with the word of Canadians. You, Harper and the goons are stealing our democracy and we are no longer
allowing it. We are here, and you won't stop us. We are Humanity, We are Many, We are Strong, We are Love, You are few.
Canada it's our time to show the Globalists what it means to be Human, it's our time to reclaim Canada.
#OpPartyCrasher



s.16(2)

From: COMDO
Sent: November 3, 2012 6:08 PM
To: Swift, Andrew; Miller, Kevin
Cc: CYBERDO; GOC-COG
Subject: FYI - Twitter: Second target

TxANONxH 5:59pm via web
Great job everyone! commencing Day 1 #OpPartyCrasher target 2 will be up at midnight.

Swift, Andrew

From: COMDO
Sent: Sunday, November 04, 2012 7:43 AM
To: Swift, Andrew
Cc: Miller, Kevin
Subject: FYI: CCIRC CE12-003885 [#OpPartyCrasher
Attachments:

Categories: ATI PRINT

Minister Flahery's website is current up and running. I will continue to monitor for any media coverage, and provide updates.

-----Original Message-----
From: CCIRC-CCRIC
Sent: November 4, 2012 12:57 AM
To:
Cc:
Subject: CCIRC CE12-003885 [#OpPartyCrasher - www.jimflahertymp.ca]

Greetings,

CCIRC is aware of your web site was listed as a target in the Anonymous twitter.com #OpPartyCrasher channel. They are planning to execute a Distributed Denial-of-Service attack. You will find the following Mitigation Guidelines for Denial-of-Service Attacks at http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Please consider the following:

Establish contact with your technical team or host provider.

Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.

Establish 24/7 contact information for your ISP and alternate methods for communications.

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613- Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada

contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Pages 701 to / à 707

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

COMDO

From: COMDO
Sent: Monday, November 05, 2012 11:27 AM
To: GOC-COG
Subject: Tweet re: DDoS attacks

I'm not sure if CCIRC might know what "pastebay" is all about, but maybe this info is useful to them?

Anonymous Canada @binn200798
#OpPartyCrasher Engaged! pastebay.net/ [redacted] #DenounceHarper #DenounceDianneWatts Even Translink Is Corrupt!

s.16(2)

Duval, Jean Paul

From: Filipps, Lisa
Sent: Monday, November 05, 2012 3:38 PM
To: Duval, Jean Paul; Slack, Jessica
Subject: FW: Response - Public Safety Canada

So standard response - we do not comment on security related incidents but we are protected etc. Check quickly with Mark Matz then up through Andrew and Stéphanie.

-----Original Message-----
From: PS Media Relations / Relations médias SP
Sent: Monday, November 05, 2012 3:26 PM
To: Filipps, Lisa; Slack, Jessica; Swift, Andrew; Swift, Andrew; Picard, Josée; Manning, Kerri; Wilson, Barbara; Champoux, Martin; Van Criekingen, Jane; Duval, Jean Paul
Subject: FW: Response - Public Safety Canada

From: [redacted]
Sent: Monday, November 05, 2012 3:22:16 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject: Re: Response - Public Safety Canada

Est-il vrai que la menace émanerait d'Anonymous? La menace provient-elle de l'extérieur du pays ou de l'intérieur?

Le 12-11-05 15:20, « PS Media Relations / Relations médias SP » <PSMediaRelations@ps-sp.gc.ca> a écrit :

>Bonjour [redacted]
>
>À moins d'avoir d'autres questions pour nous, nous avons rien à ajouter
>à ce moment.
>
>Au plaisir,
>JP
>
>-----Original Message-----
>From: [redacted] [mailto: [redacted]@LeDroit.com]
>Sent: Monday, November 05, 2012 12:56 PM
>To: Duval, Jean Paul
>Cc: PS Media Relations / Relations médias SP
>Subject: Re: Response - Public Safety Canada
>

>Bonjour,
>
>Y a-t-il du nouveau dans ce dossier?
>
>
>
>
>
>Le 12-11-03 15:39, « Duval, Jean Paul » <JeanPaul.Duval@ps-sp.gc.ca> a
>écrit :
>
>>Good day
>>
>>In response to your questions, I can confirm the Government of Canada
>>is aware of the threat to organize Distributed Denial of Service
>>attacks on government websites. We are taking the necessary measures
>>to protect against this malicious activity.
>>
>>While we do not discuss details of our response for security reasons,
>>the Government has taken significant action to protect its own IT
>>systems as part of Canada's Cyber Security Strategy.
>>
>>Regards,
>>
>>Jean Paul Duval
>>Public Safety Canada / Sécurité publique Canada Media@ps-sp.gc.ca
>
>
>

Austria, Jamela

From: Austria, Jamela
Sent: Monday, November 05, 2012 3:44 PM
To: 'ted.francis@ssc-spc.gc.ca'
Cc: Carta, John; Willey, Chris; Slack, Jessica
Subject: RE: DDoS lines for OGGO

Hello Ted,

As mentioned on my voicemail, please find pasted below our proposed changes – we recommend adding more clarity regarding the difference between CSEC's and CCIRC's federal/non-federal roles:

Bullet 1:

- The Cyber Threat Evaluation Centre (GC CTEC) within Communications Security Establishment Canada provides a focal point for cyber threat and vulnerability warning, analysis and response **for federal organizations**.

Bullet 1.5
Alternatively, please feel free to use these media lines about CSEC that we have been using:

- The Communications Security Establishment Canada (CSEC) is the Government of Canada Cyber Threat Evaluation Centre (GC-CTEC). As such, CESC detects and analyses the impact of cyber security incidents that affect the confidentiality, integrity or availability of GoC networks.
- CSEC provides mitigation advice to GoC systems owners, as well as guidance and training to promote best IT security practices. CSEC shares cyber threat information and mitigation advice with Public Safety for further dissemination to other levels of government and the private sector.

Last but not least, please find pasted below our proposed change to bullet 3:

- SSC plays a key role in preventing cyber threats and unwarranted intrusions by protecting and securing the integrity of the Government of Canada's IT systems and information. SSC will be leading the mitigation effort with the **federal** service providers as required.

Please feel free to contact me if you would like to discuss.

Thank you,

Jamela Austria
Senior Communications Advisor | Conseillière principale en communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-1675
Mobile | Cellulaire : [redacted] s.19(1)
Fax | Télécopieur : 613-954-0800
E-mail | Courriel: jamela.austria@ps-sp.gc.ca

-----Original Message-----
From: Slack, Jessica
Sent: Monday, November 05, 2012 3:05 PM
To: Austria, Jamela
Subject: FW: DDoS lines for OGGO

Not to add to your load, but I just spoke with John on this request and he said it was ok to flip it your way...not sure to what extent this needs to be in line with Graham's committee appearance materials so will recommend Ted get in touch with you..fyi I told him we were likely not able to respond by 3:30 and he would need to check with CSE about the CTEC line anyway...

Her appearance is later this week...

-----Original Message-----
From: Ted Francis [mailto:Ted.Francis@ssc-spc.gc.ca]
Sent: November-05-12 2:38 PM
To: Slack, Jessica; Champoux, Martin
Cc: Filipps, Lisa
Subject: Re: DDoS lines for OGGO

LOL

Sorry, I assume I can throw out acronyms and all will be understood.

Standing Committee on Ops and Estimates

----- Original Message -----
From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: Monday, November 05, 2012 02:33 PM
To: Ted Francis; Champoux, Martin <Martin.Champoux@ps-sp.gc.ca>
Cc: Filipps, Lisa <Lisa.Filipps@ps-sp.gc.ca>
Subject: RE: DDoS lines for OGGO

Ted, Martin is out today.
I can check on this for you, but can you advise what OGGO is...

-----Original Message-----
From: Ted Francis [mailto:Ted.Francis@ssc-spc.gc.ca]
Sent: November-05-12 2:30 PM
To: Champoux, Martin; Slack, Jessica
Subject: DDoS lines for OGGO

Hi jessica and Martin,

Our President's Office has requested lines concerning the DDoS attacks prior to her appearance at OGGO.

Would PS mind reviewing the attached responses and providing feedback, if required. If you could provide an 'OK' or changes by 3:30, it would be greatly appreciated.

Apologies for the short notice.

- The Government of Canada is aware of the threat by Anonymous to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.

- While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as one pillar of Canada's Cyber Security Strategy.

- The Cyber Threat Evaluation Centre (GC CTEC) within Communications Security Establishment Canada provides a focal point for cyber threat and vulnerability warning, analysis and response. The Cyber Threat Evaluation Centre (CTEC) helps ensure that critical infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest.

- SSC plays a key role in preventing cyber threats and unwarranted intrusions by protecting and securing the integrity of the Government of Canada's IT systems and information. SSC will be leading the mitigation effort with the service providers as required.

- The Government of Canada works with its domestic and international partners to protect critical IT infrastructure from threats.

Thanks,

Ted Francis
Media Relations | Relations avec les médias Shared Services Canada | Services partagés Canada
613-996-0478
434 Queen Street | 434 Rue Queen
PO Box 9808 STN T CSC
ted.francis@ssc-spc.gc.ca

Duval, Jean Paul

From: Filipps, Lisa
Sent: Monday, November 05, 2012 4:03 PM
To: Duval, Jean Paul
Cc: Slack, Jessica
Subject: RE: Media Call: Cyber Threat

That's the one! Thanks.

From: Duval, Jean Paul
Sent: Monday, November 05, 2012 4:03 PM
To: Filipps, Lisa
Cc: Slack, Jessica
Subject: Media Call: Cyber Threat

Lisa is this the line you had in mind as a response to [redacted]? I'll send to translation asap to be sure it comes across correctly.

- We do not comment nor provide details on specific security-related incidents. That said, there are robust measures in place to address cyber incidents and ensure the resilience of Government networks.

Thanks,
JP

****
From: [redacted]
Sent: Monday, November 05, 2012 3:22:16 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject: Re: Response - Public Safety Canada

Est-il vrai que la menace émanerait d'Anonymous? La menace provient-elle de l'extérieur du pays ou de l'intérieur?

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

Duval, Jean Paul

From: Carmichael, Julie
Sent: Monday, November 05, 2012 5:01 PM
To: Duval, Jean Paul; McGrath, Andrew; Johnson, Mark
Cc: Durand, Stéphanie; Swift, Andrew; Filipps, Lisa; Slack, Jessica
Subject: RE: Notification: Media Call - Cyber Attack

Approved

From: Duval, Jean Paul
Sent: November-05-12 4:47 PM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark
Cc: Durand, Stéphanie; Swift, Andrew; Filipps, Lisa; Slack, Jessica
Subject: Notification: Media Call - Cyber Attack

Julie,

We received a media call from Radio Canada on possible DDoS attacks. Do you approve our use of the previously approved lines below?

Approved lines:
-The Government of Canada is aware of the threat to organize Distributed Denial of Service attacks on government websites. We are taking the necessary measures to protect against this malicious activity.
-While we do not discuss details of our response for security reasons, the Government has taken significant action to protect its own IT systems as part of Canada's Cyber Security Strategy.
****
-Le gouvernement du Canada est conscient de menaces d'attaques de déni de service distribué contre les sites Web du gouvernement. Nous prenons les mesures nécessaires pour les protéger contre ces activités malveillantes.
-Pour des raisons de sécurité, nous ne pouvons pas fournir de détails sur les mesures considérables que le gouvernement a prises pour protéger ses systèmes informatiques, qui sont l'un des piliers de la Stratégie de cybersécurité du Canada.

Thanks,
JP

Reporter's Name	[redacted]
Media Outlet	Radio Canada
Call Date	11/5/2012 5:00 PM
Telephone	[redacted]
E-mail address	[redacted]@radio-canada.ca
Deadline	11/6/2012 12:00 PM
Status	Consulting
Branch	
Subject	Cyber Attack
Questions	Quel sont vos commentaires à l'égard de cyber attaques potentiels de déni de service?

s.19(1)

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

s.19(1)

Duval, Jean Paul

From: Carmichael, Julie
Sent: Monday, November 05, 2012 5:30 PM
To: Duval, Jean Paul; McGrath, Andrew; Johnson, Mark
Cc: Durand, Stéphanie; Swift, Andrew; Filipps, Lisa; Slack, Jessica
Subject: RE: For approval: Media Call - Cyber Attack

approved

From: Duval, Jean Paul
Sent: November-05-12 5:25 PM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark
Cc: Durand, Stéphanie; Swift, Andrew; Filipps, Lisa; Slack, Jessica
Subject: For approval: Media Call - Cyber Attack

Julie,

We received a follow-up question from Le Droit seeking confirmation that possible DDoS attacks originate from *Anonymous*. The response below is a translation of previously approved lines. Do you approve?

Thank you,
JP

Proposed response :
We do not comment nor provide details on specific security-related incidents. That said, there are robust measures in place to address cyber incidents and ensure the resilience of Government networks.
***
Nous ne formulons pas de commentaires et nous ne fournissons pas de détails sur des incidents liés à la sécurité. Ceci dit, des mesures robustes sont en place pour faire face aux cyberincidents et assurer la résilience des réseaux du gouvernement.

Reporter's Name	[redacted]	
Media Outlet	Le Droit	
Call Date	11/5/2012 5:00 PM	s.19(1)
Telephone	[redacted]	
E-mail address	[redacted]@LeDroit.com	
Deadline		
Status	Consulting	
Branch		
Subject	Cyber Attack	
Questions	(follow-up to questions on Nov. 3)	
	Est-il vrai que la menace émanerait d'Anonymous? La menace provient-elle de l'extérieur du pays ou de l'intérieur?	

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

s.19(1)

COMDO

From: COMDO
Sent: Tuesday, November 06, 2012 12:13 PM
To: GOC-COG
Subject: FYI - Anonymous tweet re: DDoS target.

s.16(2)

Pages 720 to / à 722

are duplicates of

sont des duplicatas des

pages 1145 to / à 1147

Austria, Jamela

From: Austria, Jamela
Sent: Monday, November 19, 2012 5:01 PM
To: Matz, Mark; Anderson, Windy; Labelle, Sébastien; Hatfield, Adam
Cc: Willey, Chris; Carta, John; Weir, Sarah; Fortunato, Stephanie
Subject: FYI: ATI Release: A-2011-00318(3) - Anonymous Hacker group
Attachments: PS-SP-#723885-R-A-2011-00318(3).PDF.DRF

Hello,

For your information: please find attached an advance copy of ATI Release (2011-00318), which requested "All records relating to the online hacker group Anonymous. Timeline for request is between Nov 1, 2011, and Feb 10, 2012. Please exclude cabinet confidences. Please include any records originating from Communications Security Establishment Canada." The attached file will be released to the requester tomorrow.

We are currently reviewing it for any communications implications and will advise if media lines are needed, and if any media enquiries come in.

If there is anything in the attached that NCSD feels would require communications products, please feel free to contact Chris Willey or myself.

Thank you,

Jamela Austria
Senior Communications Advisor | Conseillière principale en communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-1675
Mobile | Cellulaire : [redacted] s.19(1)
Fax | Télécopieur : 613-954-0800
E-mail | Courriel: jamela.austria@ps-sp.gc.ca

From: Cormier, Louise
Sent: Wednesday, November 14, 2012 1:42 PM
To: * ATIP Notification / Notification AIPRP; Barake, Elias
Subject: A-2011-00318(3) - ADVANCE COPY - PS ATI Release / Avis de Divulgation Imminente - Demande AI de SP

Notification of ATI Release
Avis de Communication AI
Final release

Documents will be released on / Les documents seront divulgués le : November 20, 2012

Advance copy sent/posted on Share Point / Exemplaire prédivulgation expédié/téléchargé sur Share Point le: November 14, 2012

File # / No de dossier: A-2011-00318 / EB

Request text / texte de la demande : All records relating to the online hacker group Anonymous. Timeline for request is between Nov 1, 2011, and Feb 10, 2012. Please exclude cabinet confidences. Please include any records originating from Communications Security Establishment Canada.

Source : _X_ Media/Média ___Organization/Organisation ___ Public/Publique

Subject / Sujet: *Anonymous Hacker group*

Contact Person in Communications / Personne contacte aux communications :
Lisa Filipps (949-9741)

MAIN POINTS / POINTS IMPORTANTS: *(Bullet form summary of main issues included in release / Résumé des questions principales contenues dans la divulgation)*

- Records were received from: NS
- Final release subsequent to the September 21st interim release. Consultations completed with CSIS, CSEC, IC, CNSC, DFAIT and CBSA. RCMP was consulted but did not respond

Wilson, Barbara

From: Wilson, Barbara
Sent: Tuesday, November 20, 2012 8:30 AM
To: Picard, Josée
Subject: RE: Quick question re ATIP Summary report

Yes, that's fine.

Barbara Wilson
Senior Communications Advisor
Issues management and media relations
Conseillère principale en communications
Gestion des enjeux et relations avec les médias
Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue W/ 269, avenue Laurier ouest
Ottawa, (ON) K1P 0P8
(613) 944-4920
barbara.wilson@ps-sp.gc.ca

From: Picard, Josée
Sent: Monday, November 19, 2012 5:02 PM
To: Wilson, Barbara
Subject: Quick question re ATIP Summary report

Barb - do you think it`s fair to say we are currently consulting with NS policy on the ATI being released tomorrow re Anonymous Hacker Group. I haven`t heard back from Chris Willey and I don`t feel comfortable saying anything else, without knowing what`s being released. What do you think?

For your information, there is one ATI scheduled to be released on Tuesday, November 20:

Request Number	A-2011-00318
Request Text	**Subject: Anonymous Hacker group** All records relating to the online hacker group Anonymous. Timeline for request is between Nov 1, 2011, and Feb 10, 2012. Please exclude cabinet confidences. Please include any records originating from Communications Security Establishment Canada.
Comms Assessment	Currently consulting with NS Policy.

Josée Picard

Agente des communications | Communications Officer
Gestion des enjeux, Affaires publiques | Issues Management Team, Public Affairs Division
Ministère de la sécurité publique | Department of Public Safety
T : 613-993-1302 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Pages 726 to / à 727

are not relevant

sont non pertinentes

Slack, Jessica

From: Slack, Jessica
Sent: February-01-13 10:55 AM
To: 'Greg Cox'; Julie Gagnon
Cc: Wilson, Barbara
Subject: RE: FW: Question regarding Anonymous presence in Canada

Ok perfect.

From: Greg Cox [mailto:Greg.Cox@rcmp-grc.gc.ca]
Sent: February-01-13 10:55 AM
To: Slack, Jessica; Julie Gagnon
Cc: Wilson, Barbara
Subject: RE: FW: Question regarding Anonymous presence in Canada

You can advise him that you have forwarded his questions to me and I will respond to him via e-mail.

Greg

>>> "Slack, Jessica" <Jessica.Slack@ps-sp.gc.ca> 2/1/2013 10:52 AM >>>

That would be great..it's more than we could provide.
Thank you.

From: Greg Cox [mailto:Greg.Cox@rcmp-grc.gc.ca]
Sent: February-01-13 10:49 AM
To: Slack, Jessica; Julie Gagnon
Cc: Wilson, Barbara
Subject: RE: FW: Question regarding Anonymous presence in Canada

I assume you are referring to us saying that we would not confirm nor deny who or what may be the subject of an investigation?

>>> "Slack, Jessica" <Jessica.Slack@ps-sp.gc.ca> 2/1/2013 10:41 AM >>>

But I could refer him to you ? And you could provide your standard lines?

From: Greg Cox [mailto:Greg.Cox@rcmp-grc.gc.ca]
Sent: February-01-13 10:24 AM
To: Slack, Jessica; Julie Gagnon

Cc: Wilson, Barbara
Subject: Re: FW: Question regarding Anonymous presence in Canada

We would not answer those questions.

Greg

>>> "Slack, Jessica" <Jessica.Slack@ps-sp.gc.ca> 2/1/2013 10:13 AM >>>
Hi Julie and Greg -
Could we refer this your way?

-----Original Message-----
From:
Sent: January-31-13 8:25 PM
To: PS Media Relations / Relations médias SP s.19(1)
Subject: Question regarding Anonymous presence in Canada

Greetings,

My name is

I have been working on research about this group and cam across an article discussing growing concerns of Canadian entities being target by this group. I'm hoping that you may be the one to help better understand a question I have been trying to get clarification on.

Given your concerns and my nations ongoing issue with this group, where does this place Christopher Doyon (aka Commander X) the US fugitive hiding in your country and who for the most part operates as a global leader or figurehead for this group as well as helps maintain communications between members and sects through his LocalLeaks site(s)?

Is he also being sought by your law enforcement to, at the very least be extradited to the US? Has he found a non-extradition policy by which he can be shielded by?

Thank you,

Sent from my iPad

Slack, Jessica

From: Wilson, Barbara
Sent: February-01-13 10:13 AM
To: Slack, Jessica
Subject: RE: Question regarding Anonymous presence in Canada

Yes, I figured RCMP was the one.

Barbara Wilson
A/Manager
Issues management and media relations
Gestionnaire intérimaire
Gestion des enjeux et relations avec les médias Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue W/ 269, avenue Laurier ouest Ottawa, (ON) K1P 0P8
(613) 944-4920
barbara.wilson@ps-sp.gc.ca

-----Original Message-----
From: Slack, Jessica
Sent: Friday, February 01, 2013 10:12 AM
To: Wilson, Barbara
Subject: FW: Question regarding Anonymous presence in Canada

I am going to send this to the RCMP and DOJ to see if they have any input...

s.19(1)

-----Original Message-----
From: [redacted]
Sent: January-31-13 8:25 PM
To: PS Media Relations / Relations médias SP
Subject: Question regarding Anonymous presence in Canada

Greetings,

My name is [redacted]

I have been working on research about this group and cam across an article discussing growing concerns of Canadian entities being target by this group. I'm hoping that you may be the one to help better understand a question I have been trying to get clarification on.

Given your concerns and my nations ongoing issue with this group, where does this place Christopher Doyon (aka Commander X) the US fugitive hiding in your country and who for the most part operates as a global leader or figurehead for this group as well as helps maintain communications between members and sects through his LocalLeaks site(s)?

Is he also being sought by your law enforcement to, at the very least be extradited to the US? Has he found a non-extradition policy by which he can be shielded by?

Thank you,

s.19(1)

[redacted]

Sent from my iPad

Slack, Jessica

From: Slack, Jessica
Sent: February-01-13 10:39 AM
To: 'Saindon, Carole'
Cc: Wilson, Barbara; Girouard, Christian
Subject: RE: FW: Question regarding Anonymous presence in Canada

Thanks..I agree...

From: Saindon, Carole [mailto:Carole.Saindon@justice.gc.ca]
Sent: February-01-13 10:39 AM
To: Slack, Jessica
Cc: Wilson, Barbara; Girouard, Christian
Subject: RE: FW: Question regarding Anonymous presence in Canada

Hi Jessica: I think this is yet another inquiry that should have been addressed to law enforcement - not that they would reveal details of an investigation if one is in progress of course... Do you agree?

☺

From: Slack, Jessica [mailto:Jessica.Slack@ps-sp.gc.ca]
Sent: 2013-Feb-01 10:33 AM
To: Saindon, Carole
Cc: Wilson, Barbara
Subject: FW: FW: Question regarding Anonymous presence in Canada

Hi Carole- this individual has been in the news...
Is this something DOJ could respond to?

-----Original Message-----
From:
Sent: January-31-13 8:25 PM
To: PS Media Relations / Relations médias SP
Subject: Question regarding Anonymous presence in Canada

s.19(1)

Greetings,

My name is

I have been working on research about this group and cam across an article discussing growing concerns of Canadian entities being target by this group. I'm hoping that you may be the one to help better understand a question I have been trying to get clarification on.

Given your concerns and my nations ongoing issue with this group, where does this place Christopher Doyon (aka Commander X) the US fugitive hiding in your country and who for the most part operates as a global leader or figurehead for this group as well as helps maintain communications between members and sects through his LocalLeaks site(s)?

Is he also being sought by your law enforcement to, at the very least be extradited to the US? Has he found a non-extradition policy by which he can be shielded by?

Thank you,

[redacted] s.19(1)

Sent from my iPad

Wilson, Barbara

From: Slack, Jessica
Sent: Friday, February 01, 2013 10:42 AM
To: Greg Cox; Julie Gagnon
Cc: Wilson, Barbara
Subject: RE: FW: Question regarding Anonymous presence in Canada

But I could refer him to you ? And you could provide your standard lines?

From: Greg Cox [mailto:Greg.Cox@rcmp-grc.gc.ca]
Sent: February-01-13 10:24 AM
To: Slack, Jessica; Julie Gagnon
Cc: Wilson, Barbara
Subject: Re: FW: Question regarding Anonymous presence in Canada

We would not answer those questions.

Greg

>>> "Slack, Jessica" <Jessica.Slack@ps-sp.gc.ca> 2/1/2013 10:13 AM >>>
Hi Julie and Greg -
Could we refer this your way?

-----Original Message-----
From:
Sent: January-31-13 8:25 PM
To: PS Media Relations / Relations médias SP
Subject: Question regarding Anonymous presence in Canada

s.19(1)

Greetings,

My name is

I have been working on research about this group and cam across an article discussing growing concerns of Canadian entities being target by this group. I'm hoping that you may be the one to help better understand a question I have been trying to get clarification on.

Given your concerns and my nations ongoing issue with this group, where does this place Christopher Doyon (aka Commander X) the US fugitive hiding in your country and who for the most part operates as a global leader or figurehead for this group as well as helps maintain communications between members and sects through his LocalLeaks site(s)?

Is he also being sought by your law enforcement to, at the very least be extradited to the US? Has he found a non-extradition policy by which he can be shielded by?

Thank you,

Sent from my iPad

Wilson, Barbara

From: Duval, Jean Paul
Sent: Monday, February 25, 2013 2:07 PM
To: Swift, Andrew; Champoux, Martin
Cc: Wilson, Barbara; Slack, Jessica
Subject: FW: Media Call: STRATFOR Cyber Incident

Andrew, Martin

FYI - See timeline below.

-----Original Message-----
From: Beaudoin, Luc
Sent: Monday, February 25, 2013 2:01 PM
To: Anderson, Windy; Clow, Patrick; Duval, Jean Paul; Dick, Robert
Subject: RE: Media Call: STRATFOR Cyber Incident

CE11-2549 [Stratfor Hack affected Canadians] CCIRC received a report from law enforcement community about a hack of Stratfor by Anonymous. The information was initially posted on Pastebin.
STRATFOR's client list including emails, passwords, home/office addresses and credit card information were posted publically. This event is quite extensive as approximately 75,000 credit card numbers and 860,000 login credentials have been compromised.
Stratfor sent a notification email to all its clients. FOR THIS REASON, mitigation was already taking place according to best practices and responsible disclosure. CCIRC can only notify potential victims in such case. This was done already.

Timeline:
25 Dec, 21h22: GOC email sent to CCIRC about media reporting (Associated press) of Stratfor user database being hacked by Anonymous. Cyberdo not paged.
26 Dec, 22h22: initial list of potential victims obtained by CCIRC
27 Dec, 00h07: CE11-2549 Opened to track. Confirmation of reception sent.
27 Dec, 13h30: Notified Federal CERT that some gc.ca emails were involved.
27 Dec to 4 Jan: various datasets of the breach were obtained and reported to CCIRC primarily from RCMP. Parsing of the data and analysis.
5 Jan: Notification sent to provinces.

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

-----Original Message-----
From: Anderson, Windy
Sent: Monday, February 25, 2013 1:05 PM
To: Beaudoin, Luc; Clow, Patrick
Subject: Fw: Media Call: STRATFOR Cyber Incident

Pat - get Luc involved. He has the "real facts". Last time he was brought in too late.

Windy

From: Duval, Jean Paul
Sent: Monday, February 25, 2013 01:03 PM
To: Dick, Robert; Matz, Mark; Anderson, Windy
Cc: Hatfield, Adam; Wilson, Barbara; Slack, Jessica; Clow, Patrick
Subject: Media Call: STRATFOR Cyber Incident

Robert, Mark, Windy,

FYI – We have received a media call relating to a STRATFOR cyber incident. I will get back to you soon with some proposed messaging.

Glad to discuss at your convenience.

Thanks,
JP

Jean Paul Duval

Communications Directorate | Direction générale des communications

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone : 613-991-1689

Cell | Portable: [redacted] s.19(1)
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

From:
Sent: Monday, February 25, 2013 12:22:00 PM (UTC-05:00) Eastern Time (US & Canada)
To: andrew.macdougall@pmo.gc.ca; PS Media Relations / Relations médias SP
Cc:
Subject: URGENT

CBC is preparing to air a story tonite for The National reporting that on Dec. 24, 2011, 880 federal government workers and 109 provincial government users in nine provinces had their credit card information, passwords, security codes and other sensitive personal and government info stolen by hackers during an attack on the US intelligence firm Stratfor.

We have a list of federal departments affected and are contacting them individually.

We are quoting extensively from a memo to the then deputy minister of Public Safety from the then sr. ADM Lynda Clairmont dated Jan 12, 2012.

We also have documents showing the Cyber Incident Response Centre did not respond to the impact of the attack on so many federal public servants and depts until three days after the fact because it was closed for the Christmas holiday.

We would like to talk to someone about this incident and what the ramifications have been for depts and public servants affected.

We would also like some comment from a minister.

Our deadline is 3pm. TODAY.

Thanks for your help.

cheers,

s.19(1)

CBC National News

(Twitter) @

(Private)

Slack, Jessica

From: Duval, Jean Paul
Sent: February-25-13 3:03 PM
To: Swift, Andrew
Cc: Wilson, Barbara; Slack, Jessica
Subject: FW: Info on Stratfor

Andrew,

FYI - This email below was sent from Mark to Lynda (w/CC to Stéphanie).

From: Matz, Mark
Sent: Monday, February 25, 2013 2:57 PM
To: Clairmont, Lynda
Cc: Gordon, Robert; Dick, Robert; Durand, Stéphanie; Duval, Jean Paul; Clow, Patrick; Gélinas, Emilie
Subject: Info on Stratfor

We are also looking through ATIP to see what may have triggered the current story's premise as to timeline. As the timeline below notes, CCIRC was informed by the RCMP on Dec 26, 22:22, and opened an incident file within two hours.
– mark

Stratfor Hack affected Canadians: CCIRC received a report from RCMP about a hack of Stratfor by Anonymous. The information was initially posted on Pastebin.

STRATFOR's client list including emails, passwords, home/office addresses and credit card information were posted publically. This event is quite extensive as approximately 75,000 credit card numbers and 860,000 login credentials have been compromised.

Stratfor sent a notification email to all its clients. FOR THIS REASON, mitigation was already taking place according to best practices and responsible disclosure. CCIRC can only notify potential victims in such case. This was done already.

Of note:
- This attack was not on federal and provincial systems. It was on a private company.
- This attack happened on a foreign private sectors systems, which is not within CCIRC's mandate.
- The impact to federal and provincial public servant was limited to their email addresses and password for this external website. The passwords were reset early by Stratfor. A limited number of the 860 000 victims had their credit card numbers stolen and were promptly notified accordingly by the victimized company.
- Federal public servant email addresses are for the most part publicly available
- The risk to critical infrastructures and vital systems of Canada was assessed to VERY LOW, therefore CCIRC only performed due diligence by pointing out the event to its federal and provincial affected partners.
- No additional mitigation was required as all victims were informed promptly by Stratfor accordingly.

Timeline:
25 Dec, 21h22: GOC email sent to CCIRC about media reporting (Associated press) of Stratfor user database being hacked by Anonymous. Cyber duty officer not paged.
26 Dec, 22h22: RCMP sends initial list of potential victims to CCIRC

27 Dec, 00h07: An incident report is opened by CCIRC for tracking and handling (CE11-2549).
27 Dec, 13h30: Notified Federal CERT (CSEC) that some gc.ca emails were involved.
27 Dec to 4 Jan: Various datasets of the breach were obtained and reported to CCIRC, primarily from RCMP. Parsing of the data and analysis.
5 Jan: Notification sent to provinces.

Messaging on changes to CCIRC since December 2011:
- $13 million over 5 years in new funding to bring CCIRC to 30 personnel available, including 15/7 onsite operations and 24/7 emergency access.
- New Industrial Control System laboratory.
- A new virus lab: Advanced Malware Analysis Capabilities with new computer and human resources.
- PS-DHS Cyber Security Action Plan enabling closer CCIRC/US-CERT collaboration.
- Embedding CCIRC personnel in the Government Cyber Threat Evaluation Centre at CSEC.
- CCIRC and other Public Safety cyber resources brought under a single management structure to ensure clear focus on cyber security issues from policy through to operational matters.

Mark Matz
Director, Policy and Issues Management /
Directeur, Politiques cyber et gestion des enjeux
NATIONAL CYBER SECURITY / CYBERSÉCURITÉ NATIONALE
613-993-9635

Duval, Jean Paul

From: Duval, Jean Paul
Sent: Monday, February 25, 2013 5:11 PM
To: Matz, Mark; Clairmont, Lynda
Cc: Gordon, Robert; Dick, Robert; Clow, Patrick; Gélinas, Emilie
Subject: RE: Info on Stratfor

s.19(1)

Good evening Lynda, Mark,

FYI - PS media relations has confirmed receipt of the STRATFOR response with [redacted] noted that [redacted] piece may or may not air tonight, but indicated [redacted] would give us a heads-up if/when it would air on another day.

Thank you all for your assistance on this file.

Kind regards,
JP

From: Matz, Mark
Sent: Monday, February 25, 2013 2:57 PM
To: Clairmont, Lynda
Cc: Gordon, Robert; Dick, Robert; Durand, Stéphanie; Duval, Jean Paul; Clow, Patrick; Gélinas, Emilie
Subject: Info on Stratfor

We are also looking through ATIP to see what may have triggered the current story's premise as to timeline. As the timeline below notes, CCIRC was informed by the RCMP on Dec 26, 22:22, and opened an incident file within two hours.
– mark

Stratfor Hack affected Canadians: CCIRC received a report from RCMP about a hack of Stratfor by Anonymous. The information was initially posted on Pastebin.

STRATFOR's client list including emails, passwords, home/office addresses and credit card information were posted publically. This event is quite extensive as approximately 75,000 credit card numbers and 860,000 login credentials have been compromised.

Stratfor sent a notification email to all its clients. FOR THIS REASON, mitigation was already taking place according to best practices and responsible disclosure. CCIRC can only notify potential victims in such case. This was done already.

Of note:
- This attack was not on federal and provincial systems. It was on a private company.
- This attack happened on a foreign private sectors systems, which is not within CCIRC's mandate.
- The impact to federal and provincial public servant was limited to their email addresses and password for this external website. The passwords were reset early by Stratfor. A limited number of the 860 000 victims had their credit card numbers stolen and were promptly notified accordingly by the victimized company.
- Federal public servant email addresses are for the most part publicly available
- The risk to critical infrastructures and vital systems of Canada was assessed to VERY LOW, therefore CCIRC only performed due diligence by pointing out the event to its federal and provincial affected partners.
- No additional mitigation was required as all victims were informed promptly by Stratfor accordingly.

Timeline:
25 Dec, 21h22: GOC email sent to CCIRC about media reporting (Associated press) of Stratfor user database being hacked by Anonymous. Cyber duty officer not paged.
26 Dec, 22h22: RCMP sends initial list of potential victims to CCIRC
27 Dec, 00h07: An incident report is opened by CCIRC for tracking and handling (CE11-2549).
27 Dec, 13h30: Notified Federal CERT (CSEC) that some gc.ca emails were involved.
27 Dec to 4 Jan: Various datasets of the breach were obtained and reported to CCIRC, primarily from RCMP. Parsing of the data and analysis.
5 Jan: Notification sent to provinces.

Messaging on changes to CCIRC since December 2011:
- $13 million over 5 years in new funding to bring CCIRC to 30 personnel available, including 15/7 onsite operations and 24/7 emergency access.
- New Industrial Control System laboratory.
- A new virus lab: Advanced Malware Analysis Capabilities with new computer and human resources.
- PS-DHS Cyber Security Action Plan enabling closer CCIRC/US-CERT collaboration.
- Embedding CCIRC personnel in the Government Cyber Threat Evaluation Centre at CSEC.
- CCIRC and other Public Safety cyber resources brought under a single management structure to ensure clear focus on cyber security issues from policy through to operational matters.

Mark Matz
Director, Policy and Issues Management /
Directeur, Politiques cyber et gestion des enjeux
NATIONAL CYBER SECURITY / CYBERSÉCURITÉ NATIONALE
613-993-9635

Pages 743 to / à 745

are not relevant

sont non pertinentes

Champoux, Martin

From: Champoux, Martin
Sent: Monday, April 08, 2013 12:15 PM
To: Anderson, Windy
Cc: Swift, Andrew; Hatfield, Adam
Subject: RE: CYBER NOTIFICATION-13-007 –LOW IMPACT SEVERITY – MEDIA INTEREST - Anonymous - OpIsrael Websites

Thanks Windy, I was just checking. I appreciate the amount and care and considerations that needs to go into this. We will hold off on any distribution.

Have a great week.

Martin

From: Anderson, Windy
Sent: Monday, April 08, 2013 10:21 AM
To: Champoux, Martin
Cc: Swift, Andrew; Hatfield, Adam
Subject: RE: CYBER NOTIFICATION-13-007 –LOW IMPACT SEVERITY – MEDIA INTEREST - Anonymous - OpIsrael Websites

Martin,

We are still working through the Standard Operating Procedure for this product. PS met with the DG's (DG Ops – CSIS, RCMP, DND, CSEC, PS) last Friday to seek agreement from all of these departments (plus SSC when they take over some duties from CSEC) to have PS "write" a Standard Operating Procedure for all departments to follow regarding this product. They did all agree that this type of product was extremely useful and they all wanted a copy of it every time it comes out. And, they all "in principal" agreed to follow the SOP and possibly even write some CNT's themselves.

The next step is for Adam (and I) to call a Director's meeting with all the same players (departments) to go over the actual details of when these are produced, **who** can see them, what are the escalation procedures, etc. etc. Although CCIRC has completed most of that work already (as we had to internally to PS), it has not been seen, much less agreed to, by the other departments. If I am not mistaken, Adam should be calling that meeting sometime this week or next.

I understand you would love to send this forward but I would ask that you please wait until we go through the process and get the rules and regulations agreed to by all parties. I hope it will not take too long. Once a decision is made, I will inform you what can and cannot be released and under what conditions.

I would not be doing my job properly if I didn't take extra care on how some of our more sensitive CNT's are handled. It would be extremely harmful to CCIRC's reputation if some of the more sensitive information that we put in these documents gets out. We would actually lose credibility with our clients as we promise not to release anything proprietary about a company/victim in the public domain and if someone accidently did that, it would be my organization and PS at large that would suffer.

Thanks for your patience and if you have any other questions/concerns, please let me know.

Have a great day,

Windy
Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Champoux, Martin
Sent: April-08-13 9:48 AM
To: Anderson, Windy
Cc: Swift, Andrew
Subject: Fw: CYBER NOTIFICATION-13-007 –LOW IMPACT SEVERITY – MEDIA INTEREST - Anonymous - OpIsrael Websites

Windy

Further to our conversation a couple weeks ago is this one of the CNTs I can share with a select number of partners in the federal Comms community (RCMP, CSEC, IC, CSIS)?

Martin.

From: CCIRC-CCRIC
Sent: Sunday, April 07, 2013 08:52 AM
To: Clairmont, Lynda; Dick, Robert; Gordon, Robert; Jarmyn, Tom; Johnson, Mark; Mueller, Mike; 'Tony.Pickett@rcmp-grc.gc.ca' <Tony.Pickett@rcmp-grc.gc.ca>; [redacted]@CSE-CST.GC.CA' <[redacted]@CSE-CST.GC.CA>; 'ROBERT.MAZZOLIN@forces.gc.ca' <ROBERT.MAZZOLIN@forces.gc.ca>; 'cnoir@pco-bcp.gc.ca' <cnoir@pco-bcp.gc.ca>; 'bdiogo@pco-bcp.gc.ca' <bdiogo@pco-bcp.gc.ca>; 'Eric.Belzile@ssc-spc.gc.ca' <Eric.Belzile@ssc-spc.gc.ca>; Durand, Stéphanie; MacDonald, Michael; Wong, Suki
Cc: Anderson, Windy; Hatfield, Adam; Matz, Mark; Campbell, Tom; Duschner, Gabrielle; Paquet, Alain; Swift, Andrew; DeJong, Michael; Bendelier, Kenneth; Clow, Patrick; Beaudoin, Luc; Klassen, Nathan; Proulx, Véronique; Pacha, Tomasz; Fortunato, Stephanie; Champoux, Martin; Hunt, Ryan; CYBERDO; GOC-COG
Subject: CYBER NOTIFICATION-13-007 –LOW IMPACT SEVERITY – MEDIA INTEREST - Anonymous - OpIsrael Websites

CYBER NOTIFICATION – INCIDENT

Incident Number: CNT-13-007 – VERY LOW IMPACT SEVERITY – MEDIA INTEREST

Description of Incident: CCIRC is aware of media coverage on cyber attacks by the group Anonymous on Israeli web sites. No significant impact is reported. CCIRC remains vigilant and has reached out to Israeli CERT to offer assistance if needed.

Sources of reporting: Open Media Sources

Current actions: CCIRC has reached out to the Israeli CERT and shared its related mitigation product.

Initial analysis / assessment:

There is no reported Canadian Impact.

Disclaimer:

This notification is only for distribution within the Government of Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Chris Briffett
Approved by: Windy Anderson

Champoux, Martin

From: Champoux, Martin
Sent: Tuesday, April 10, 2012 10:07 AM
To: Dick, Robert; Hatfield, Adam; Anderson, Windy
Subject: FW: The Hill Times: House Affairs likely to end probe of Anonymous threats against Toews, opposition MPs say study's going nowhere

FYI – in case you have not seen this already

Bob got this when it was initially sent out

House Affairs likely to end probe of Anonymous threats against Toews, opposition MPs say study's going nowhere
April 9, 2012, 00:00 ET
The Hill Times, By: Laura Ryckewaert

The Procedure and House Affairs Committee, which is investigating threats against **Public Safety Minister Vic Toews** by hacker group Anonymous, will likely wrap up its probe once the House returns in two weeks.

Conservative MP Joe Preston (Elgin-Middlesex-London, Ont.), chair of the House Affairs Committee, told The Hill Times that when MPs return from the two-week break on April 23, the committee will likely look at an interim report on its study thus far, but said he personally thinks the investigation is nearing its end.

Leading experts were called to shed light about the online hacker group Anonymous and threats against the Cabinet minister, but the experts had little insights to share into who's behind Anonymous because it's anonymous.

On Feb. 17—three days after **Public Safety Minister Toews** (Provencher, Man.) tabled Bill C-30, the Protecting Children from Internet Predators Act, in the House and responded to an opposition critique by saying that those against the bill were "with the child pornographers"—a video was posted on YouTube by "hacktivist" group Anonymous, demanding that **Mr. Toews** resign from his position and scrap Bill C-30 and threatening to expose further details of **Mr. Toews'** personal life as part of "operation white north" if he didn't comply.

In the meantime, shortly after **Mr. Toews** made the provocative "child pornographers" remark, messy details began to be tweeted about **Mr. Toews'** divorce under the Twitter handle @Vikileaks which attracted national attention. The Liberals discovered that one of their own, Liberal staffer Adam Carroll, was responsible for the account and was fired. The Twitter account was killed.

Mr. Toews' Bill C-30 also inspired more social media action on Twitter when tweeps tweeted under the hash tag, #TellVicEverything.

House Speaker Andrew Scheer (Regina-Qu'Appelle, Sask.) ruled on March 6 that the Anonymous video constituted a "direct threat" against the minister and ruled it to be a breach of **Mr. Toews'** privileges as an elected official.

On April 3, the committee heard testimony from Toni Moffa, deputy chief of IT security with the Communications Security Establishment Canada; Scott Jones, director general of cyber defence at CSE; Robert Gordon, special adviser in cyber security at the Canadian Cyber Incident Response Centre in the Department of **Public Safety and Emergency Preparedness**; James Malizia, assistant commissioner in the protective policing branch of the RCMP; and Tony Pickett, the officer in charge of the RCMP's technological crime branch.

Ms. Moffa told the 12-member committee that Communications Security Establishment Canada's role is to provide advice to protect internet systems, working with federal partners like the Treasury Board Secretariat, CSIS, the RCMP and **Public Safety Canada** to "diminish the threat to federal systems," and advise such federal partners in relevant investigations. Ms. Moffa said there is a system monitoring IT threats in government and said when incidents occur, they're shared across the government, including the Parliamentary precinct, in order to prevent it in the future.

However, Ms. Moffa told the committee, from the Communications Security Establishment Canada's perspective, the matter before them isn't a case of an IT breach, and, following further prompting by the committee, said she didn't see any security threat.

Ms. Moffa said it's part of CSE's mandate to help federal partners upon request, but said CSE looks at threats that "are not publicly known," and that are "derived from classified information."

Mr. Gordon, from the **Public Safety Department**, said information sharing is an essential part of what the department does and said they act as a national coordination centre for monitoring threats from outside government. But he told the committee that the department is not an investigative body, but instead works towards prevention and preparation against cyber threats.

RCMP officials had even less to say at the meeting. The RCMP confirmed at the committee that it is investigating the activities of Anonymous and threats against **Mr. Toews**, and as a result, couldn't answer the majority of questions posed by committee members.

The international network of protesters objects to the federal government's controversial online surveillance bill introduced by **Mr. Toews**.

Mr. Malizia told the committee that all members, if they feel threatened, can report incidents to the RCMP who "may initiate an investigation," on a case-by-case basis. Mr. Malizia said cyber crime is growing around the globe and is challenging to monitor.

With regard to the group Anonymous, Mr. Malizia said the hackers group is best described as a movement with undefined memberships and said few are criminals but sometimes their actions violate laws.

Perhaps the most intriguing moment of the meeting was when NDP MP Philip Toone (Gaspésie-Îles-de-la-Madeleine, Que.) stated it was his understanding—and the witnesses didn't contradict him—that the YouTube video threatening **Mr. Toews** was posted by someone outside Canada.

Committee members were up front with the witnesses about the fact that they were still struggling to shape their investigation and asked questions with a range of relevancy to the threats against **Mr. Toews**.

Conservative MP Bob Zimmer (Prince George-Peace River, B.C.) asked how Canadians in general could protect themselves from "this" kind of IT threat, and Conservative MP Laurie Hawn (Edmonton Centre, Alta.) also asked for internet security tips.

Ms. Moffa, and later Mr. Gordon, directed the committee to the public safety website for tips on how to better protect themselves from hacking and other IT threats.

In a checklist familiar to any secondary school student who uses the internet in class, Ms. Moffa said it's important to ensure passwords are difficult and secure, and told committee members that software is constantly being updated with patches and that swiftly patching the system is a good way of preventing risks. Mr. Gordon said it's important to think before you click, and warned the committee against opening unfamiliar or unexpected attachments and emails.

Mr. Hawn also asked about hacking techniques that could be used and asked what sort of IT threat data sticks can pose.

Ms. Moffa said as another way to access your computer, using a data stick increases risks.

NDP MP Joe Comartin (Windsor-Tecumseh, Ont.) caused the witnesses to stumble when he asked what agency would have the expertise to track down the poster of a YouTube video. Eventually, Mr. Pickett said the RCMP, the CSE and similar federal partners share information and that the expertise doesn't lie in one particular area and collaboration would be sought.

Mr. Malizia said as each investigation is unique, whether or not the RCMP can trace an IP address is on a case-by-case basis, but said "sometimes, we can't."

NDP MP Alexandrine Latendresse (Louis-Saint-Laurent, Que.) asked if there was anything the committee could do. Mr. Gordon said raising awareness about IT security threats and the issue at large is a useful exercise.

Mr. Hawn asked if the witnesses thought the committee's study was shedding "helpful light" on the situation. Mr. Malizia said he was not in a position to comment.

This is the third meeting the Procedure and House Affairs Committee has held to study Anonymous threats. The committee first met on March 15 to hear testimony from House Clerk Audrey O'Brien, Sergeant-at-arms Kevin Vickers and House Chief Information Officer Louis Bard, updating them on the state of Parliament's internet security systems. At the meeting, the committee was told internet security systems are already regularly updated.

On March 27, the committee met to study the breach of privilege for a second time and heard testimony from **Public Safety Minister Toews**. **Mr. Toews** told the committee he thinks all Canadians of all political backgrounds should be concerned by "these types of threats posed to our democracy" by online "thugs," and said Parliament owes it to the future generation of politicians to look at what can be done to protect them.

Mr. Toews was repeatedly asked what remedies he hoped would result from the committee's investigation.

Mr. Toews said it wasn't up to him to propose remedies but suggested they speak with security enforcement agencies to get their advice.

"***If they say there's nothing that can be done then perhaps we have our answer***," **said Mr. Toews**.

Committee chair Mr. Preston said even though witnesses were unable to answer many of the questions posed by the committee, it was important that those questions were at least asked.

"I'm thinking we're coming to an end," said Mr. Preston.

Ms. Latendresse said she doesn't think the committee is going anywhere with its study.

"It's very interesting to have all this information about the security of the internet...but it's just, the case here is that someone posted a YouTube video and that's all. And that's what we have to look at. There was no hacking, there was no breach of our internet security, so we don't see where it is going right now," said Mr. Latendresse.

Going forward, Ms. Latendresse said she doesn't see another angle with which to approach the study.

"We'll see what the other parties will recommend, if there's other witnesses they want. But in our point of view we've done all we could," said Ms. Latendresse.

Mr. Zimmer said he thinks it's been a "pretty comprehensive" study already and said with the RCMP investigating the threats, he thinks it should be left to "take its course, and hopefully they can found out whoever is making the threat."

Mr. Preston said committee analysts will be preparing the evidence heard thus far over Parliament's two-week break and when MPs return the committee will review what's already been heard.

"It will certainly be up to the committee...I think we've heard the list of witnesses. I think sometimes once you kind of prepare an interim report, then that in your mind makes you think, 'Hey, wait, maybe we should see so and so,' so I'm not suggesting we're finished, but I think we're nearing it," said Mr. Preston.

Meanwhile, Bill C-30 is at first reading the Commons.

Link

Slack, Jessica

From: Greg Cox <Greg.Cox@rcmp-grc.gc.ca>
Sent: April-10-13 3:27 PM
To: Miller, Kevin; Julie Gagnon
Cc: Swift, Andrew; Wilson, Barbara; Duval, Jean Paul; Slack, Jessica
Subject: FYI - Open Letter Re: Rehteah Parsons Case (RCMP Mentioned)

Thank you Kevin.

Greg

>>> "Miller, Kevin" <Kevin.Miller@ps-sp.gc.ca> 4/10/2013 2:19 PM >>>
Julie, Greg,

Just a heads up, in case you haven't seen it, the following open letter was posted on Warren Kinsella's website addressed to Anonymous re: the Rehteah Parsons case (An RCMP member's name is mentioned):

Dear Anonymous:

I have never written to you, the global hacktivist group, before. Like everyone else, I have read about your exploits and, more than once, nodded my head with approval. It's comforting to see citizens periodically bring certain groups to heel, like child pornographers or the Church of Scientology.

I am writing to you today about something else, however.

In Cole Harbour, Nova Scotia, a girl named Rehtaeh Parsons killed herself last week. She was 17 years old. That's her, up above.

Her name was Heather spelled backwards. Rehtaeh was a straight-A student, she was much-loved by her family and others. She was a good kid.

In November 2011, when she was 15 years old – just a *child* – she was raped by four males in a basement. One of them photographed her being raped, and then circulated it to many others. They thought it was funny.

Rehtaeh was thereafter harassed and abused and bullied by students at her school. The torment got bad enough that Rehtaeh had to move to another town. Months later, she returned, but the bullying and abuse never stopped. She was sent messages calling her a "slut."

You may ask what happened to the four males who raped her, and who circulated the photograph of Rehtaeh being raped – which, incidentally, meets the definition in Canadian law of child pornography.

Nothing. *Nothing* happened to them.

The RCMP, who allegedly investigated, are led in Nova Scotia by Alphonse MacNeil. He calls himself a "consensus builder" and has two daughters. I'm sure you could find his email address if you needed to.

The Nova Scotia government, which agreed with – and energetically defended – the RCMP's decision to do nothing about the rape or the child pornography, is led by NDP leader Darrell Dexter. Interestingly, he represents Cole Harbour in the provincial legislature. His email isn't readily available, either, but I know you'll find that, too.

His Attorney-General is Ross Landry. Yesterday, Landry refused to reopen the case; by the afternoon, he had seemingly changed his tune. His constituency office email is here. I don't know what his email is.

The names of the little bastards who did this, and who are still alive and walk free in Cole Harbour, are unknown to most of us. But, as in the Steubenville, Ohio case, I am certain anyone who is sufficiently motivated can find out who the little bastards are, and name and shame them.

I'm unclear how to appeal to you, Anonymous. But if there was ever a case that cried out for your attention – and if there were ever men like MacNeil, Dexter and Landry who deserved to be fired, or worse, for their pathetic responses – I don't know what it is. What happened to Rehtaeh and her family is so horrible, so evil, I am ashamed that it happened in my country.

In closing, I should note that Rehtaeh's heart was sent to Toronto yesterday, to be transplanted into another person. I don't know why I feel a need to mention that to you, but I do.

Maybe because, in some way, it feels like Rehtaeh is still watching now, to see who will do something, and who will do nothing.

Sincerely,

Warren

The link to the site is as follows: http://warrenkinsella.com/2013/04/an-open-letter-to-anonymous-about-rehtaeh-parsons/

Thanks,
K

Kevin K. Miller
Communications Manager | Gestionnaire de Communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-9741
Fax | Télécopieur : 613-954-6048
Email | Courriel : Kevin.Miller@ps-sp.gc.ca

Miller, Kevin

From: Miller, Kevin
Sent: Thursday, April 11, 2013 11:40 AM
To: greg.cox@rcmp-grc.gc.ca; Julie Gagnon (julie.gagnon@rcmp-grc.gc.ca) (julie.gagnon@rcmp-grc.gc.ca)
Cc: Wilson, Barbara; Swift, Andrew
Subject: FW: Peaceful protest at Halifax RCMP headquarters - Re: Rehteah Parsons

Categories: Green Category

Hi Julie, Greg,

FYI – Please see below.

K

From: Mehes, Sabrina
Sent: Thursday, April 11, 2013 11:39 AM
To: * Media Monitoring / Suivi des médias
Cc: PSPMediaCentre/CentredesmediasPSP
Subject: Peaceful protest at Halifax RCMP headquarters - Re: Rehteah Parsons

FYI - Metro News is reporting that the hacker group Anonymous will be holding a peaceful protest at the Halifax RCMP headquarters at 2 p.m. this Sunday outside 1975 Gottingen St.

Sabrina

Anonymous protest at Halifax RCMP headquarters will demand justice for Rehtaeh Parsons

Metro News - Philip Croucher
April 11, 2013

The hacker group Anonymous says it will be holding a peaceful demonstration in front of Halifax police location on Gottingen Street this weekend to demand justice for Rehteah Parsons.

The release says the protest will take place starting at 2 p.m. this Sunday outside 1975 Gottingen St. – the home to the headquarters of the Halifax RCMP and Halifax Regional Police.

The group says it's demanding two things from the protest: that the RCMP continue to investigate the alleged rape of Parsons, who took her life last week after two years of relentless bullying, and that Justice Minister Ross Landry will launch an investigation into the case that was dismissed from the police. "

Anonymous is continuing to gather information about the circumstances surrounding Rehtaeh's death," the release states. "We are determined to find justice for Rehtaeh.

" The group has already claimed to have identified four of the alleged assailants are threatening to go public with their names.

Sunday's protest isn't the only public gathering since the Parsons' suicide story went public this week.

On Thursday at 7 p.m., a community vigil is taking place at Victoria Park in Halifax.

Metro News

Swift, Andrew

From: Swift, Andrew
Sent: Thursday, April 11, 2013 4:29 PM
To: Carmichael, Julie; Johnson, Mark; Mueller, Mike; McGrath, Andrew
Cc: Durand, Stéphanie; Tomlinson, Jamie; Wilson, Barbara; Miller, Kevin; Slack, Jessica
Subject: HEADS UP: Halifax Police & RCMP statement on the investigation into Rehtaeh Parsons

Importance: High

Categories: ATI PRINT

Julie,

See heads up below from RCMP on a joint statement they are releasing with Halifax Regional Police on Rehtaeh Parsons. We will monitor.

Andrew

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Marc Richer [mailto:Marc.Richer@rcmp-grc.gc.ca]
Sent: Thursday, April 11, 2013 3:53 PM
To: Swift, Andrew; Wilson, Barbara; Slack, Jessica; Durand, Stéphanie
Cc: Miller, Kevin; Lavoie, Daniel; Derek Cefaloni; Greg Cox; Joe De Mora; Julie Gagnon
Subject: Fwd: final statement- Parsons
Importance: High

This is being issued in Nova Scotia.

The Halifax Police Chief and Supt Wells of the RCMP, will respond to requests from media.

Marc

Marc Richer, Supt/Sdt.
Acting Director General | Directeur Général intérimaire
National Communication Services | Services nationaux de communication
Royal Canadian Mounted Police |Gendarmerie Royale du Canada
73 promenade Leikin Drive
Ottawa, ON K1A 0R2
Tel: 613 843 4561
Cell: [redacted] **s.19(1)**

marc.richer@rcmp-grc.gc.ca
FINAL

Partners in Policing Release - Parsons Investigation

2013-04-11

Prepared by: Lia Scanlan, Paula Sibley-Fox, Lauren Leal

Approved by: Chief Blais/ Supt. Wells

Joint Statement from HRP/ RCMP on Rehtaeh Parsons investigation

Earlier this afternoon, Halifax Regional Police Chief Jean-Michel Blais and Halifax District RCMP Superintendent Roland Wells met with Leah Parsons, the mother of Rehtaeh Parsons. Both officers expressed their sincere condolences at this terrible tragedy and offered their continued support on behalf of both police agencies. The family has asked police to convey their wish for their privacy to be respected by both the media and the public during the days leading up to and including Rehtaeh's funeral. Out of respect for Ms. Parsons and her family, the remaining details of this meeting will not be shared. This is a devastating tragedy that impacts the community as a whole and we are all saddened by Rehtaeh's passing.

HRP and RCMP would like to advise the public of the investigative structure involved in sexual assault investigations. The investigation into this sexual assault complaint was led by a Halifax Regional Police officer assigned to the Integrated Sexual Assault Investigation Team, a unit comprised of both HRP and RCMP officers who have a wide range of experience and specialized training. The team is responsible for investigating complaints of sexual assault including those involving children under the authority of the Children and Family Services Act. Sexual assault investigations are complex and require significant time to gather evidence and to interview all parties involved. Because the incident occurred in RCMP jurisdiction an RCMP spokesperson will continue to handle all media inquiries.

We continue to ask people with specific information about this incident to report to police or Crime Stoppers. Though police reports cannot be accepted through social media, tips can be reported anonymously to Crime Stoppers by calling toll-free 1-800-222-TIPS (8477), submitting a secure web tip at www.crimestoppers.ns.ca or texting a tip - Tip 202 + your message to 274637.

Police are continuing to face the challenge of the wide circulation of misinformation within the public forum. This has led to some suggestions of vigilante action against individuals alleged to be involved in this case, which we cannot condone. We discourage anyone from taking the law into their own hands, or in any way encouraging vigilante justice. The information being used is unverified or may lead to an assumption of guilt towards people that may not actually be involved. Only a police investigation in which evidence is collected and verified can lead to such conclusions.

We understand there are a number of pages and comments on social networking sites that are targeting Rehtaeh's memory and people related to this incident. A number of these pages and comments have been shut down or deleted by various Social Media Networking sites. Police want to make clear that making a threat or allegation against someone's life is a criminal offence. Given the volume of potential sites that may exist, police become involved if there are threats or evidence of a criminal nature.

Anyone who uses a Social Networking site can report pages that are breaking the acceptable use policies of those sites directly to the site providers. Social media sites like Twitter or Facebook have community standards and Terms of Use policies that clearly outline what is acceptable behaviour and content. It is a community responsibility to ensure we collectively do not tolerate, perpetuate or condone this.

We also remind citizens that there are resources available. If you or someone you know are having suicidal thoughts, please call the toll-free Kid's Help Line at 1-800-668-6868 or the toll-free Suicide Prevention Line at 1-888-429-8167. Also please check out http://www.suicideprevention.ca and the list of warning signs at http://www.suicideprevention.ca/about-suicide/warning-signs/.

Signed by:

Halifax Regional Police Chief Jean-Michel Blais

Halifax District RCMP Superintendent Roland Wells

-30-

Contact person:

Cpl. Scott MacRae
Media Relations
Halifax District RCMP
Cell: [redacted] s.19(1)
scott.macrae@rcmp-grc.gc.ca

Swift, Andrew

From: COMDO
Sent: Thursday, April 11, 2013 7:37 PM
To: Swift, Andrew; Miller, Kevin; De Curtis, Laura
Subject: Tweet re. Anonymous Interview on Friday

Categories: ATI PRINT

FYI – Please advise if you'd like me to order a transcript from H&K.

YourAnonNews 7:10pm via GroupTweet
One of our correspondents will be on @TheCurrentCBC tomorrow morning w/ a member of the #RCMP to discuss #OpJustice4Rehtaeh.

Wilson, Barbara

From: Slack, Jessica
Sent: Friday, April 12, 2013 1:34 PM
To: Carmichael, Julie; Mueller, Mike; McGrath, Andrew; Johnson, Mark
Cc: Swift, Andrew; Durand, Stéphanie; Miller, Kevin
Subject: FW: Commr Paulson scrum in Alberta

Julie-RCMP just flagged scrum of Commissioner Paulson. See below.
We will watch for coverage.
Jessica

From: Marc Richer [mailto:Marc.Richer@rcmp-grc.gc.ca]
Sent: April-12-13 1:30 PM
To: Swift, Andrew; Wilson, Barbara; Slack, Jessica; Durand, Stéphanie
Cc: Lavoie, Daniel; Derek Cefaloni; Greg Cox; Joe De Mora; Julie Gagnon
Subject: Commr Paulson scrum in Alberta

on Reateh Parsons:

Joint effort lead by Halifax Police Service
Analysis of info complex
Asked about RCMP willingness to work with Anonymous
Said rcmp will work with anyone but Anonymous isn't held to same standard of truth
We will work with them if they take the mask off

Marc

Slack, Jessica

From: Swift, Andrew
Sent: April-12-13 1:49 PM
To: 'Marc Richer'; Wilson, Barbara; Slack, Jessica; Durand, Stéphanie
Cc: Lavoie, Daniel; Derek Cefaloni; Greg Cox; Joe De Mora; Julie Gagnon
Subject: RE: Commr Paulson scrum in Alberta

Merci Marc.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Marc Richer [mailto:Marc.Richer@rcmp-grc.gc.ca]
Sent: Friday, April 12, 2013 1:30 PM
To: Swift, Andrew; Wilson, Barbara; Slack, Jessica; Durand, Stéphanie
Cc: Lavoie, Daniel; Derek Cefaloni; Greg Cox; Joe De Mora; Julie Gagnon
Subject: Commr Paulson scrum in Alberta

on Reateh Parsons:

Joint effort lead by Halifax Police Service
Analysis of info complex
Asked about RCMP willingness to work with Anonymous
Said rcmp will work with anyone but Anonymous isn't held to same standard of truth
We will work with them if they take the mask off

Marc

Swift, Andrew

From: Slack, Jessica
Sent: Friday, April 12, 2013 3:20 PM
To: Carmichael, Julie; Mueller, Mike; Johnson, Mark; McGrath, Andrew
Cc: Swift, Andrew; Durand, Stéphanie; Miller, Kevin; Tomlinson, Jamie
Subject: FW: "H" Div Parson Statement

Categories: ATI PRINT

Julie- see below for statement going out on re-opening of investigation re Ms. Parsons.
Jessica

From: Greg Cox [mailto:Greg.Cox@rcmp-grc.gc.ca]
Sent: April-12-13 3:16 PM
To: Swift, Andrew; Wilson, Barbara; Slack, Jessica; Miller, Kevin
Cc: Durand, Stéphanie; Lavoie, Daniel; Derek Cefaloni; Joe De Mora; Julie Gagnon; Marc Richer
Subject: "H" Div Parson Statement

FYI, this is going out now.....

New Information Leads to Reopening of Rehtaeh Parsons Investigation

April 12, 2013, Halifax Regional Municipality (HRM).....In light of new and credible information that has recently been brought forward to police, HRM Partners in Policing are reopening the investigation involving Rehtaeh Parsons.

An investigative team from the Criminal Investigation Division, comprised of both RCMP and Halifax Regional Police officers, has been assigned to review this new information as it relates to the totality of this file.

This information did not come from an on-line source. The person providing the information is willing to verify who they are, the reason they're providing it and is willing to work with police as part of the investigation.

We continue to ask people with specific information about this incident to report it to police or Crime Stoppers. Though police reports cannot be accepted through social media, tips can be reported anonymously to Crime Stoppers by calling toll-free 1-800-222-TIPS (8477), submitting a secure web tip at www.crimestoppers.ns.ca or texting a tip - Tip 202 + your message to 274637.

On behalf of the family, we again ask that both the media and public respect their request for privacy at this difficult time. Our thoughts remain with Rehteah's family and other loved ones.
-30-

Contact person:

Cpl. Scott MacRae

Pages 762 to / à 764

are duplicates of

sont des duplicatas des

pages 787 to / à 789

From: Pamela Williams <Pamela.Williams@ssc-spc.gc.ca>
Sent: Wednesday, October 24, 2012 12:38 PM
To: 'ctec@cse-cst.gc.ca'; CYBERDO
Cc: Lucie Levesque; Erik Caron; Denis Patenaude; Alain Robert; RCN GPS CPI - NCR SMD IPC; Chris Lemieux
Subject: 1 of 3

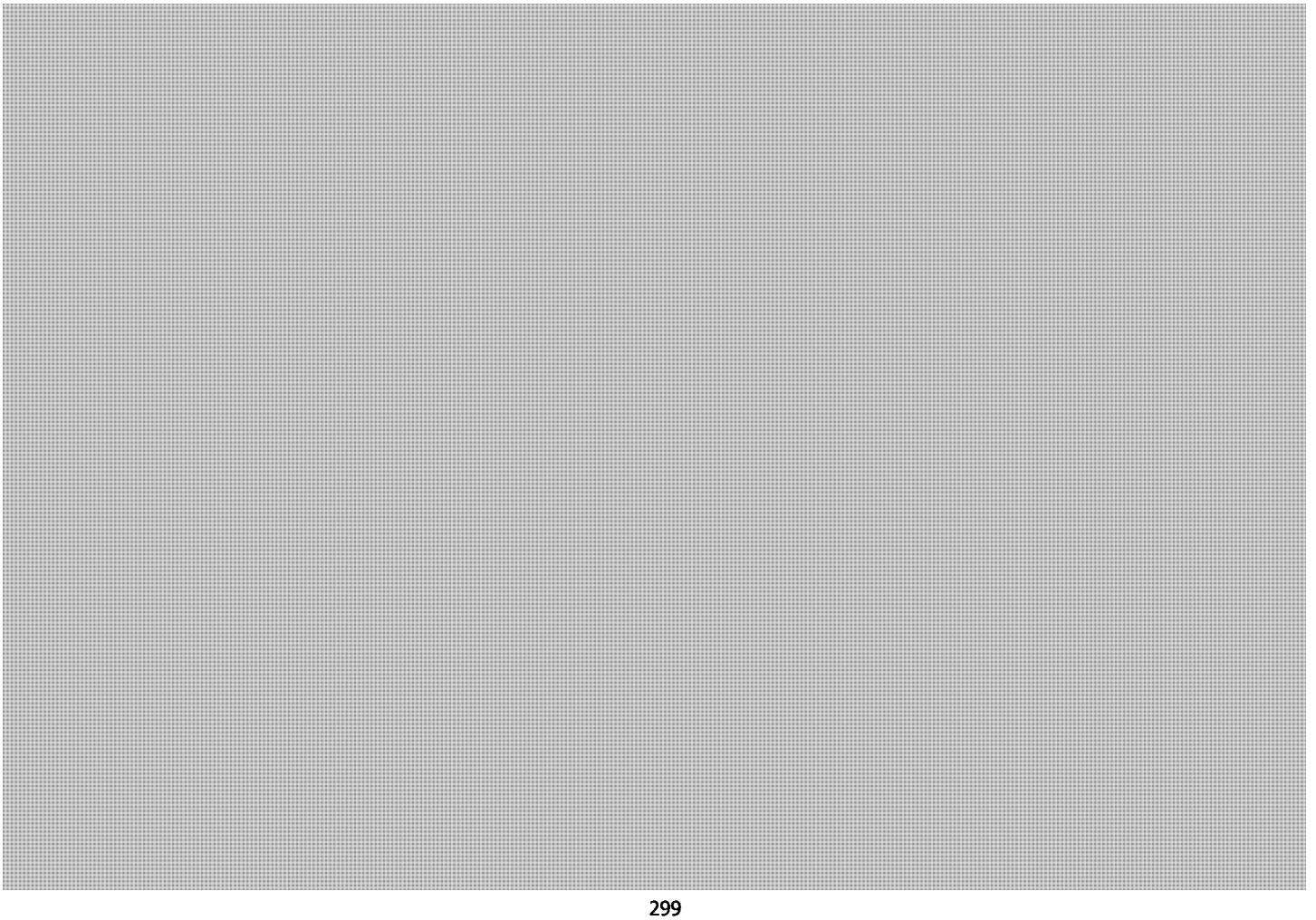
For your attention and awareness, here is addition information we have found with regards to the current situation. Multiple emails (3) for ease of reference.

If you have any questions, please contact DA Chris Lemieux at 819-956-1006.

Thanks,
Pamela L. Williams
Phone: 819-956-6318

-----Original Message-----
From: Christopher Locke
Sent: Wednesday, October 24, 2012 12:32
To: Pamela Williams
Subject: FW:

s.16(2)
s.16(2)(c)



Pages 766 to / à 773

are withheld pursuant to sections

sont retenues en vertu des articles

16(2), 16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

From: Pamela Williams <Pamela.Williams@ssc-spc.gc.ca>
Sent: Wednesday, October 24, 2012 12:39 PM
To: 'ctec@cse-cst.gc.ca'; CYBERDO
Cc: Lucie Levesque; Erik Caron; Denis Patenaude; Alain Robert; RCN GPS CPI - NCR SMD IPC; Chris Lemieux
Subject: 3 of 3

For your attention and awareness, here is addition information we have found with regards to the current situation. Multiple emails (3) for ease of reference.

If you have any questions, please contact DA Chris Lemieux at 819-956-1006.

Thanks,

Pamela L. Williams
Phone: 819-956-6318

-----Original Message-----
From: Christopher Locke
Sent: Wednesday, October 24, 2012 12:32
To: Pamela Williams
Subject: FW: sched

s.16(2)
s.16(2)(c)

[redacted]

From: Pamela Williams <Pamela.Williams@ssc-spc.gc.ca>
Sent: Wednesday, October 24, 2012 12:39 PM
To: 'ctec@cse-cst.gc.ca'; CYBERDO
Cc: Lucie Levesque; Erik Caron; Denis Patenaude; Alain Robert; RCN GPS CPI - NCR SMD IPC; Chris Lemieux
Subject: 2 of 3

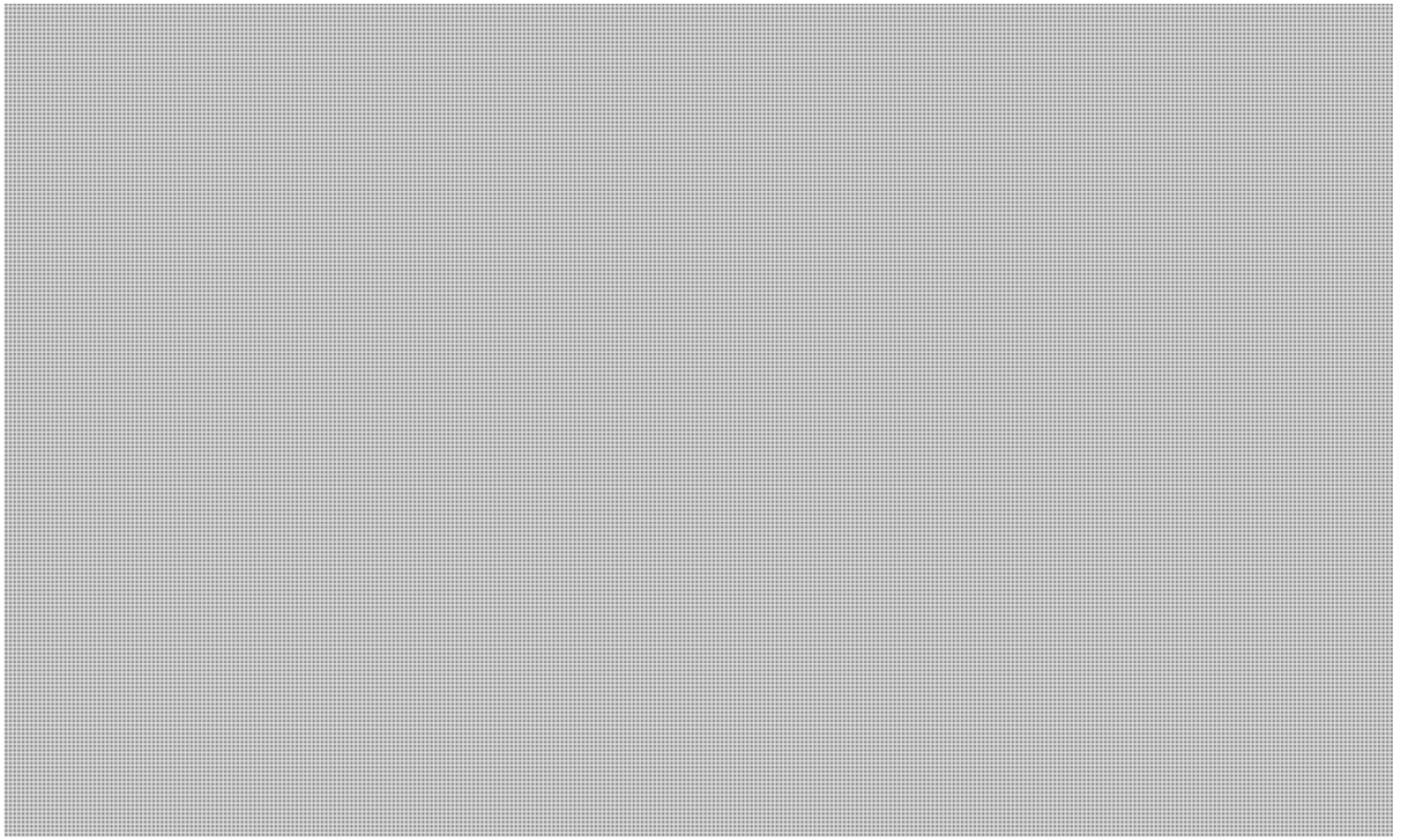
For your attention and awareness, here is addition information we have found with regards to the current situation. Multiple emails (3) for ease of reference.

If you have any questions, please contact DA Chris Lemieux at 819-956-1006.

Thanks,
Pamela L. Williams
Phone: 819-956-6318

-----Original Message-----
From: Christopher Locke
Sent: Wednesday, October 24, 2012 12:32
To: Pamela Williams
Subject: FW:

s.16(2)
s.16(2)(c)



Pages 776 to / à 782

are withheld pursuant to sections

sont retenues en vertu des articles

16(2), 16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO
Sent: Wednesday, October 24, 2012 1:59 PM
To: 'Pamela Williams'
Cc: CYBERDO
Subject: CE12-003863 [#OpPartyCrasher Anonymous DDoS] RE: Other Manifest

Pamela,
thanks for reporting this to us, we have assigned the following reference number CE12-003863 [#OpPartyCrasher Anonymous DDoS] for any future correspondence.
We will take appropriate action and notify potentially affected victims.

Again thanks for your time.

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613- s.16(2)(c) Facsimile | Télécopieur +1 613-991-3574 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Pamela Williams [mailto:Pamela.Williams@ssc-spc.gc.ca]
Sent: Wednesday, October 24, 2012 1:28 PM
To: 'ctec@cse-cst.gc.ca'; CYBERDO
Cc: Lucie Levesque; Erik Caron; Denis Patenaude; Alain Robert; RCN GPS CPI - NCR SMD IPC; Chris Lemieux
Subject: Other Manifest

For your attention and awareness, here is addition information we have found with regards to the current situation. Multiple emails for ease of reference.

If you have any questions, please contact DA Chris Lemieux at 819-956-1006.

Thanks,

Pamela L. Williams
Phone: 819-956-6318

-----Original Message-----
From: Christopher Locke
Sent: Wednesday, October 24, 2012 13:19
To: Pamela Williams
Subject: FW: manifest

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Wednesday, October 24, 2012 2:13 PM
To: CYBERDO
Cc: CTEC
Subject: RE: [CE2012-1289] #OpPartyCrasher Anonymous DDoS attacks

Classification: UNCLASSIFIED

We are actively working with ensuring protection of

Cheers,

s.15(1) - Subv

Incident Handler
Cyber Threat Evaluation Centre
ctec@cse-cst.gc.ca

To report incidents affecting GC infrastructures contact GC-CTEC at ctec@cse-cst.gc.ca. Any government department suspecting cyber incidents should provide a written report to GC-CTEC.

-----Original Message-----
From: CYBERDO [mailto s.16(2)(c)
Sent: October 24, 2012 2:03 PM
To: CTEC; CYBERDO
Subject: RE: [CE2012-1289] #OpPartyCrasher Anonymous DDoS attacks

Could you Just confirm that CTEC will notify the fol: s.16(2)

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Wednesday, October 24, 2012 1:26 PM
To: CYBERDO
Cc: CTEC
Subject: [CE2012-1289] #OpPartyCrasher Anonymous DDoS attacks

Classification: UNCLASSIFIED

Good afternoon,

Please see below text,

<<sched2.txt>>

This is part of a larger campaign against the GoC, and looks to now be including Conservative party assets. We are sending this to you, to follow-up as needed with the Conservative parties, as they fall outside of our scope.

Cheers,

From: [redacted]@CSE-CST.GC.CA>
Sent: Wednesday, October 24, 2012 2:20 PM
To: Pamela Williams; CTEC; CYBERDO
Cc: Lucie Levesque; Erik Caron; Denis Patenaude; RCN GPS CPI - NCR SMD IPC; Chris Lemieux

Classification: UNCLASSIFIED

Thanks for the info Pam. s.15(1) - Subv

[redacted]
Team Leader GC-CTEC Incident Handling
Communications Security Establishment

-----Original Message-----
From: Pamela Williams [mailto:Pamela.Williams@ssc-spc.gc.ca]
Sent: October 24, 2012 12:17 PM
To: CTEC; "CYBERDO' ([redacted] s.16(2)(c)
Cc: Lucie Levesque; Erik Caron; Denis Patenaude; RCN GPS CPI - NCR SMD IPC; Chris Lemieux
Subject: As discussed [redacted]

As discussed with Duty Analyst, here's the information:

s.16(2)

[redacted]

Page 788

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Pamela L. Williams
Spécialiste de la sécurité de la TI / IT Security Specialist Opérations de sécurité / Security Operations Services partagés Canada / Shared Services Canada Gatineau, Quebec, K1A 0S5 Pamela.Williams@TPSGC-PWGSC.GC.CA Téléphone / Telephone 819-956-6318 Gouvernement du Canada / Government of Canada

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Wednesday, October 24, 2012 2:38 PM
To: CYBERDO
Cc: CTEC
Subject: RE: [CE2012-1289] #OpPartyCrasher Anonymous DDoS attacks

Classification: UNCLASSIFIED

Part 2 of the ever growing list. Starred ones will be dealt with at the federal level.

Cheers,

[redacted]

s.15(1) - Subv
s.16(2)

[redacted]

From: CYBERDO
Sent: Wednesday, October 24, 2012 2:52 PM
To: 'RCMP_TCB_Operations@rcmp-grc.gc.ca'
Cc: CYBERDO
Subject: CE12-003863 [#OpPartyCrasher Anonymous DDoS]
Attachments:

FYI,
Please see below and find attached information on a Potential DDOS campaign that was posted on Pastebin, we are actively notifying and will follow up.

Cyber Duty Officer | Officier de veille cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613 s.16(2)(c)
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

s.16(2)

We have assigned reference numberCE12-003863 for all future correspondence regarding this event.

Cyber Duty Officer | Officier de veille cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613- s.16(2)(c)
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

Pages 793 to / à 795

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

s.16(2)(c)

Turbide, Frank

From: Alain.Labossiere@ic.gc.ca
Sent: October-24-12 3:32 PM
To: [redacted]@ic.gc.ca
Subject: U2 - N1 - ANONYMOUS DDoS Activity - OpPartyCrasher etc (U2 - N2)

Importance: High

Folks

I am re-forwarding this email as CTEC called me to inform me that [redacted]

s.20(1)(c)

Please confirm reception.

Also please reply to CTEC questions if applicable.

Thank you.

Alain

s.15(1) - Subv
s.16(2)

-----Original Message-----

From: [redacted] [mailto:[redacted]@CSE-CST.GC.CA]
Sent: Wednesday, October 24, 2012 3:01 PM
To: [redacted]
Subject: ANONYMOUS DDoS Activity - OpPartyCrasher etc (U2 - N2)

Classification: UNCLASSIFIED

Hi [redacted] members, Anonymous is starting a few new DDoS Ops. The tool of choice appears to be [redacted]

[redacted]

Thanks

[redacted]

GC-CTEC
CSEC

s.15(1) - Subv
s.16(2)

==========

[redacted]

Pages 798 to / à 802

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Proulx, Véronique

From: Proulx, Véronique
Sent: October-24-12 4:17 PM
To: Dick, Robert; Matz, Mark; Hatfield, Adam; Labelle, Sébastien; Anderson, Windy; Gordon, Robert
Cc: Bendelier, Kenneth; Klassen, Nathan; Proulx, Véronique; Pacha, Tomasz; Beaudoin, Luc; Clow, Patrick; Fortunato, Stephanie;
Subject: CYBER NOTIFICATION-12-014 – LOW IMPACT SEVERITY – MEDIA INTEREST– Distributed Denial-of-Service Attacks Targeting Government Entities

CYBER NOTIFICATION – INCIDENT

Incident Number: CNT-12-014 – LOW IMPACT SEVERITY – MEDIA INTEREST

Description of Incident: CCIRC has become aware of distributed denial-of-service (DDoS) attacks that are currently targeting municipal, provincial, and federal government entities.

Sources of reporting: Trusted partners and open sources.

Current actions: CCIRC has directly notified its affected partners, and is collaborating with federal and non-federal partners to further assess the situation. CCIRC will continue to monitor and if necessary, will release further products. CCIRC's DDoS mitigation guidelines are available on its website.

Initial analysis / assessment:

- From initial reporting, CCIRC believes that these
-
-
-

s.16(2)

Disclaimer:

This notification is only for distribution within Public Safety Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Nate Klassen & Véronique Proulx (991-6052 & 990-7102)
Approved by: Windy Anderson (991-7055)

Véronique Proulx
Analyst | Analyste
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada

257 Slater St. | 257 rue Slater
Ottawa, Ontario, Canada K1A 0P8
Tel : (613) 990-7102
veronique.proulx@ps-sp.gc.ca

From: Beaudoin, Luc
Sent: Wednesday, October 24, 2012 4:19 PM
To:
Cc: CYBERDO; Bendelier, Kenneth; Clow, Patrick
Subject: Re: CE12-003863 [OpPartyCrasher Anonymous]

Brilliant. Well done.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

s.16(2)(c)

Sent from a mobile device | Envoyé d'un appareil portable

s.16(2)

From:
Sent: Wednesday, October 24, 2012 03:53 PM
To: Beaudoin, Luc
Cc: CYBERDO
Subject: FW: CE12-003863 [OpPartyCrasher Anonymous]

FYI, We notified the 3 cities (Surrey, Vancouver and Toronto) that they were listed as possible targets. CTEC is addressing all Fed items. We will notify the conservative party websites contacts in the am.

Spoke with Bruce (cyberdo) and he is aware of the situation.

Thanks,

From:
Sent: Wednesday, October 24, 2012 3:37 PM
To: * CyberIH
Cc: CYBERDO
Subject: CE12-003863 [OpPartyCrasher Anonymous]

Here's a nice summary.

Reminder, here is a link to our DoS Mitigation guide: http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Cheers,

From: Clow, Patrick
Sent: Wednesday, October 24, 2012 3:27 PM
To: Proulx, Véronique; Klassen, Nathan

Cc: Anderson, Windy; [redacted]
Subject: Information

s.16(2)

[redacted]

Pages 807 to / à 811

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

s.15(1) - Subv
s.16(2)
s.16(2)(c)

Turbide, Frank

From: Frank.Turbide@ps-sp.gc.ca
Sent: October-24-12 4:44 PM
To: Clow, Patrick
Cc: Bergeron, Dominic
Subject: FW: ANONYMOUS DDoS Activity - OpPartyCrasher etc (U2 - N2)

I had a chat with [redacted] He tells me the lead on this is Shared Services and that they are working on a product for Gov only to be completed tomorrow morning. He had no other indicators or samples to offer, and could not speak authoritatively [redacted] I suggest we bring it up tomorrow morning at the brief.

Frank

-----Original Message-----
From: [redacted] [mailto [redacted] @CSE-CST.GC.CA]
Sent: October-24-12 4:05 PM
To: [redacted] @ic.gc.ca
Subject: ANONYMOUS DDoS Activity - OpPartyCrasher etc (U2 - N2)

Classification: UNCLASSIFIED

Let's try resending this email [redacted] At least now you'll know what to search for in your junk mail folder.

Thanks
[redacted]

-----Original Message-----
From: [redacted]
Sent: October 24, 2012 3:01 PM
To: [redacted] @ic.gc.ca
Subject: ANONYMOUS DDoS Activity - OpPartyCrasher etc (U2 - N2)

Classification: UNCLASSIFIED

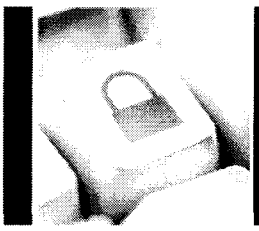
Hi [redacted] members, Anonymous is starting a few new DDoS Ops. The tool of choice appears to be [redacted]

[redacted]

Thanks

[redacted]
GC-CTEC
CSEC

==========



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****
s.16(2)
Date: 25 October 2012
CYBERDO: Bruce
****

[FOUO] NEW EVENTS:

1. Title: CE12-003860 [Malware hosted on
- Summary: CCIRC was notified of possible malware being hosted on
- Action/Decision: Notification sent to technical contact.
  - Owner: Ian
  - Status: Active

2. Title: CE12-003862 [EFax – Possible Zeus]
- Summary: CCIRC received indicators from a trusted source of possible Zeus malware.
- Action/Decision: Monitoring.
  - Owner: Ian
  - Status: Active

3. Title: CE12-003863 [DDoS – #OpPartyCrasher]
- Summary: CCIRC was notified by a Federal partner of a potential DDoS against municipal, provincial and federal entities.
- Action/Decision: Notifications sent to potential targets.
  - Owner: Steve
  - Status: Active

4. Title: CE12-003865 [Malware – Hosted on
- Summary: CCIRC was notified of possible malicious malware being hosted on

- Action/Decision: Notification sent to technical contact.
  - Owner: Ian
  - Status: Active

Canada

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE: NIL

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. **US-CERT :** [redacted]
2. **US-CERT: Weekly Cyber Threat Review**

PUBLICATIONS:

1. **CCIRC ADVISORY AV12-043: Security Update Available of Adobe Shockwave Player**
   Reference: **http://www.publicsafety.gc.ca/prg/em/ccirc/2012/av12-043-eng.aspx**

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. **New cybercrime monetization methods**
   AVG's new report investigates a number of malicious software developments including the newly launched 2.0 version of the Blackhole Exploit Toolkit, the evolution in malware targeting mobile banking services, a surge in malicious ads targeting social network users and a trick to hide malware inside image files.
   Reference: http://www.net-security.org/malware_news.php?id=2303

2. **The Michigan fight song and four other reasons to avoid Internet voting**
   [...] Even more ambitious than the use of electronic voting machines in polling places would be to do away with the polling places altogether, conducting elections over the Internet. We didn't discuss this option in our previous piece because Internet voting has yet to catch on in the United States, but the topic crops up regularly in discussions (including in the Ars forums). So we thought it would be worthwhile to discuss five reasons it would be a big mistake to allow Americans to cast their votes online: Hacked servers, Client-side malware, Authentication, Coercion and bribery and Usability problems.
   Reference: http://arstechnica.com/tech-policy/2012/10/the-michigan-fight-song-and-four-other-reasons-to-avoid-internet-voting/

3. **IDF To Double Unit 8200 Cyber-War Manpower – OpEd**
The Israel's Channel 2 reports (Hebrew) that the IDF intends to double the manpower of its Unit 8200, which is charged with waging cyber-war on Israel's enemies. It plays a role akin to the NSA here in the U.S. and was responsible for creating Stuxnet, Flame and the other cyber-viruses which have decimated Iran's nuclear and oil facilities.
Reference: http://www.eurasiareview.com/24102012-idf-to-double-unit-8200-cyber-war-manpower-oped/

4. **Phishing websites proliferate at record speed**
"Phishers seem to be concentrating their efforts on compromising legitimate websites using automated attack tools, or purchasing access to them on the burgeoning underground market," said Rod Rasmussen, CTO of Internet Identity and co-author of the report. "This allows them to leverage the good reputation of a website's domain name, making it harder to block in either spam filters or via suspension, and makes takedown of that domain impractical."
Reference: http://www.eurasiareview.com/24102012-idf-to-double-unit-8200-cyber-war-manpower-oped/

5. **Huawei offers Australia source code access**
Chinese telecommunications equipment manufacturer Huawei has offered the Australian government unrestricted access to its source code and hardware to appease fears of backdoors in its products, according to a BBC report. The Australian government had previously prevented the company from providing hardware for its national broadband network, citing concerns about the company's ties to the Chinese military.
Reference: http://www.h-online.com/security/news/item/Huawei-offers-Australia-source-code-access-1735921.html

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	

Secunia (http://secunia.com/advisories/historic/) ☒
TrendLabs Malware Blog (http://blog.trendmicro.com/) ☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html) ☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/) ☒
Internet Storm Center – Sans (http://isc.sans.org) ☒
Softpedia – Security (http://news.softpedia.com/cat/Security/) ☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/) ☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/) ☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/) ☒
The H Security (http://www.h-online.com/security/) ☒
Help Net Security (http://www.net-security.org/) ☒
SecuriTeam (http://www.securiteam.com/) ☒

News and Trends:

The Kaspersky Lab Security News Service (http://threatpost.com/) ☒
Sucuri Research Blog (http://blog.sucuri.net/) ☒
F-Secure (http://www.f-secure.com/weblog/) ☒
Topix News (http://www.topix.net/tech/computer-security) ☒
Krebs on Security (http://krebsonsecurity.com/) ☒
Threat Level (http://www.wired.com/threatlevel/) ☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security) ☒
Info Security News Mailing List (http://seclists.org/isn/) ☒

[FOUO] GENERAL INFORMATION:

Turbide, Frank

From: Clow, Patrick
Sent: October-25-12 10:56 AM
To: CYBERDO
Cc: Turbide, Frank; Bergeron, Dominic; Beaudoin, Luc
Subject: FW: files
Attachments:

CYBERDO,

As promised, please find attached a copy of the associated with the event we're currently tracking.

From: Turbide, Frank
Sent: Thursday, October 25, 2012 8:28 AM
To: Clow, Patrick
Subject: files

Pages 819 to / à 829

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Page 830

is withheld pursuant to sections

est retenue en vertu des articles

16(2), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 831 to / à 851

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

http://pastebin.com/6P3i40wb

Canadian Charter of Rights and Freedoms
BY: A GUEST ON OCT 17TH, 2012 | SYNTAX: NONE | SIZE: 16.66 KB | HITS: 76 | EXPIRES: NEVER

CONSTITUTION ACT, 1982 (80)
1982, c. 11 (U.K.), Schedule B
PART I
CANADIAN CHARTER OF RIGHTS AND FREEDOMS
Whereas Canada is founded upon principles that recognize the supremacy of God and the rule of law:
GUARANTEE OF RIGHTS AND FREEDOMS
Marginal note:Rights and freedoms in Canada
1. The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.
FUNDAMENTAL FREEDOMS
Marginal note:Fundamental freedoms
2. Everyone has the following fundamental freedoms:
• (a) freedom of conscience and religion;
• (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;
• (c) freedom of peaceful assembly; and
• (d) freedom of association.
DEMOCRATIC RIGHTS
Marginal note:Democratic rights of citizens
3. Every citizen of Canada has the right to vote in an election of members of the House of Commons or of a legislative assembly and to be qualified for membership therein.
Marginal note:Maximum duration of legislative bodies
• 4. (1) No House of Commons and no legislative assembly shall continue for longer than five years from the date fixed for the return of the writs at a general election of its members. (81)
• Marginal note:Continuation in special circumstances
(2) In time of real or apprehended war, invasion or insurrection, a House of Commons may be continued by Parliament and a legislative assembly may be continued by the legislature beyond five years if such continuation is not opposed by the votes of more than one-third of the members of the House of Commons or the legislative assembly, as the case may be. (82)
Marginal note:Annual sitting of legislative bodies
5. There shall be a sitting of Parliament and of each legislature at least once every twelve months. (83)
MOBILITY RIGHTS
Marginal note:Mobility of citizens
• 6. (1) Every citizen of Canada has the right to enter, remain in and leave Canada.
• Marginal note:Rights to move and gain livelihood
(2) Every citizen of Canada and every person who has the status of a permanent resident of Canada has the right
o (a) to move to and take up residence in any province; and
o (b) to pursue the gaining of a livelihood in any province.
• Marginal note:Limitation
(3) The rights specified in subsection (2) are subject to
o (a) any laws or practices of general application in force in a province other than those that discriminate among persons primarily on the basis of province of present or previous residence; and
o (b) any laws providing for reasonable residency requirements as a qualification for the receipt of publicly provided social services.
• Marginal note:Affirmative action programs
(4) Subsections (2) and (3) do not preclude any law, program or activity that has as its object the amelioration in a province of conditions of individuals in that

province who are socially or economically disadvantaged if the rate of employment in that province is below the rate of employment in Canada.

LEGAL RIGHTS

Marginal note:Life, liberty and security of person

7. Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.

Marginal note:Search or seizure

8. Everyone has the right to be secure against unreasonable search or seizure.

Marginal note:Detention or imprisonment

9. Everyone has the right not to be arbitrarily detained or imprisoned.

Marginal note:Arrest or detention

10. Everyone has the right on arrest or detention

- (a) to be informed promptly of the reasons therefor;
- (b) to retain and instruct counsel without delay and to be informed of that right; and
- (c) to have the validity of the detention determined by way of habeas corpusand to be released if the detention is not lawful.

Marginal note:Proceedings in criminal and penal matters

11. Any person charged with an offence has the right

- (a) to be informed without unreasonable delay of the specific offence;
- (b) to be tried within a reasonable time;
- (c) not to be compelled to be a witness in proceedings against that person in respect of the offence;
- (d) to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal;
- (e) not to be denied reasonable bail without just cause;
- (f) except in the case of an offence under military law tried before a military tribunal, to the benefit of trial by jury where the maximum punishment for the offence is imprisonment for five years or a more severe punishment;
- (g) not to be found guilty on account of any act or omission unless, at the time of the act or omission, it constituted an offence under Canadian or international law or was criminal according to the general principles of law recognized by the community of nations;
- (h) if finally acquitted of the offence, not to be tried for it again and, if finally found guilty and punished for the offence, not to be tried or punished for it again; and
- (i) if found guilty of the offence and if the punishment for the offence has been varied between the time of commission and the time of sentencing, to the benefit of the lesser punishment.

Marginal note:Treatment or punishment

12. Everyone has the right not to be subjected to any cruel and unusual treatment or punishment.

Marginal note:Self-crimination

13. A witness who testifies in any proceedings has the right not to have any incriminating evidence so given used to incriminate that witness in any other proceedings, except in a prosecution for perjury or for the giving of contradictory evidence.

Marginal note:Interpreter

14. A party or witness in any proceedings who does not understand or speak the language in which the proceedings are conducted or who is deaf has the right to the assistance of an interpreter.

EQUALITY RIGHTS

Marginal note:Equality before and under law and equal protection and benefit of law

- 15. (1) Every individual is equal before and under the law and has the right to the equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.
- Marginal note:Affirmative action programs

(2) Subsection (1) does not preclude any law, program or activity that has as its object the amelioration of conditions of disadvantaged individuals or groups including those that are disadvantaged because of race, national or ethnic origin, colour, religion, sex, age or mental or physical disability. (84)

OFFICIAL LANGUAGES OF CANADA

Marginal note:Official languages of Canada

• 16. (1) English and French are the official languages of Canada and have equality of status and equal rights and privileges as to their use in all institutions of the Parliament and government of Canada.

• Marginal note:Official languages of New Brunswick

(2) English and French are the official languages of New Brunswick and have equality of status and equal rights and privileges as to their use in all institutions of the legislature and government of New Brunswick.

• Marginal note:Advancement of status and use

(3) Nothing in this Charter limits the authority of Parliament or a legislature to advance the equality of status or use of English and French.

Marginal note:English and French linguistic communities in New Brunswick

• 16.1 (1) The English linguistic community and the French linguistic community in New Brunswick have equality of status and equal rights and privileges, including the right to distinct educational institutions and such distinct cultural institutions as are necessary for the preservation and promotion of those communities.

• Marginal note:Role of the legislature and government of New Brunswick

(2) The role of the legislature and government of New Brunswick to preserve and promote the status, rights and privileges referred to in subsection (1) is affirmed.(85)

Marginal note:Proceedings of Parliament

• 17. (1) Everyone has the right to use English or French in any debates and other proceedings of Parliament. (86)

• Marginal note:Proceedings of New Brunswick legislature

(2) Everyone has the right to use English or French in any debates and other proceedings of the legislature of New Brunswick. (87)

Marginal note:Parliamentary statutes and records

• 18. (1) The statutes, records and journals of Parliament shall be printed and published in English and French and both language versions are equally authoritative.(88)

• Marginal note:New Brunswick statutes and records

(2) The statutes, records and journals of the legislature of New Brunswick shall be printed and published in English and French and both language versions are equally authoritative. (89)

Marginal note:Proceedings in courts established by Parliament

• 19. (1) Either English or French may be used by any person in, or in any pleading in or process issuing from, any court established by Parliament. (90)

• Marginal note:Proceedings in New Brunswick courts

(2) Either English or French may be used by any person in, or in any pleading in or process issuing from, any court of New Brunswick. (91)

Marginal note:Communications by public with federal institutions

• 20. (1) Any member of the public in Canada has the right to communicate with, and to receive available services from, any head or central office of an institution of the Parliament or government of Canada in English or French, and has the same right with respect to any other office of any such institution where

o (a) there is a significant demand for communications with and services from that office in such language; or

o (b) due to the nature of the office, it is reasonable that communications with and services from that office be available in both English and French.

• Marginal note:Communications by public with New Brunswick institutions

(2) Any member of the public in New Brunswick has the right to communicate with, and to receive available services from, any office of an institution of the legislature or government of New Brunswick in English or French.

Marginal note:Continuation of existing constitutional provisions

21. Nothing in sections 16 to 20 abrogates or derogates from any right, privilege or obligation with respect to the English and French languages, or either of them, that exists or is continued by virtue of any other provision of the Constitution of Canada. (92)

Marginal note:Rights and privileges preserved

22. Nothing in sections 16 to 20 abrogates or derogates from any legal or customary right or privilege acquired or enjoyed either before or after the coming into force

of this Charter with respect to any language that is not English or French.

MINORITY LANGUAGE EDUCATIONAL RIGHTS

Marginal note:Language of instruction

• 23. (1) Citizens of Canada

o (a) whose first language learned and still understood is that of the English or French linguistic minority population of the province in which they reside, or

o (b) who have received their primary school instruction in Canada in English or French and reside in a province where the language in which they received that instruction is the language of the English or French linguistic minority population of the province,

have the right to have their children receive primary and secondary school instruction in that language in that province. (93)

• Marginal note:Continuity of language instruction

(2) Citizens of Canada of whom any child has received or is receiving primary or secondary school instruction in English or French in Canada, have the right to have all their children receive primary and secondary school instruction in the same language.

• Marginal note:Application where numbers warrant

(3) The right of citizens of Canada under subsections (1) and (2) to have their children receive primary and secondary school instruction in the language of the English or French linguistic minority population of a province

o (a) applies wherever in the province the number of children of citizens who have such a right is sufficient to warrant the provision to them out of public funds of minority language instruction; and

o (b) includes, where the number of those children so warrants, the right to have them receive that instruction in minority language educational facilities provided out of public funds.

ENFORCEMENT

Marginal note:Enforcement of guaranteed rights and freedoms

• 24. (1) Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.

• Marginal note:Exclusion of evidence bringing administration of justice into disrepute

(2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

GENERAL

Marginal note:Aboriginal rights and freedoms not affected by Charter

25. The guarantee in this Charter of certain rights and freedoms shall not be construed so as to abrogate or derogate from any aboriginal, treaty or other rights or freedoms that pertain to the aboriginal peoples of Canada including

• (a) any rights or freedoms that have been recognized by the Royal Proclamation of October 7, 1763; and

• (b) any rights or freedoms that now exist by way of land claims agreements or may be so acquired. (94)

Marginal note:Other rights and freedoms not affected by Charter

26. The guarantee in this Charter of certain rights and freedoms shall not be construed as denying the existence of any other rights or freedoms that exist in Canada.

Marginal note:Multicultural heritage

27. This Charter shall be interpreted in a manner consistent with the preservation and enhancement of the multicultural heritage of Canadians.

Marginal note:Rights guaranteed equally to both sexes

28. Notwithstanding anything in this Charter, the rights and freedoms referred to in it are guaranteed equally to male and female persons.

Marginal note:Rights respecting certain schools preserved

29. Nothing in this Charter abrogates or derogates from any rights or privileges guaranteed by or under the Constitution of Canada in respect of denominational,

separate or dissentient schools. (95)
Marginal note:Application to territories and territorial authorities
30. A reference in this Charter to a province or to the legislative assembly or legislature of a province shall be deemed to include a reference to the Yukon Territory and the Northwest Territories, or to the appropriate legislative authority thereof, as the case may be.
Marginal note:Legislative powers not extended
31. Nothing in this Charter extends the legislative powers of any body or authority.
APPLICATION OF CHARTER
Marginal note:Application of Charter
• 32. (1) This Charter applies
o (a) to the Parliament and government of Canada in respect of all matters within the authority of Parliament including all matters relating to the Yukon Territory and Northwest Territories; and
o (b) to the legislature and government of each province in respect of all matters within the authority of the legislature of each province.
• Marginal note:Exception
(2) Notwithstanding subsection (1), section 15 shall not have effect until three years after this section comes into force.
Marginal note:Exception where express declaration
• 33. (1) Parliament or the legislature of a province may expressly declare in an Act of Parliament or of the legislature, as the case may be, that the Act or a provision thereof shall operate notwithstanding a provision included in section 2 or sections 7 to 15 of this Charter.
• Marginal note:Operation of exception
(2) An Act or a provision of an Act in respect of which a declaration made under this section is in effect shall have such operation as it would have but for the provision of this Charter referred to in the declaration.
• Marginal note:Five year limitation
(3) A declaration made under subsection (1) shall cease to have effect five years after it comes into force or on such earlier date as may be specified in the declaration.
• Marginal note:Re-enactment
(4) Parliament or the legislature of a province may re-enact a declaration made under subsection (1).
• Marginal note:Five year limitation
(5) Subsection (3) applies in respect of a re-enactment made under subsection (4).
CITATION
Marginal note:Citation
34. This Part may be cited as the Canadian Charter of Rights and Freedoms.

Pages 857 to / à 864

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 865 to / à 866

are duplicates of

sont des duplicatas des

pages 516 to / à 517

Pages 867 to / à 868

are duplicates of

sont des duplicatas des

pages 518 to / à 519

Pages 869 to / à 872

are duplicates of

sont des duplicatas des

pages 518 to / à 521

CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****
Date: 26 October 2012
CYBERDO: Bruce
****

[FOUO] NEW EVENTS:

1. Title: CE12-003871 [Notification – Zeus p2p – Telecom]
- Summary: CCIRC analyzed multiple malware samples and found 38 Zeus p2p malware attempting to communicate with a telecom partner's IP address.
- Action/Decision: Notification sent to technical contact.
  - Owner: Patrick
  - Status: Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. CE12-003863 [#OpPartyCrasher Anonymous DDoS]
Request sent by Federal partner for CRR on site www[.]anonpaste[.]me. It was decided to review and discuss before requesting a CRR. Conference call with other Federal partners set for 0915 10/26/12.

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. **US-CERT :**
2. **ICS-CERT: ICS-ALERT-12-046-01A (Update) Increasing Threat to Industrial Control Systems**
Reference: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-046-01A.pdf

PUBLICATIONS:NIL

VULNERABILITY WATCH: NIL

THREAT WATCH:

1. **New Hack and Attack Tools Alert**
Cythosia Botnet v.2.0 Package

Detection rate 3/42
Tested with spynet,vertexnet,Xtreme,BlackShades
Reference: hxxp://www[.]mediafire[.]com/?egho57vdq257u0f

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. **SSL certificates and "the most dangerous code in the world"**
SSL is the de facto standard for secure, encrypted internet connections, but that security requires that a program validates the receiver's identity, specifically its SSL certificate. This is exactly where the researchers see a problem: in their study "The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software", they say that "SSL certificate validation is completely broken in many security-critical applications and libraries".
References: http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf
http://www.h-online.com/security/news/item/SSL-certificates-and-the-most-dangerous-code-in-the-world-1737168.html

2. **Operation High Roller Banked on Fast-Flux Botnet to Steal Millions**
A fraud ring that attacked financial transfer systems in an attempt to get at wealthy high-end banking customers used a complicated web of malware and compromised servers in several countries to walk off with an estimated $78 million earlier this year. While the attacks targeted financial systems, the victims seem to be limited to companies involved in manufacturing, import-export businesses, and state or local governments.
Reference: http://threatpost.com/en_us/blogs/operation-high-roller-banked-fast-flux-botnet-steal-millions-102412

3. **Attackers Turn to Open DNS Resolvers to Amplify DDoS Attacks**
Although DDoS attacks have been a serious problem for more than a decade now and security staffs have a good handle on how they're executed and how to handle them, attackers constantly adjust their tactics in order to defeat the best defenses available. One of the more recent tactics adopted by attackers is the use of open DNS resolvers to amplify their attacks, and this technique, while not novel, is beginning to cause serious problems for the organizations that come under these attacks.
Reference: http://threatpost.com/en_us/blogs/attackers-turn-open-dns-resolvers-amplify-ddos-attacks-102412

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION: NIL

From: CYBERDO
Sent: Friday, October 26, 2012 10:40 AM
To: 'Christopher Locke'; 'CTEC (ctec@cse-cst.gc.ca)'
Cc: 'Denis Patenaude'; 'RCN GPS CPI - NCR SMD IPC'; 'Lucie Levesque'
Subject: RE: Packet Sample [CCIRC CE12-003863]

Received.

CCIRC is tracking all activities regarding Anonymous DDoS Op PartyCrasher under event CE12-003863. Please refer to this number in the subject of all related correspondence. A TAR has been submitted for review by one of our technical analysts.

Bruce Moore
Incident Handler | Gestionnaire d'incident Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613 s.16(2)(c)
Facsimile | Télécopieur +1 613-991-3574 cyber-incident@ps-sp.gc.ca PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Christopher Locke [mailto:Christopher.Locke@tpsgc-pwgsc.gc.ca]
Sent: October-26-12 10:33 AM
To: 'CTEC (ctec@cse-cst.gc.ca)'; CYBERDO
Cc: Denis Patenaude; RCN GPS CPI - NCR SMD IPC; Lucie Levesque
Subject: Packet Sample s.16(2)

Hello,

Please find attached a sample packet pair for one of the event types I will be getting more packets today and will advise at that time.

Cheers,
Chris

Chris Locke
IT Security Analyst
Services partagés Canada | Shared Services Canada GOP/SIS/SOM Place du Portage, Phase III, Room 3E-823
11 Laurier St., Gatineau, Que. K1A 0S5

Téléphone | Telephone 819-956-6495
christopher.locke@pwgsc.gc.ca

From: Anderson, Windy
Sent: Friday, October 26, 2012 11:36 AM
To: Bendelier, Kenneth; [redacted] Beaudoin, Luc; Clow, Patrick
Cc: CYBERDO
Subject: RE: TBS Question

s.19(1)

Yes, thanks all. We can chat about this situation next week when we have a few minutes. I called Michel (he is [redacted] – co-worker of Stephane) to find out the scoop. I will explain the whole gory situation next week.

Have a great day,

Windy

Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Bendelier, Kenneth
Sent: October-26-12 11:34 AM
To: [redacted] Beaudoin, Luc; Anderson, Windy; Clow, Patrick
Cc: CYBERDO
Subject: Re: TBS Question

Merci [redacted]

From: [redacted]
Sent: Friday, October 26, 2012 11:31 AM
To: Bendelier, Kenneth; Beaudoin, Luc; Anderson, Windy; Clow, Patrick
Cc: CYBERDO
Subject: RE: TBS Question

Stephane Parson was asking a similar question and we sent him the following reply:

//////

We have not produced an IN specific to this DDoS. We have however notified the provincial and municipal entities that were listed as targets in the pastebin posts.

Along with the relevant information we also provided a link to our DDoS mitigation advice product:
http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Hopefully, you know that CTEC issued an IN note yesterday to its clients.

I can be reached at [redacted] today if needed. s.16(2)

Cheers,
[redacted]

-----Original Message-----
From: Parson, Stephane [mailto:Stephane.Parson@tbs-sct.gc.ca]
Sent: Friday, October 26, 2012 10:02 AM
To: Beaudoin, Luc; [redacted]
Subject: Ddos

Has ccirc produced an information note on the ddos? Can I get a copy please. Thx
---
Sent using BlackBerry

///////

I've also attached the CTEC IN.

[redacted]

From: Bendelier, Kenneth
Sent: Friday, October 26, 2012 11:12 AM
To: Beaudoin, Luc; Anderson, Windy; Clow, Patrick
Cc: CYBERDO
Subject: TBS Question

OK,

Here's one that's not my call

Received a phone call from Michel Proulx at TBS. They was to send a communique to Federal Depts (this morning) with respect to an "ongoing DDOS" attack.

He is requesting any "information" that we have sent to provinces with respect to this to include as background in the communique.

Michel is in GEDS. I sent him a "test" e-mail and he has responded so I am satisfied he is who he says he is. (attached)

So:

1. Have we sent anything to the provinces or others; (CYBERDO probably best to answer)
2. Is its info we would share with TBS which would then, in turn, share with Federal Depts.
3. Is this something better done through GC CTEC?

We sent the following through our chain as a CNT:

CYBER NOTIFICATION – INCIDENT

Incident Number: CNT-12-014 – LOW IMPACT SEVERITY – MEDIA INTEREST

Description of Incident: CCIRC has become aware of distributed denial-of-service (DDoS) attacks that are currently targeting municipal, provincial, and federal government entities.

Sources of reporting: Trusted partners and open sources.

Current actions: CCIRC has directly notified its affected partners, and is collaborating with federal and non-federal partners to further assess the situation. CCIRC will continue to monitor and if necessary, will release further products. CCIRC's DDoS mitigation guidelines are available on its website.

Initial analysis / assessment:

-
- Partners at the federal level have already reported these attacks.
- According to open source reports, it is possible that these attacks may also target Canadian political entities at various levels,
- CCIRC is aware, through open source reports, that Anonymous has been promoting two operations, named *#opf***harper* and *#oppartycrasher*, which call for DDoS attacks against government targets, beginning on November 3, 2012.

Disclaimer:

This notification is only for distribution within Public Safety Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Nate Klassen & Véronique Proulx (991-6052 & 990-7102)
Approved by: Windy Anderson (991-7055)

Véronique Proulx
Analyst | Analyste
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater St. | 257 rue Slater
Ottawa, Ontario, Canada K1A 0P8
Tel : (613) 990-7102
veronique.proulx@ps-sp.gc.ca

Ken Bendelier, CD, MSc
Manager – Operational Analysis and Support Section
Gestionnaire – Section de l'analyse et du support opérationnel
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-993-5042
Facsimile | Télécopieur +1 613-954-3097
Kenneth.Bendelier@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

Pages 882 to / à 883

are duplicates of

sont des duplicatas des

pages 562 to / à 563

Pages 884 to / à 886

are duplicates of

sont des duplicatas des

pages 573 to / à 575

Page 887

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 888 to / à 889
are withheld pursuant to section
sont retenues en vertu de l'article

16(2)

of the Access to Information
de la Loi sur l'accès à l'information

From: Klassen, Nathan
Sent: Monday, October 29, 2012 11:04 AM
To: CYBERDO
Subject: FW: CYBER NOTIFICATION-12-014-1 – LOW IMPACT SEVERITY – MEDIA INTEREST– NOT FOR ESCALATION -Distributed Denial-of-Service Attacks Targeting Government Entities (UPDATE One)

FYI

From: Klassen, Nathan
Sent: Monday, October 29, 2012 10:32 AM
To: Coady, Therese; Danaitis, Algis; Duguay, Marcel; Boily, Mario; Ku, Shawn; Guitor, Denis; McLeod, Tim; Currie, Chris; Duschner, Gabrielle; Mattioli, Mary-Ann; GOC-COG; Durand, Stéphanie; Champoux, Martin; Filipps, Lisa; Swift, Andrew; MacDonald, Michael; Wong, Suki; DeJong, Michael
Cc: Anderson, Windy; Bendelier, Kenneth; Klassen, Nathan; Proulx, Véronique; Pacha, Tomasz
Subject: CYBER NOTIFICATION-12-014-1 – LOW IMPACT SEVERITY – MEDIA INTEREST– NOT FOR ESCALATION - Distributed Denial-of-Service Attacks Targeting Government Entities (UPDATE One)

CYBER NOTIFICATION – INCIDENT

Note: Updates / Changes in **BOLD** text

Incident Number: CNT-12-014-**1** – LOW IMPACT SEVERITY – MEDIA INTEREST – NOT FOR ESCALATION

Description of Incident: CCIRC has become aware of distributed denial-of-service (DDoS) attacks that are currently targeting municipal, provincial, and federal government entities.

Sources of reporting: Trusted partners and open sources.

Current actions: CCIRC has directly notified its affected partners, and is collaborating with federal and non-federal partners to further assess the situation. CCIRC will continue to monitor and if necessary, will release further products. CCIRC's DDoS mitigation guidelines are available on its website.

Initial analysis / assessment:

-
- Partners at the federal level have already reported these attacks.
- According to open source reports, it is possible that these attacks may also target Canadian political entities at various levels,
- CCIRC is aware, through open source reports, that Anonymous has been promoting two operations, named *#opf***harper* and *#oppartycrasher*, which call for DDoS attacks against government targets, beginning on November 3, 2012.

- **Shared Services Canada is the lead on this incident and the Communications Security Establishment Canada is providing coordination support. CCIRC will continue to monitor the situation and will inform its affected partners if necessary.**

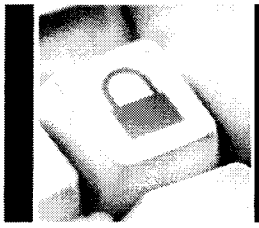
Disclaimer:

This notification is only for distribution within Public Safety Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Nate Klassen & Gregg Murphy (991-6052 & 991-3579)
Approved by: Ken Bendelier (993-5042)

Pages 892 to / à 894
are duplicates of
sont des duplicatas des
pages 582 to / à 584

Public Safety Canada / Sécurité publique Canada



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****
Date: 29 October 2012
CYBERDO: Bruce
****

[FOUO] NEW EVENTS:

1. Title: CE12-003877 [Possible BHEK]
- Summary: CCIRC was notified by a trusted source of possible blacole malware on site [redacted]
- Action/Decision: Technical Analysis Request (TAR) opened to investigate.
  - Owner: Ian
  - Status: Active

2. Title: CE12-003880 [Indicators provided by Financial Partner]
- Summary: A financial partner provided new indicators after using the indicators found in the CCIRC weekly technical report.

[redacted]

- Action/Decision: Shared with tech team.
  - Owner: Gregg
  - Status: Closed

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. CE12-003863 [#OpPartyCrasher Anonymous DDoS]

[redacted]

Canada

[redacted]

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. **ICS-CERT: ICS-ALERT-12-097-02A (Update) 3S Software Codesys Improper Access Control**
   Reference: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-097-02A.pdf
   http://www.3s-software.com/index.shtml?codesys_dev_dir

2. **US-CERT:** [redacted]

PUBLICATIONS:NIL

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. **Critical flaw found in software used by many industrial control systems**
   CoDeSys, a piece of software running on industrial control systems (ICS) from over 200 vendors contains a vulnerability that allows potential attackers to execute sensitive commands on the vulnerable devices without the need for authentication, according to a report from security consultancy Digital Bond.
   References:http://www.computerworld.com/s/article/9232956/Critical_flaw_found_in_software_used_by_many_industrial_control_systems

Reference: http://www.zdnet.com/cybergeddon-now-industrial-control-systems-targeted-7000006491/

2. **DHS Warns of 'Hacktivist' Threat Against Industrial Control Systems**
The U.S. Department of Homeland Security is warning that a witches brew of recent events make it increasingly likely that politically or ideologically motivated hackers may launch digital attacks against industrial control systems. The alert was issued the same day that security researchers published information about an undocumented software backdoor in industrial control systems sold by hundreds different manufacturers and widely used in power plants, military environments and nautical ships.
Reference: http://krebsonsecurity.com/2012/10/dhs-warns-of-hacktivist-threat-against-industrial-control-systems/

3. **Google App Engine Back Up After Major Service Disruption – Dropbox and Tumblr Also Suffer**
A Google spokesperson said an "event" occurred this morning, which caused the load balancing issue. They are still looking into the root cause. They plan to post an incidence report.
References: http://thenextweb.com/insider/2012/10/26/major-sites-and-platforms-experiencing-outages-today-including-dropbox-and-google-app-engine/
http://internettrafficreport.com/namerica.htm
http://techcrunch.com/2012/10/26/google-app-engine-down-with-major-service-disruption-as-dropbox-and-tumblr-also-suffer/

4. **Windows 8 security focuses on early malware detection**
Security experts say Windows 8 is the most secure Microsoft OS to date, but that doesn't mean malware won't evolve to exploit it. In Windows 8, Microsoft has greatly improved the operating system's ability to detect malware before it has a chance to run, experts say. Windows 8 should also make it more difficult for people to unknowingly install malware in the first place.
Reference:http://features.techworld.com/security/3407482/windows-8-security-focuses-on-early-malware-detection/

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒

ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION: NIL

From: CYBERDO
Sent: Tuesday, October 30, 2012 4:06 PM
To: [redacted] CYBERDO
Subject: RE: Anonymous envisage des attaques contre le gouvernement fédéral

[redacted]

Luc

-----Original Message-----
From: [redacted] [mailto [redacted]
Sent: October-30-12 3:58 PM
To: CYBERDO
Subject: Anonymous envisage des attaques contre le gouvernement fédéral

Bonjour,

Une de nos collaboratricea nous a fait suivre cette information.

[redacted]

Le court article prétend que le Centre de la sécurité des télécommunications du Canada en est informé.

Bien que l'article date d'hier, je vous le transmet au cas où vous n'en auriez pas encore pris connaissance.

Merci de nous tenir au courant si ces attaques se concrétisent et débordent de notre côté.

Bonne fin de journée,

[redacted]

--

[redacted]

Pages 900 to / à 907

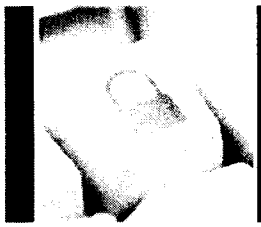
are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****
Date: 30 October 2012
CYBERDO: Bruce
****
[FOUO] NEW EVENTS:

1. Title: CE12-003882 [Zeus Infection – Financial Partner]
- Summary: CCIRC was notified by a vendor that they had information about possible Zeus infections affecting a financial institution.
- Action/Decision: Notification sent to a manager at the financial institution.
  - Owner: Ian
  - Status: Closed

2. Title: CE12-003883 [Increasing Traffic from [redacted]
- Summary: CCIRC received a request from an Energy client seeking advice that they could follow if a DDoS occurred.
- Action/Decision: Advice given to technical contact.
  - Owner: Patrick
  - Status: Closed

3. Title: CE12-003884 [Leaked Provincial Account Information]
- Summary: CCIRC was notified of a pastebin post that contained possible accounts of provincial government employees.
- Action/Decision: Notification sent to technical contact.
  - Owner: Ian
  - Status: Closed

4. Title: CE12-003886 [CIBC Phishing Sample – Financial Sector]
- Summary: CCIRC received CIBC phishing sample from a financial sector organization.
- Action/Decision: Analysis found the phishing domain was inactive.
  - Owner: Ian
  - Status: Closed

s.13(1)(b)
s.16(2)

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. CE12-003863 [#OpPartyCrasher Anonymous DDoS]

CRU scheduled for 1400 today. Purpose of this meeting is:

- validate the processes established within the IMP for escalation and reporting
- ensure that the roles and responsibilities as identified in the IMP are understood and respected

Escalation processes and procedures within the GC IT IMP will be reviewed, and the communication strategy for public reporting will be reviewed.

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. [redacted]

PUBLICATIONS:NIL

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. Malware hides behind the mouse

Malware samples use increasingly refined trickery to avoid being detected by automated threat analysis systems. Anti-virus company Symantec reports that it has found a trojan which attaches its malicious code to the routines for handling mouse events. Since nobody moves the mouse in an automated threat analysis system, the code will remain inactive, and the malware undetected.
Reference: http://www.h-online.com/security/news/item/Malware-hides-behind-the-mouse-1738577.html

2. Shift May Be Coming for Information Sharing on Attacks

The sharing of information on threats and attacks between government agencies and companies in the private sector has been tried numerous times and in many different ways over the last decade, with varying degrees of success. The need for information flowing in both directions likely is more pressing than ever right now,

with high-level attacks targeting critical infrastructure systems and utilities every day, but much of that data in the government realm remains classified and few enterprises are eager to reveal details, either. As the attacks continue, officials say there may be a need for a new mechanism to get the information flowing.
Reference: http://threatpost.com/en_us/blogs/shift-may-be-coming-information-sharing-attacks-102912

3. **Why Most Companies Are Fighting The Wrong Security Battle**
[...] Much of the money you are spending on computer security is focused on fighting the previous generation of threats, not the current ones that are the most dangerous that compromise over 95% of organizations. Aziz, who is founder, CEO and CTO of FireEye, which offers a solution that addresses the current style of attacks, presents a compelling case. What was even more interesting to me was the design of FireEye's solution, which combines aspects of machine learning and cloud computing into a system that gets better the more people use it. I believe that FireEye's architecture shows the way toward the next generation of applications and provides lessons that CIOs and CTOs can apply right away in areas outside of security.
Reference: http://www.forbes.com/sites/danwoods/2012/10/29/why-most-companies-are-fighting-the-wrong-security-battle/

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒

Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION: New CyberDO - Vireak

Clow, Patrick

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Tuesday, October 30, 2012 5:29 PM
To: CTEC
Subject: Update 6: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 30 October 2012
==========

==========
Update 6: 30 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

[redacted]

SUGGESTED ACTION
==========

[redacted]

Departments should implement the mitigation advice in GCCF12-008: DDoS campaign against the GC.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca.

From:
Sent: Wednesday, October 31, 2012 10:30 AM
To: Beaudoin, Luc
Cc: Anderson, Windy; Clow, Patrick; CYBERDO
Subject: CE12-003863 [DDoS]

Luc,

Pages 915 to / à 917

are duplicates of

sont des duplicatas des

pages 969 to / à 971

Turbide, Frank

From: Di Stefano Alain (NHQ-AC) <Alain.DiStefano@CSC-SCC.GC.CA>
Sent: October-31-12 5:03 PM
To: Beaudoin, Luc; Turbide, Frank
Subject: RE: événement courant

Excellent! LOL

Je ne m'attendais pas à une réponse aussi officielle à des commentaires informels. Merci de cette réponse officielle que j'ai bien su décoder.

A.

From: Beaudoin, Luc [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: Wednesday, October 31, 2012 4:57 PM
To: Di Stefano Alain (NHQ-AC); Turbide, Frank
Subject: RE: événement courant

Le coordonateur federal est GC-CTEC. CCIRC n a pas envoye de produit sur ce sujet autre une notification aux groupes potentiellement vise identifie sur pastebin. CCIRC n a aucune information liant les attaques recentes sur le federal au groupe anonymous. [redacted]

Pour plus d information sur les DDOS, vous pouvez consulter notre guide, disponible sur notre site web (google : DDOS CCIRC). N hesitez pas a consulter votre CERT governemental pour de plus ample renseignement.

Merci

Luc
CCIRC

From: Di Stefano Alain (NHQ-AC) [mailto:Alain.DiStefano@CSC-SCC.GC.CA]
Sent: October-31-12 4:45 PM
To: Turbide, Frank; Beaudoin, Luc
Subject: événement courant

Salut messieurs

Petite question et commentaires informels :

[redacted]

[redacted]

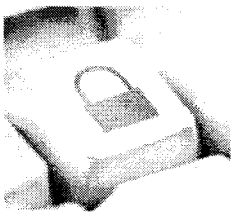
Toujours de façon informelle: il y a beaucoup de messages qui se ressemblent sur le sujet provenant de CTEC/CCIRC. Vous connaissez sûrement l'histoire du petit garçon qui criait au loup. Un moment donné, vous allez envoyer quelque chose d'important et on va le manquer.

Toujours de façon informelle et non officielle : le fait que les CIOs aient reçu un message de la CIO-B aura probablement créé un self inflicted DoS attack sur le GdC. On peut d'ors et déjà dire qu'ils ont atteint leurs objectifs. Sans oublier que tout ça n'était peut-être que diversion...

Finalement, avec la forte possibilité que l'événement courant soit coordonné, du moins en partie, [redacted] est-ce que quelqu'un a pensé à faire une attaque distribuée de déni de service sur ce service?

A.

OPERATIONAL SUMMARY
CCIRC Cyber Awareness Product



Weekly Technical Report

Issued: 31 October 2012

Volume 2012 - 43

DISCLAIMER

This publication is **UNCLASSIFIED - For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator. The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flash marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information, or Technical
- **Operational Summary:** Daily, Weekly, Monthly

NOTE TO READERS

CCAPs are available at the following website: http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx. If you have any questions, please contact the Public Safety Cyber Duty Officer @ [redacted] s.16(2)(c)

Traffic Light Protocol: RED: Designated for a specific audience/Non-sharable
AMBER: Sharable within organization on a need-to-know basis/Non-publishable
GREEN: Sharable within organization or community/Non-publishable
WHITE: Free to distribute

Table of Contents

Executive Summary

During the reporting period, the Canadian Cyber Incident Response Centre (CCIRC) handled 13 incidents, affecting partners in public and private sector organizations in the information and communications technology, finance, and energy sectors, and in federal and provincial governments.

CCIRC sent victim notifications to its partners in public and private organizations who were found to have hosts infected with malware, such as Zeus. CCIRC handled several phishing attempts, and provided mitigation advice to partners targeted by attempted and successful distributed denial-of-service (DDoS) attacks.

CCIRC regularly issues information products to inform its partners of potential, imminent or actual cyber threats. During the reporting period, CCIRC issued an Advisory (AV12-043 – *Security Update Available of Adobe Shockwave Player 4*) to its website.

Threat and vulnerability monitoring identified the Adobe detailed in AV12-043, and highlighted a new Cythosia Botnet 2.0 package.

This week's noteworthy news included the release of Trend Micro's *Q3 Security Roundup – Android Under Siege: Popularity Comes at a Price*, and highlighted the continuing DDoS attacks targeting United States (U.S.) financial institutions which began in September 2012, the newly launched Blackhole Exploit Toolkit 2.0, and a recent upswing in targeted phishing.

During the reporting period, the U.S. Department of Homeland Security's Industrial Control Systems Computer Emergency Response Team (ICS-CERT) released an Advisory and two Alerts, including an update to their February 2012 alert regarding the increasing threat to ICS.

CCIRC'S *INDUSTRIAL CONTROL SYSTEMS BEST PRACTICES*

In recognition of the risks facing industrial control systems, CCIRC recently published the *Industrial Control Systems Security Best Practice Guide*, which has been published to CCIRC's secure Community Portal and is also available upon request. The *Guide* includes an overview of the challenges and threats facing ICS owners and operators, and presents lessons from actual ICS security incidents.

Incident Reporting

This section contains information related to incidents affecting Critical Infrastructure in Canada.

1. CE12-003852 [Malware Notifications – Generic Botnets]

Hosts within these organizations were infected with Generic Botnet related malware. Notifications were sent to IT security or technical contacts in the following CI sector organizations:
Total IP count: 2472
Number of affected organisations receiving a notification: 116
Provincial: 3
Telecom: 87
Energy: 1
Health: 2
Academia: 23

2. CE12-003862 [EFax – Possible Zeus]

CCIRC received indicators from a trusted source of a possible Zeus hosted on Canadian domains. CCIRC is monitoring and researching.

Federal Government

1. CE12-003863 [#OpPartyCrasher Anonymous DDoS – Federal Department]

(CE12-003848).
(CE12-003854). Later CCIRC was notified
Anonymous DDoS attack planned against municipal, provincial and federal organizations. CCIRC sent notifications to municipal and provincial organizations. Federal organizations were notified by the federal CSIRT, including a series of product releases by the federal CSIRT.

Provincial and Territorial Government

1. CE12-003884 [Leaked Provincial Account Information]

CCIRC was notified of a pastebin post that contained possible accounts of provincial government employees. Notification was sent to security contacts at the affected provincial government organization.

Municipal Government

NIL

Information and Communication Technology

1. CE12-003856 [DDoS - Telecom]

CCIRC was notified by a Canadian telecom company that they had experienced a DDoS attack. The telecom company successfully mitigated the attack.

2. CE12-003860 [Malware Hosted - Telecom]

CCIRC was notified of malware being hosted on

Detection ratio: 9 / 42

Code Removal Request (CRR) sent to the hosting provider.

3. CE12-003865 [Malware Hosted - Telecom]

CCIRC was notified of malware being hosted on

Detection ratio: 26 / 44

CRR sent to the hosting provider.

4. CE12-003871 [Zeus p2p Activity - Telecom]

Finance

Energy and Utilities

1. CE12-003877 [Possible BHEK- Energy Sector]

CCIRC was notified by a trusted source of possible Black Hole malware hosted at CCIRC technical analyst confirmed there was a malicious obfuscated script on this site that would redirect users. This script creates a hidden iframe that redirects to the following site:

CCIRC sent a CRR to the hosting provider to remove the obfuscated script from forstereng[.]com. The malware/exploit site was already deactivated.

Transportation

NIL

Manufacturing

NIL

Health

NIL

Food

NIL

Water

NIL

Other (Academia)

NIL

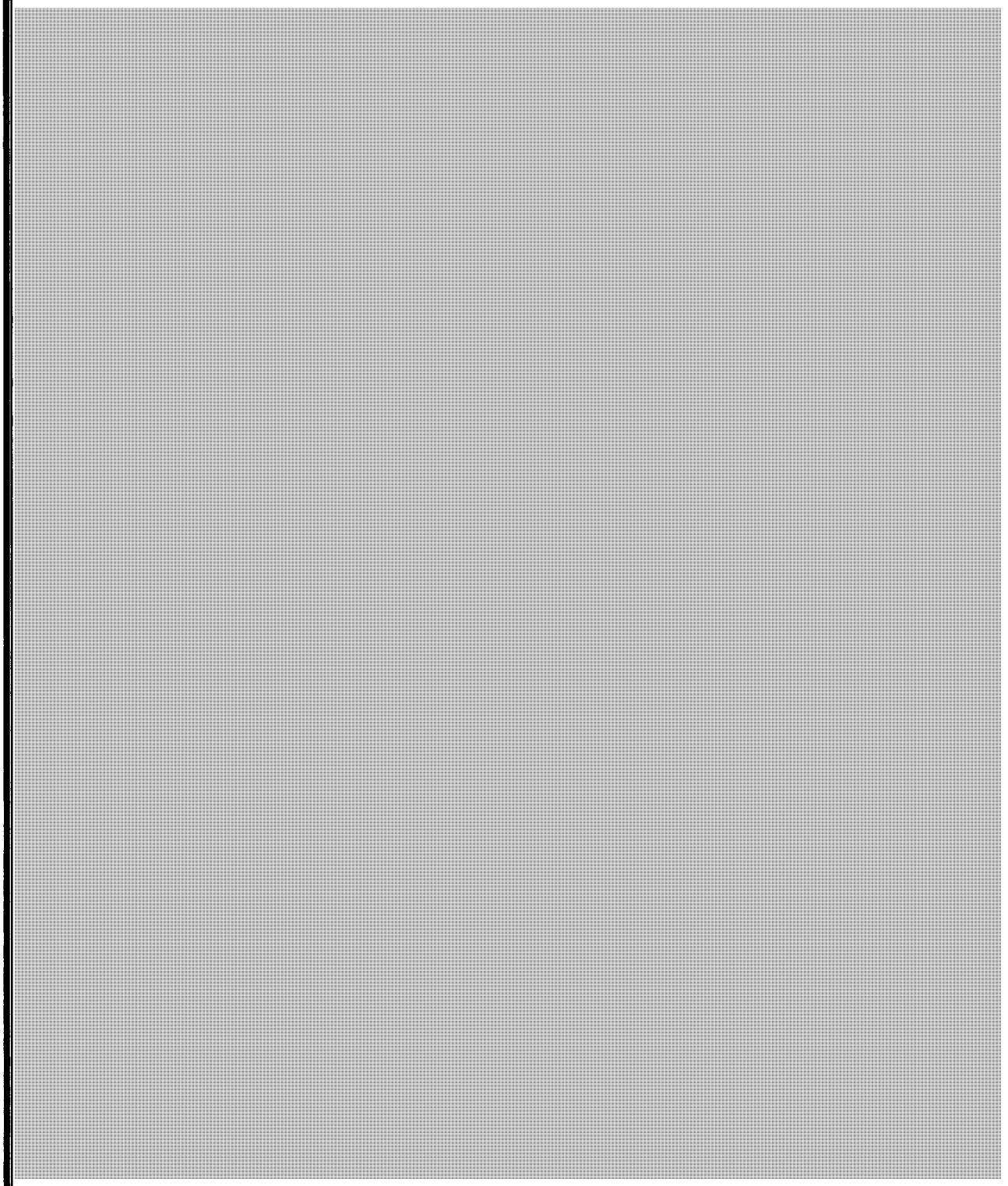
Other Organizations

NIL

Partners

Watch List

NIL



CCIRC Cyber Awareness Products

Alerts

NIL

Advisories

1. **CCIRC ADVISORY AV12-043: Security Update Available of Adobe Shockwave Player**
   Reference: http://www.publicsafety.gc.ca/prg/em/ccirc/2012/av12-043-eng.aspx

Information Notes

NIL

Technical Reports

NIL

Cyber Flashes

NIL

Threat and Vulnerability Monitoring

This section contains threats and vulnerabilities that did not meet the publication criteria for CCIRC products other than operational summaries. It is not meant to be an exhaustive list but rather a heads-up on potentially significant threats and vulnerabilities affecting technologies available to CCIRC communities of interest.

Vulnerabilities

1. **[Adobe Shockwave Player Multiple Vulnerabilities]**
   Multiple vulnerabilities have been reported in Adobe Shockwave Player, which can be exploited through buffer overflow or memory corruption to compromise a user's system. CVE-2012-4172 to 4176, and CVE-2012-5273. A vendor patch is available.
   Reference: http://www.adobe.com/support/security/bulletins/apsb12-23.html

Threat Watch

1. **[New Hack and Attack Tools Alert]**
   Cythosia Botnet v.2.0 Package
   UNCLASSIFIED / FOUO 2
   Detection rate 3/42 Tested with spynet,vertexnet,Xtreme,BlackShades
   Reference: hxxp://www[.]mediafire[.]com/?egho57vdq257u0f

SCADA/ICS

1. **ICS-CERT: ICSA-12-297-02 - Korenix JetPort 5600 Hard-coded Credentials**
   http://www.us-cert.gov/control_systems/pdf/ICSA-12-297-02.pdf

2. **ICS-CERT: ICS-ALERT-12-046-01A (Update) Increasing Threat to Industrial Control Systems**
   http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-046-01A.pdf

3. ICS-CERT: ICS-ALERT-12-097-02A (Update) 3S Software Codesys Improper Access Control

http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-097-02A.pdf
http://www.3s-software.com/index.shtml?codesys_dev_dir

Noteworthy News

1. How a Google Headhunter's E-Mail Unraveled a Massive Net Security Hole

"It was a strange e-mail, coming from a job recruiter at Google, asking Zachary Harris if he was interested in a position as a site-reliability engineer. [...]Harris was intrigued, but skeptical. He wondered if the e-mail might have been spoofed. Then he noticed something strange. Google was using a weak cryptographic key to certify to recipients that its correspondence came from a legitimate Google corporate domain. The problem lay with the DKIM key (DomainKeys Identified Mail) Google used for its google.com e-mails. DKIM involves a cryptographic key that domains use to sign e-mail originating from them – or passing through them – to validate to a recipient that the header information on an e-mail is correct and that the correspondence indeed came from the stated domain. When e-mail arrives at its destination, the receiving server can look up the public key through the sender's DNS records and verify the validity of the signature."
Reference: http://www.wired.com/threatlevel/2012/10/dkim-vulnerability-widespread/

2. Trend Micro Q3 security report

"Trend Micro has released the report "3Q 2012 SECURITY ROUNDUP -Android Under Siege: Popularity Comes at a Price" that presents a worrying trend for malware growth increased of 483%. The increment include cyber espionage malware and also destructive malicious agents targeting mainly the mobile world and in particular Google Android platform."
Reference: http://securityaffairs.co/wordpress/9672/cyber-crime/trend-micro-q3-security-report.html

3. An Overview of Exploit Packs (Update 17) October 12, 2012

"The long overdue Exploit pack table Update 17 is finally here. It got a colorful facelift and has newer packs (Dec. 2011-today) on a separate sheet for easier reading. Updates / new entries for the following 13 packs have been added."
Reference: http://contagiodump.blogspot.ca/2010/06/overview-of-exploit-packs-update.html

4. The 6th Week, Operation Ababil

"As you know, Operation Ababil is a retaliation in response of organized insulting to the Prophet of Islam done by some arrogant western governments. [...] Due to approaching Eid al-Adha and to commemorate this breezy and blessing day, we will stop our attack operations during the next days. Instead, we are going to have an interview with one of the American media and press about our ideas and positions."
Reference: http://pastebin.com/QWXkfPhG

5. New cybercrime monetization methods

" AVG's new report investigates a number of malicious software developments including the newly launched 2.0 version of the Blackhole Exploit Toolkit, the evolution in malware targeting

mobile banking services, a surge in malicious ads targeting social network users and a trick to hide malware inside image files."
Reference: http://www.net-security.org/malware_news.php?id=2303

6. The Michigan fight song and four other reasons to avoid Internet voting

" [...] Even more ambitious than the use of electronic voting machines in polling places would be to do away with the polling places altogether, conducting elections over the Internet. We didn't discuss this option in our previous piece because Internet voting has yet to catch on in the United States, but the topic crops up regularly in discussions (including in the Ars forums). So we thought it would be worthwhile to discuss five reasons it would be a big mistake to allow Americans to cast their votes online: Hacked servers, Client-side malware, Authentication, Coercion and bribery and Usability problems."
Reference: http://arstechnica.com/tech-policy/2012/10/the-michigan-fight-song-and-four-other-reasons-to-avoid-internet-voting/

7. IDF To Double Unit 8200 Cyber-War Manpower – OpEd

"The Israel's Channel 2 reports (Hebrew) that the IDF intends to double the manpower of its Unit 8200, which is charged with waging cyber-war on Israel's enemies. It plays a role akin to the NSA here in the U.S. and was responsible for creating Stuxnet, Flame and the other cyber-viruses which have decimated Iran's nuclear and oil facilities."
Reference: http://www.eurasiareview.com/24102012-idf-to-double-unit-8200-cyber-war-manpower-oped/

8. Phishing websites proliferate at record speed

""Phishers seem to be concentrating their efforts on compromising legitimate websites using automated attack tools, or purchasing access to them on the burgeoning underground market," said Rod Rasmussen, CTO of Internet Identity and co-author of the report. "This allows them to leverage the good reputation of a website's domain name, making it harder to block in either spam filters or via suspension, and makes takedown of that domain impractical."
Reference: http://www.eurasiareview.com/24102012-idf-to-double-unit-8200-cyber-war-manpower-oped/

9. Huawei offers Australia source code access

"Chinese telecommunications equipment manufacturer Huawei has offered the Australian government unrestricted access to its source code and hardware to appease fears of backdoors in its products, according to a BBC report. The Australian government had previously prevented the company from providing hardware for its national broadband network, citing concerns about the company's ties to the Chinese military."
Reference: http://www.h-online.com/security/news/item/Huawei-offers-Australia-source-code-access-1735921.html

10. SSL certificates and "the most dangerous code in the world"

"SSL is the de facto standard for secure, encrypted internet connections, but that security requires that a program validates the receiver's identity, specifically its SSL certificate. This is exactly where the researchers see a problem: in their study "The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software", they say that "SSL certificate validation is completely broken in many security-critical applications and libraries".
References: http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf

http://www.h-online.com/security/news/item/SSL-certificates-and-the-most-dangerous-code-in-the-world-1737168.html

11. Operation High Roller Banked on Fast-Flux Botnet to Steal Millions

"A fraud ring that attacked financial transfer systems in an attempt to get at wealthy high-end banking customers used a complicated web of malware and compromised servers in several countries to walk off with an estimated $78 million earlier this year. While the attacks targeted financial systems, the victims seem to be limited to companies involved in manufacturing, import-export businesses, and state or local governments."
Reference: http://threatpost.com/en_us/blogs/operation-high-roller-banked-fast-flux-botnet-steal-millions-102412

12. Attackers Turn to Open DNS Resolvers to Amplify DDoS Attacks

"Although DDoS attacks have been a serious problem for more than a decade now and security staffs have a good handle on how they're executed and how to handle them, attackers constantly adjust their tactics in order to defeat the best defenses available. One of the more recent tactics adopted by attackers is the use of open DNS resolvers to amplify their attacks, and this technique, while not novel, is beginning to cause serious problems for the organizations that come under these attacks."
Reference: http://threatpost.com/en_us/blogs/attackers-turn-open-dns-resolvers-amplify-ddos-attacks-102412

13. Critical flaw found in software used by many industrial control systems

"CoDeSys, a piece of software running on industrial control systems (ICS) from over 200 vendors contains a vulnerability that allows potential attackers to execute sensitive commands on the vulnerable devices without the need for authentication, according to a report from security consultancy Digital Bond."
References:
http://www.computerworld.com/s/article/9232956/Critical_flaw_found_in_software_used_by_many_industrial_control_systems
http://www.zdnet.com/cybergeddon-now-industrial-control-systems-targeted-7000006491/

14. DHS Warns of 'Hacktivist' Threat Against Industrial Control Systems

"The U.S. Department of Homeland Security is warning that a witches brew of recent events make it increasingly likely that politically or ideologically motivated hackers may launch digital attacks against industrial control systems. The alert was issued the same day that security researchers published information about an undocumented software backdoor in industrial control systems sold by hundreds different manufacturers and widely used in power plants, military environments and nautical ships."
Reference: http://krebsonsecurity.com/2012/10/dhs-warns-of-hacktivist-threat-against-industrial-control-systems/

15. Google App Engine Back Up After Major Service Disruption – Dropbox and Tumblr Also Suffer

"A Google spokesperson said an "event" occurred this morning, which caused the load balancing issue. They are still looking into the root cause. They plan to post an incidence report."

References: http://thenextweb.com/insider/2012/10/26/major-sites-and-platforms-experiencing-outages-today-including-dropbox-and-google-app-engine/
http://internettrafficreport.com/namerica.htm
http://techcrunch.com/2012/10/26/google-app-engine-down-with-major-service-disruption-as-dropbox-and-tumblr-also-suffer/

16. Windows 8 security focuses on early malware detection

"Security experts say Windows 8 is the most secure Microsoft OS to date, but that doesn't mean malware won't evolve to exploit it. In Windows 8, Microsoft has greatly improved the operating system's ability to detect malware before it has a chance to run, experts say. Windows 8 should also make it more difficult for people to unknowingly install malware in the first place."
Reference: http://features.techworld.com/security/3407482/windows-8-security-focuses-on-early-malware-detection/

17. Malware hides behind the mouse

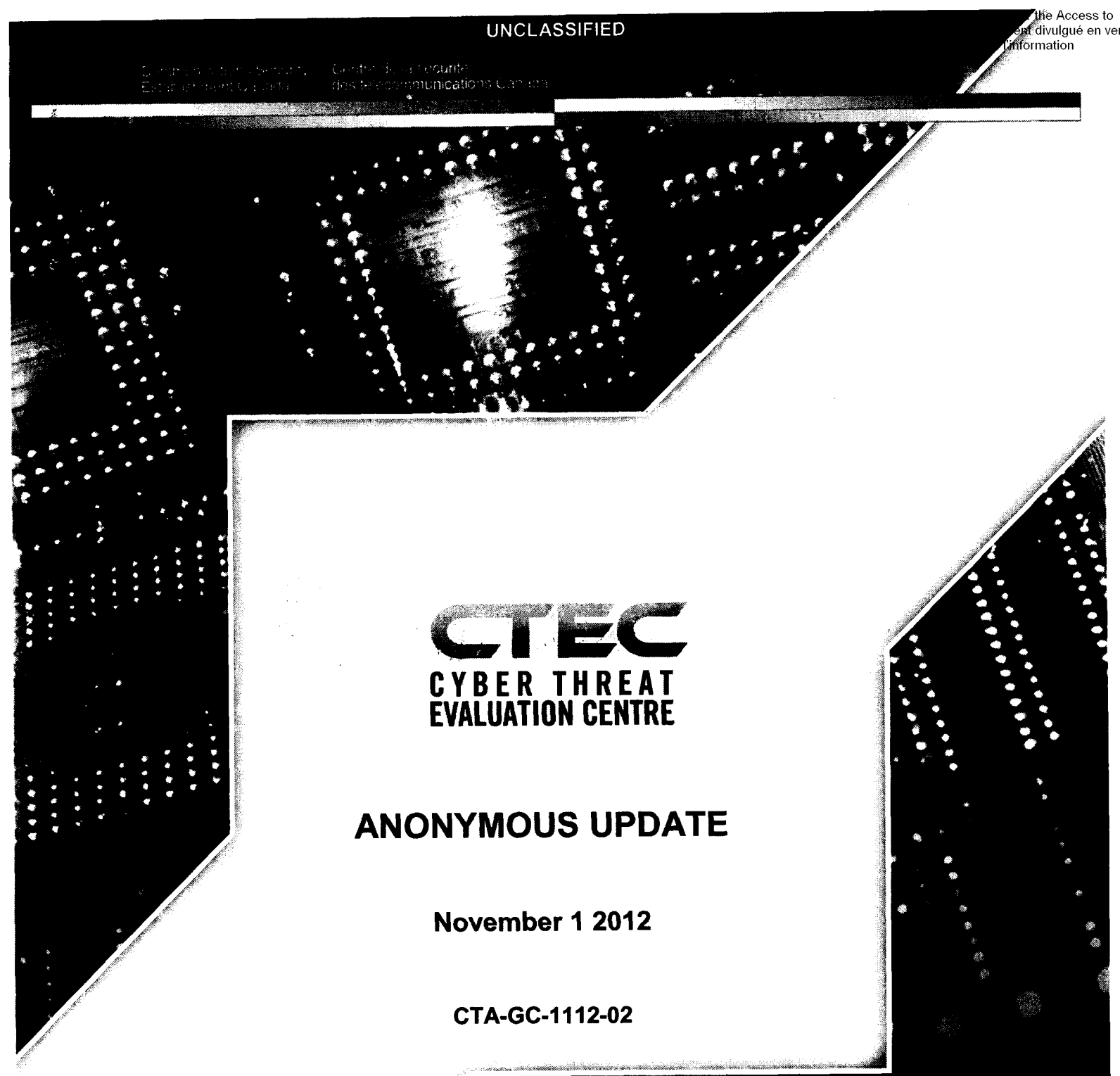
"Malware samples use increasingly refined trickery to avoid being detected by automated threat analysis systems. Anti-virus company Symantec reports that it has found a trojan which attaches its malicious code to the routines for handling mouse events. Since nobody moves the mouse in an automated threat analysis system, the code will remain inactive, and the malware undetected."
Reference: http://www.h-online.com/security/news/item/Malware-hides-behind-the-mouse-1738577.html

18. Shift May Be Coming for Information Sharing on Attacks

"The sharing of information on threats and attacks between government agencies and companies in the private sector has been tried numerous times and in many different ways over the last decade, with varying degrees of success. The need for information flowing in both directions likely is more pressing than ever right now, with high-level attacks targeting critical infrastructure systems and utilities every day, but much of that data in the government realm remains classified and few enterprises are eager to reveal details, either. As the attacks continue, officials say there may be a need for a new mechanism to get the information flowing."
Reference: http://threatpost.com/en_us/blogs/shift-may-be-coming-information-sharing-attacks-102912

19. Why Most Companies Are Fighting The Wrong Security Battle

"[...] Much of the money you are spending on computer security is focused on fighting the previous generation of threats, not the current ones that are the most dangerous that compromise over 95% of organizations. Aziz, who is founder, CEO and CTO of FireEye, which offers a solution that addresses the current style of attacks, presents a compelling case. What was even more interesting to me was the design of FireEye's solution, which combines aspects of machine learning and cloud computing into a system that gets better the more people use it. I believe that FireEye's architecture shows the way toward the next generation of applications and provides lessons that CIOs and CTOs can apply right away in areas outside of security."
Reference: http://www.forbes.com/sites/danwoods/2012/10/29/why-most-companies-are-fighting-the-wrong-security-battle/



CTEC
CYBER THREAT
EVALUATION CENTRE

ANONYMOUS UPDATE

November 1 2012

CTA-GC-1112-02

TABLE OF CONTENTS

The intended audience for this report is GC IT decision makers, security officers and technical practitioners.

EXECUTIVE SUMMARY

This report provides an update to the original Anonymous report (CTA-GC-1111-01) and includes: information on Anonymous's organizational structure, tradecraft, and targets, the threat to GC systems, and CTEC's prevention and mitigation advice.

- Anonymous has evolved to include local chapters in many different countries. These chapters support global Anonymous operations and conduct separate campaigns.

- Anonymous continues to target governments, private firms and individuals whose activities or purposes appear to be in conflict with principles espoused by the group. (Comment: For more information, please refer to the "Choosing Targets" section.)

- Based on a view of previous targeting by Anonymous, Government of Canada systems could continue to be a target due to:
  - continued government legislative initiatives that may be perceived as a violation of personal privacy (e.g. Bill C-12 *Safeguarding Canadians' Personal Information Act*).

- There are two upcoming operations that have been announced by Anonymous:
  - Operation Party Crasher: planned DDoS[1] attacks against a variety of Canadian Government institutions and political party websites.
  - Operation V: a peaceful demonstration in front of U.K. parliamentary buildings

- Anonymous typically uses a variety of open-source tools against its targets. These tools perform functions including DDoS, password cracking, SQL injections[2], reconnaissance activity, and email spamming.

- The "Mitigation" section includes mitigation and prevention advice to defend against tradecraft known to be used by Anonymous.

[1] A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users. Similarly, a denial-of-service (DoS) attack is the same type of attack that comes from a single source.

[2] An SQL server is a relational database server that can store and retrieve data across a network (e.g. the Internet). Queries from client machines are formatted in the SQL language. The majority of web-based sites use an SQL database.

STRUCTURE

With the infamy of the Anonymous group, local chapters have been developed in different countries, including in Canada. These local chapters conduct activities within their respective countries, as well as provide support for other Anonymous operations worldwide.

SELECTING TARGETS

Since Anonymous is decentralized and divided into many different chapters, new targets are determined in a variety of ways. In the past year, Anonymous has continued to select targets in response to perceptions of direct or indirect provocation by governments, by other hacking groups or security companies, or against the principles to which Anonymous adheres. Examples include:

- Protesting the arrest of former/current Anonymous members (Anons);
- Protesting against perceived internet censorship laws (such as SOPA[3], PIPA[4], etc.);
- Protesting against allegedly corrupt corporations and governments (as part of their continued AntiSec[5] campaign);
- Protesting against alleged government infringement of citizens` rights and freedoms (including privacy infringement);
- Protesting against defamation attempts against Anonymous[6];
- Protesting against cyber-bullying[7];
- Protesting against the neo-Nazi agenda; and
- Protesting against exploitation of children/minors.

COORDINATION

Anonymous, being a "loose coalition of Internet denizens[8]," uses a variety of means to coordinate attacks on selected targets. When an operation is called,

---

[3] *Stop Online Piracy Act* (SOPA).
[4] *Protect IP Act* (PIPA)
[5] AntiSec, or AntiSecurity is a key Anonymous raison d'être. It is the declaration of cyber warfare on governments and corporations in response to perceived corruption and Internet censorship.
[6] @FawkesSecurity was a Twitter identity claiming links to Anonymous who allegedly posted a video created by Anonymous stating that bombs had been planted in a government building in the USA. Anonymous formally denounced the allegations stating that they were not a terrorist organization and that it does not condone violence, but rather supports justice and universal equal rights.
[7] Anonymous attempted to disclose the identity of the perpetrator in the recent cyber-bullying case of a Canadian teenage victim. (http://www.dailymail.co.uk/news/article-2218532)

notices are briefly posted on internet sites and the operation hashtag (e.g. #OpPartyCrasher) is created and used on a variety of sites to coordinate their activities on services such as Twitter, Facebook, and VoxAnon[9].

PAST TARGETS/BEHAVIOUR

Anonymous has initiated cyber threat activities in protest of government decisions and in support of Anonymous's own principles. Its hacktivism[10] efforts have recently been concentrated on the various Occupy[11] movements, protesting Internet censorship and Internet filtering, protesting against oppressive regimes, and in retaliation against arrests of alleged Anons.

These hacktivism campaigns include:

2012

OPERATION ANAHEIM (USA)

- *Action*: Anonymous released personal information of some top officials within the Anaheim Police departments, including that of their police chief.
- *Reason*: To protest two fatal shootings in Anaheim, California. These actions were perceived by Anons as police brutality.

MEGAUPLOAD (USA)

- *Action*: DDoS attack against the websites of various US music-related organizations, the US Department of Justice, the US Copyright Office, the FBI, and HADOPI[12].
- *Reason*: To retaliate against the takedown action of the file sharing service Megaupload, the subsequent arrest of four Megaupload employees, SOPA and PIPA.

FBI/SCOTLAND YARD (USA and UK)

- *Action*: Anonymous posted an audio file of an intercepted confidential call

---

[8] James Harrison (February 12, 2008). "Scientology protesters take action around world". The State News (student newspaper) (Michigan State University). http://www.lansinglowdown.com/index.php/blog/entertainment/2008/02/internet_group__. Retrieved February 25, 2008.

[9] VoxAnon is an anonymous IRC Community created by Anonymous as a platform to facilitate private communications between members. hxxp://anonnews.org/press/item/1354/

[10] Hacktivism is a portmanteau of hack and activism. It refers to the usage of hacking as a means to protest or to promote political means.

[11] According to open source, the Occupy movement refers to an international protest movement directed against high unemployment, social and economic inequality and perceived corruption in corporations and government.

[12] HADOPI is the French anti-piracy agency.

between the FBI and Scotland Yard to YouTube. The call included sensitive information including law enforcement's tracking of hacktivist groups, dates of planned arrest and details of evidence held against them. Anonymous also published the email addresses of alleged call participants.
- *Reason*: Allegedly, to expose the FBI's poor security practices.

CENTRAL INTELLIGENCE AGENCY (CIA) (USA)
- *Action*: Sustained DDoS attack against the CIA's website which disabled the site for more than five hours.
- *Reason*: Anonymous claimed to have hacked into servers actively hosting child pornography and used them to DDoS the CIA website. Anonymous stated that CIA would have to take down the servers in order to stop the DDoS activity.

OPERATION BLITZKRIEG (Germany and USA)
- *Action*: Published email exchanges and personal messages between neo-Nazi organizations, as well as the names of their supporters and donors. In addition, Anonymous conducted web-defacement of neo-Nazi websites.
- *Reason*: To protest the neo-Nazi agenda.

ANONYMOUS CHINA (PRC)
- *Action*: The PRC chapter of Anonymous claimed that they had defaced five different PRC government websites. These web-defacements allegedly included links with tips on how to bypass state censorship and browse anonymously online. Anons also claimed to have leaked information from two or more PRC government websites.
- *Reason*: To protest against the Communist Party of China's alleged corruption.

APPLE UDID Leak (USA)
- *Action*: Anonymous allegedly leaked nearly one million Apple Device IDs supposedly taken from an FBI computer.
- *Reason*: To protest against government corruption and the FBI using device details for unknown agendas.

ONTARIO ASSOCIATION OF CHIEFS OF POLICE (Canada)
- *Action*: The usernames and passwords of several administrators' accounts and other personal information was stolen and published from the website of the Ontario Association of Chiefs of Police.

- *Reason*: To protest against Bill C-30 (*Protecting Children from Internet Predators Act*).

NORTON Antivirus suite (USA)

- *Action*: Anonymous posted source code of the 2006 versions of Norton Antivirus and Norton Utilities on the Pirate Bay[13].
- *Reasons*:
  - Likely in retaliation for Symantec's claims that Anons were victims of a ZeuS Trojan attack[14].
  - Possibly as a result of claims that Symantec refused to respond to extortion attempts by Anonymous.

OPERATION POLICIA (Spain)

- *Action*: DDoS attack against the official website of the Spanish police.
- *Reason*: To protest the arrests of suspected Anonymous members.

INTERPOL (UK)

- *Action*: DDoS of Interpol's website.
- *Reason*: To protest against Interpol's involvement with the arrests of 25 alleged Anonymous members in Europe and South America.

OPERATION INDECT (USA)

- *Action:* Web-defacement of a US company who are the experts in designing simple and portable flight control systems[15].
- *Reason:* To protest against the imprisonment of an American, an end to violence in Bahrain and Syria, opposition to worldwide Occupy protestors, INDECT[16], and to advocate for the closing of Guantanamo Bay.

MONDAY MAIL MAYHEM (USA)

- *Action*: Anonymous stole and published over 1.7 GB of data from the U.S. Bureau of Statistics, including internal emails.
- *Reason*: To protest against alleged government corruption.

OPERATION QUEBEC (Canada)

- *Action*: DDoS attack was launched against numerous Quebec government

[13] The Pirate Bay is a Swedish file-sharing website and allegedly one of the world's largest facilitators of illegal downloading.
[14] This would have been seen by Anons as an attempt to discredit or embarrass its members.
[15] Anonymous alleges that this company is a covert corporation funded by the CIA.
[16] INDECT is a joint research project of several European universities to automatically detect criminal threats through processing CCTV data streams. This is seen by Anonymous as a threat to personal privacy.

related websites (including the Education Department, the Ministry of Public Security, the Quebec coroner's office, the Quebec police ethics commission, the Montreal police force, etc.) and the Montreal Grand Prix website.
- *Reason*: To protest *An Act to enable students to receive instruction from the postsecondary institution they attend (*Bill 78[17]).

OPERATION Vic.Tory (#OpGreatWhiteNorth) (#OpKillBillz) (Canada):
- *Action*: As previously predicted in CTA-GC-1111-01, when the Canadian government reintroduced Lawful Access legislation (Bill C-30 *Protecting Children from Internet Predators Act* and Bill C-11 *Copyright Act*), requiring telecommunications companies to ensure intercept capabilities on their networks, Anonymous launched a smear campaign against the Canadian Public Safety Minister, demanding his resignation. In addition, Anonymous released the full names, emails and phone numbers of every federal MP who voted in support of Bill C-11 and they encouraged Canadians to contact these MPs to demand the resignation of the Public Safety Minister.
- *Reason*: To protest against perceived Internet censorship by the Canadian government, and to support the Vikileaks[18] campaign.

TELECOMMUNICATIONS COMPANIES (Australia)
- *Action*: Anonymous compromised servers of an Australian ISP and later stole and released 40 GB of partially redacted customer data.
- *Reason*: To protest alleged government censorship of its citizens and to protest the proposed package of reforms to four pieces of legislation: *The Telecommunications (Interception and Access) Act, the Telecommunications Act, the Australian Security Intelligence Organisation Act* and *the Intelligence Services Act.* If successfully passed, these acts would require ISPs to collect and retain data that would be passed over to law enforcement with the appropriate warrants.

OPERATION INDIA (India)
- *Action:* DDoS attacks against Indian government websites such as the Indian Supreme court, the All India Congress Committee, Copyrightlabs.in, the Department of Telecommunications and the Ministry of Information Technology.

[17] Bill 78 was passed in May 2012 to combat large-scale student protests in Quebec. This bill makes it illegal to assemble, protest or picket outside universities and colleges, or anywhere in Quebec with more than 50 people without prior police approval. This has been viewed by Anonymous as an attempt to impede constitutional rights.
[18] The Vikileaks Twitter campaign published was a smear campaign against the Canadian Public Safety Minister.

- *Reason:* To protest India's Internet censorship plan, which had resulted in the blocking of file-sharing and video-streaming websites (e.g. The Pirate Bay) in India.

Ongoing:

OPERATION #FFF (F*** the FBI FRIDAY) (worldwide)

- *Action*: Anonymous vowed to launch an online attack every Friday against allegedly corrupt corporate and government systems. Activities include web-defacement of the website of a supplier of police equipment and tactical gear. In addition, Anonymous conducted web-defacement of Infragard, a public-private partnership for critical infrastructure protection sponsored by the FBI.
- *Reason*: To protest against alleged government corruption.

OPERATION PEDOCHAT (OPERATION DARKNET) (worldwide)

- *Action*: Published IPs and email addresses of active users on child pornography forums.
- *Reason*: To protest against child exploitation. To attempt to purge child pornography from the Internet and to reveal the identities of those involved.

Upcoming:

OPERATION V (OPERATION VENDETTA) - Scheduled for 5 November, 2012

- *Action*: Proposed peaceful demonstration in front of UK Parliament buildings by acting out the final scene from the movie V for Vendetta[19]. Some members of Anonymous have also declared war on the US government. Details are not known.
- *Reason*: To protest against the US Cybersecurity Act[20], and to celebrate Guy Fawkes Day.

OPERATION PARTY CRASHER (#OpPartyCrasher) (Canada)

- *Action*: DDoS attacks against a variety of government institutions and the Provincial and Federal political party websites from 3 November 2012 to 15 November 2012. To exploit information about current Canadian cabinet members.

---

[19] In the final scene of the movie, a crowd enters Trafalgar Square, with each member wearing Guy Fawkes masks in front of the UK Parliament buildings.

[20] *The Cybersecurity Act of 2012* was a bill that sought to provide a framework to defend the US computer systems against cyber threats from foreign countries and from attacks on critical infrastructure. It granted companies the power to monitor user activity, retain user data and to share personal information of users with the government. It failed to pass the US Senate in August 2012.

- *Reason*: To protest against Omnibus Crime Bill[21] (C-10) and Bill C-30. To protest against perceived government infringement of citizens` rights and freedoms (e.g. CETA[22]) and to protest against the current Canadian Prime Minister.

Future Activity

Based on analysis of prior targeted campaigns by Anonymous, there is one government bill that would direct Anonymous' attention toward the Government of Canada.

Safeguarding Canadians' Personal Information Act (Bill C-12):

- This bill allows ISPs, email providers and social media websites to voluntarily share information about their subscribers with authorities and privacy security firms. It also prevents ISPs from telling customers that their personal details have been shared. (Comment: This could be seen by Anonymous as a violation of privacy. Similar perceptions have prompted Anonymous to take action against an Australian ISP.)

RETALIATION AGAINST ANON ACTIVITY

Reception for Anonymous activity has varied in the public eye. While there are many supporters of Anonymous, there are also those who oppose it. AnonNyre is a former member of anonymous who decided to help law enforcement uncover the identities of Anonymous members and drew attention to himself by DDoSing The Pirate Bay, a popular site that Anons use to publish stolen data.

Other hackers or hacking groups have been accused of targeting Anons. In May 2012, a US antivirus company claimed that an attacker changed the download link for a popular Anonymous tool Slowloris[23], replacing it with another version of Slowloris that was infected with ZeuS[24] to uncover Anons' financial banking and webmail credentials.

[21] Bill C-10, *An Act to enact the Justice for Victims of Terrorism Act and to amend the State Immunity Act, the Criminal Code, the Controlled Drugs and Substances Act and Conditional Release Act, the Youth Criminal Justice Act, the Immigration and Refugee Protection Act and other Acts.*

[22] Canada-European Comprehensive Economic and Trade Agreement.

[23] Slowloris is a DoS tool used by Anonymous.

[24] ZeuS is a popular malware that steals the victim's login credentials for social networks, email accounts, and online banking.

TRADECRAFT

As mentioned in previous reporting, Anonymous continues to use basic, effective, publicly-available or open source cyber-threat tradecraft against their targets. (Comment: The tools below do not represent a comprehensive list because Anonymous includes a large number of members and constituent member activities cannot all be tracked and attributed to Anonymous.)

Recent improvements in tools and communications have provided members with the means to better protect their identities while performing their operations to evade detection by law enforcement and other security personnel. Recommended tradecraft includes the combination of VPN technology with a proxy service to ensure that the IP or ISP originating the attack is not revealed during any activities.

Open Source resources:

Less-attributable services:

Anons use the following services in an attempt to hide their online activities:

1) Virtual Private Network (VPN):
In order to improve security, VPNs use tunneling protocols and other security procedures (e.g. encryption) to provide confidentiality and message integrity for their users. Anon is known to use "ipredator.se" or "HotspotShield.com"

2) Proxy:
Proxies mask the IP address, location and identity of the user, making it easy to conduct illicit online activities anonymously. Anons are known to proxy through hxxp://spys.ru/en/ or to use the popular service known as "The Onion Router (TOR)."

Port Scanners:

Port Scanners are used to probe a server or host to check for any open ports. This may be used for reconnaissance activity to find known vulnerabilities within the victim's host. Examples of port scanning tools used by Anons include Acunetix WVS[25], Nikto[26], and Havij[27].

[25] Acunetix scans websites for vulnerabilities such as SQL injections, Cross Site Scripting, etc.
[26] Nikto is an Open Source web server scanner which checks for dangerous files, outdated servers, and incorrect server configurations.
[27] Havij is an automated SQL injection tool that finds and exploits SQL Injection vulnerabilities on a web page.

DoS/DDoS:
Anonymous' usual method of choice is to launch DoS/DDoS attacks against a target's website in an effort to bring the host offline and to make the website unavailable to legitimate users. Two commonly used methods include:

1) Slowloris/Pyloris2:
Both Pyloris2[28] and Slowloris are utilized by Anons to send incomplete HTTP headers to the webservers in order to keep connections open. These continuous open connections will overwhelm the server and are more effective than sending thousands of complete HTTP requests.

2) High Orbit Ion Cannon (HOIC):
Anons are encouraged to download and launch the High Orbit Ion Cannon (HOIC) application, enabling them to willingly participate in a botnet. The HOIC is an improved variant of the Low Orbit Ion Cannon (LOIC). It is pointed at a target of choice, which would then disrupt the service of the victim's host. It has improved randomization of spoofed sources and has multi-threaded capability to vastly increase the severity of the attack. In addition, users can download various booster packs, including scripts that specifically target government websites.

3) Web Hive:
Web Hive is a tool that will allow the Anonymous user to specify a target, a URL, the number of requests per second and the message to be contained in the request (e.g. "We are Anonymous.") This will overwhelm a target when attempting to respond to the flood of seemingly legitimate requests.

4) Open Web Application Security Project (OWASP) HTTP Tool:
The OWASP HTTP tool was originally developed to assist penetration testers in DoS testing. It is a basic HTTP DoS tool that sends thousands of GET requests to the webserver to continuously use up resources.

5) HPING v.2, v.3:
HPING is a network tool which is able to send custom TCP/IP[29] packets. It is able to test firewall rules and conduct advanced port scanning. HPING3 is the improved version of HPING2 and is able to generate arbitrary TCP/IP packets.

[28] Pyloris2 is the updated version of Slowloris.
[29] Transmission Control Protocol/ Internet Protocol (TCP/IP) is one of the basic communication languages of the Internet.

6) PenTBox:
PenTBox is a security suite that contains security and stability-testing oriented tools for networks and systems, such as TCP Flood DoSer, TCP Flood AutoDoSer and spoofed SYN Flood DoSer. It is compatible with Linux and Windows systems.

7) DDOSIM:
DDOSIM simulates zombie[30] hosts with random IP addresses that create full TCP connections to a target server. It is able to conduct application layer DDoS attacks and other TCP based attacks.

Although these tools are used for denial of service, with the operation parameters containing a time and targets, it becomes a distributed denial of service attack through volume of participants in the operation.

Other:

Other techniques used by Anonymous include the usage of "comment flashmobs" on Facebook pages to flood the page with pre-scripted messages. This is often conducted by Anons in protest of perceived defamation attempts[31]. In addition, Anons are known to use password cracking tools to exfiltrate data from a victim's database, and to use email spamming tools such as Mess Bomber to email spam victims.

Anonymous-developed tools:

DoS/DDoS via SQL Injections:

#RefRef:
Anonymous appears to have continued its usage and development of the Perl DDoS tool #RefRef that exploits SQL vulnerabilities. This tool is a Perl script that takes advantage of a function built into MySQL and repeatedly sends a command that will use the server's own resources against it. This will eventually overwhelm the server.
As mentioned in the previous report, #RefRef could be used in combination with tools such as Havij, an SQL Injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities. As a result of SQL vulnerability exploitation, database content could be changed, or database information (e.g. user credentials or credit card information passwords) could be stolen.

---

[30] A zombie is a computer that has been previously compromised by malicious software and can be used to perform additional malicious tasks under remote direction.
[31] For example, Facebook pages run by a well-known newspaper company were the target of a spam attack by "The Anonymous Kollektiv" because they had allegedly equated Anonymous with Al-Qaeda in one of their published articles.

MITIGATION

This mitigation section contains an update to the original mitigation advice as well as points that are still valid from the previous report.

Since Anonymous continues to have a wide target set, it is difficult to measure which vulnerabilities are most frequently exploited by the group. However, as noted, the threats leveraged are generally limited to open source or well-known vulnerabilities. As a result, strong IT security practices will aid in defending and mitigating against an Anonymous cyber threat.

In addition to best practices, including the implementation of CTEC's "Top 35 Mitigation Actions", the following mitigation is available for some of the tradecraft specifically noted above:

1. DoS/DDoS mitigation
    a. Use network segmentation and segregation into security zones to protect high value assets using routers to spot and drop DDoS connections. For more information, please refer to number 16 of the "Top 35 Mitigation Actions."
    b. If the DDoS is pointed at a specific IP, the target site could be blackholed. This typically requires working with upstream network providers to forward malicious traffic to a non-existent network interface, where the offending traffic will be dropped.
    c. In some cases, if a DDoS is anticipated, it may be possible to temporarily have additional bandwidth provisioned to your network. This will lessen the impact on the target for some DDoS incidents.

2. SQL injection prevention
    a. Webcode should be hardened[32] against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users.
    b. In cases where dynamic queries are necessary for defense or legacy reasons, user input should be sanitised to prevent the SQL server from executing database functions. Examples of database functions include deleting data, accessing unauthorized data, etc.

3. Firewall Configuration
    a. Configure all firewalls to fail close[33]. In cases where the firewall

[32] Hardening minimises access between the public facing HTTP server and the SQL database. It also validates requests sent by external clients to the HTTP server.

defaults to fail open, all network traffic will be allowed into the internal network without any protection. This allows the attacker to gather sensitive information about the victim's network infrastructure, such as the number of devices connected to a network, names of servers, services utilized by the network, etc.

4. HOIC
   a. Analysis of HOIC-related traffic indicates that there is a potential for anomalies in the server requests that are sent. Creation of Intrusion Detection System (IDS[34]) signatures to block this type of traffic may reduce the amount of DoS activity reaching the victim's server.

Please see CTEC report "Government of Canada Top 35 Mitigation Actions, January 2012" for further information.

[33] When a firewall crashes, fail close will disable all network connectivity.
[34] An IDS is a software application or device that monitors networks for malicious or abnormal activities.

Page 948

is a duplicate of

est un duplicata de la

page 964

Pages 949 to / à 963

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Thursday, November 01, 2012 1:27 PM
To: george.pelletier@ssc-spc.gc.ca; CYBERDO
Cc: NA-IITB-DGIIT-DIST-IPC-CPI@hrdc-drhc.net; CTEC
Subject: RE:

Classification: UNCLASSIFIED

Good afternoon George,

Thank you for passing this information onto us.

Cheers,

GC-CTEC Cyber Duty Officer
Cyber Threat Evaluation Centre
CTEC@CSE-CST.GC.CA

-----Original Message-----
From: george.pelletier@ssc-spc.gc.ca [mailto:george.pelletier@ssc-spc.gc.ca]
Sent: November 1, 2012 9:30 AM
To: CTEC;
Cc: NA-IITB-DGIIT-DIST-IPC-CPI@hrdc-drhc.net
Subject:

Good Morning CTEC and CyberDO Teams,

You have probably already seen this

Sincerely,

George E. Pelletier, CISSP, GCIA
Centre de la protection de l'information (CPI) / Information Protection Centre (IPC) Services de la sécurité en TI (SSTI) / IT Security Services (ITSS) Réseaux et opérations de sécurité de la TI (ROSTI) / Networks and IT Security Operations (NITSO)
Shared Services Canada / Services partagés Canada T (613) 954-3571 C (613) 266-4073 F (613) 960-9304
george.pelletier@ssc-spc.gc.ca

From: [redacted] <[redacted]@CSE-CST.GC.CA>
Sent: Thursday, November 01, 2012 1:35 PM
To: Anderson, Windy
Cc: Beaudoin, Luc; Moore, Bruce; [redacted] CYBERDO
Subject: RE: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

Windy, CTEC will continue to release daily Information Notes on the Anonymous DDoS activity against GC until further notice. Also, they will be releasing cyber flashes to assist with ongoing mitigation efforts as required.

I'll provide details at the brief tomorrow.

[redacted]

-----Original Message-----
From: Anderson, Windy [mailto:Windy.Anderson@ps-sp.gc.ca]
Sent: November 1, 2012 12:11 PM
To: CYBERDO
Cc: [redacted]
Subject: FW: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Oh My Goodness,

Robert still wants us to try to get the information. I will just send it to him. Sorry guys.

Have a great day,

Windy
Director Canadian Cyber Incident Response Centre Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097 windy.anderson@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Dick, Robert
Sent: November-01-12 12:02 PM
To: Anderson, Windy
Subject: Re: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Good. Keep trying to get the email notwithstanding the last email you were cc'd on. But just give it to me.

----- Original Message -----
From: Anderson, Windy
Sent: Thursday, November 01, 2012 11:38 AM
To: CYBERDO
Cc: @CSE-CST.GC.CA) CSE-CST.GC.CA>; Dick, Robert
Subject: FW: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Bruce,

Can you please talk to SSC/CSEC to get their updated plan? SSC seems to have a plan in place - can we just get a short description on what they plan to do. Thanks.

Also - if you are talking to SSC - any chance we can get an update from them by 8:15 or 8:30 each day on this event until it has wound down? And, then you guys can pass that to me? Much appreciated.

Have a great day,

Windy
Director Canadian Cyber Incident Response Centre Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097 windy.anderson@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Wong, Suki
Sent: November-01-12 11:32 AM
To: Dick, Robert
Cc: Baulne, Lucie; Anderson, Windy
Subject: Re: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Noted. Pls prepare a short description of preparation activities for Nov 3 (bf cob today). Also pls ensure that I receive (cc. Lucie) a daily (9:00am) update going forward (until incident is no longer considered a concern. Happy to discuss further.
Tx

----- Original Message -----
From: Dick, Robert
Sent: Thursday, November 01, 2012 11:15 AM
To: Wong, Suki
Cc: Baulne, Lucie; Anderson, Windy
Subject: Re: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

s.16(2)

Csec didn't show up for the meeting. As far as we know, there's no change in status on this

----- Original Message -----
From: Wong, Suki
Sent: Thursday, November 01, 2012 10:59 AM
To: Dick, Robert
Cc: Baulne, Lucie
Subject: Fw: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Pls follow up. Tx

----- Original Message -----
From: Anderson, Windy
Sent: Thursday, November 01, 2012 08:25 AM
To: Wong, Suki; Dick, Robert
Cc: Baulne, Lucie
Subject: RE: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

This is all we have received from them but CTEC will be here at 8:30 for our morning brief. As will Shared Services Canada.

Will not have any updated information until after 9:00 (when the briefing is over). Sorry.

Have a great day,

Windy
Director Canadian Cyber Incident Response Centre Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097 windy.anderson@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Wong, Suki
Sent: November-01-12 8:23 AM
To: Anderson, Windy; Dick, Robert
Cc: Baulne, Lucie
Subject: Re: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Tx. Since the Update does not refer to level of activity or health of network, should I assume there is no change from the update I received 2 days ago? Tx

----- Original Message -----
From: Anderson, Windy
Sent: Wednesday, October 31, 2012 07:12 PM
To: Wong, Suki; Dick, Robert

Subject: Fw: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Update for tomorrow am

Windy

----- Original Message -----
From: CYBERDO
Sent: Wednesday, October 31, 2012 04:26 PM
To: Anderson, Windy
Subject: FW: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

FYI,

Vireak

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: October-31-12 4:03 PM
To: CTEC
Subject: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 31 October 2012
==========

==========
Update 7: 31 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
==========

[redacted]

Departments should implement the mitigation advice in GCCF12-008: DDoS campaign against the GC.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Thursday, November 01, 2012 4:36 PM
To: Beaudoin, Luc; CYBERDO
Cc: Breault, Stephen; CTEC
Subject: [CE2012-1289] RE: Op PartyCrasher: potential change of MO

Classification: UNCLASSIFIED

Appreciate the notice Luc. We've noted it in our ticket and verify if there's anything new.

GC-CTEC - Cyber Duty Officer

From: Beaudoin, Luc [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: November 1, 2012 2:27 PM
To: CYBERDO; CTEC
Cc: Breault, Stephen
Subject: Op PartyCrasher: potential change of MO

FYI
http://pastebay.net

////

1. #OpPartyCrasher

2.

3. Greetings, fellow Anons, Hacktivists, Activists, and The People.

4.

5. What will it take, to get you to realize? As you may or may not know, recently the Conservatives released their Omnibus Budget, which threatens many areas of everyday Canadian life. The Navigable Waters Protection Act threatens Canada's waterways, the rules weaken environmental protection for these waterways, and could limit access to lakes, rivers, and streams. The Bridge to Strengthen Trade Act, two billion dollars to build a bridge from Michigan into Ontario. The Canada Labour Code changes make it harder for employees to report discrepancies older than 6 month. The Canada Employment Insurance Financing Board Act changes allow the Minister of Finance and Minister of Human Resources to set the rate of EI in Canada, dissolving the past board (CEIFB). Merchant Seaman Compensation Board has been cut giving responsibility to the Minister of labour. Bill C45 is also damaging the Indian Act and the Fisheries Act. Stephen Harpers constant disregard of the Canadian People, Our Environment, Education, Science, Privacy, and most of all Free Speech will no longer be tolerated in Canada, whether it be Online or in the Real World. Stephen Harper is destroying the image of Canadians across the globe.

We must stop the sell out of Canada, and start to put people ahead of profit. Vic Toews has set aside 155 million dollars for cyber security, and is using this to black ball the Anonymous idea. Toews is quoted saying Anonymous is a threat to Democracy, and a threat to the security of all Canadians. The widespread corruption recently exposed within Quebec around the Construction Industry has many Federal ties, we are demanding a Public Inquiry into how deep this corruption goes and across what industry. We also demand Public Inquiry into Nathan Jacobson and his Business and Political Associates. This is the end, of injustice. This is the end, of tyranny, this is the end, of #OpPartyCrasher is here to dismiss Mr. Toews heinous allegations, and to open the eyes of the Canadian public to what we have to lose. Are more budget cuts, corporate bailouts, and corporate tax subsidies really what Canada is about? Fight now, to save the Canada we know and love, not just for ourselves but for every generation to come. We've only got one chance, one land for us to keep and the one we are leaving for our children is going downhill, very steep. Voices of reason are being drowned by insanity. Stephen Harper is leading Canada into the dark, it's time the people light our own torch. What do they have to do before you stand up? Do they have to regulate every activity you want to participate in, before this becomes real? It's real NOW, the time to stand up is NOW. When no one is left to keep fighting you'll ask what can I, do? This will be the end of our existence as we know it, if we continue to barrel down this path. Total destruction, if we ignore the warnings. Our time is running out. Stand with us before it's too late Canada. #OpPartyCrasher will commence on November 3 and last until November 7. Stephen Harper, We will no longer comply with your dictative rule over Canada, your time has come. Expect Us.

6.

7. So, Here's what we'll do;

8.

9. On November 3 2012 we will #TwitterBomb @pmharper with tweets containing #STOPHarper and #OpPartyCrasher making them #TT for maximum exposure. As well on November 3 2012, any Canadian Bank Note (Dollar Bills) you come into contact with from now until November 30 2012 write; #OpPartyCrashe in bottom left corner and #ExpectUs On the bottom right. We will place attacks on Nov 3 (12p.m. to 6p.m.), 4 (12p.m. to 6p.m.), 6 (6p.m. to 10p.m.), 7 (6p.m. to 10p.m.), 8 (6p.m. to 10p.m.), 9 (6p.m. to 10p.m.). Revised Targets and Boosters will be released on the day of attack, one hour before.

10.

11. Tweet - Dear @pmharper, We warned you before, #ExpectUs. You should have listened

12. #STOPHarper #OpPartyCrasher

13.

14. Tweet - Dear @pmharper, We are here to stop the #Globalization of #Canada

15. #STOPHarper #OpPartyCrasher

16.

17. Tweet - Dear @pmharper, We have come to crash your #Capitalist party.

18. #STOPHarper #OpPartyCrasher

19.

20. Tweet - Dear @pmharper, We put you in power, and we will take you out. #STOPHarper

21. #OpPartyCrasher

22.

23. Tweet - Dear @pmharper, #Canada isn't yours to do with as you please. #STOPHarper

24. #OpPartyCrasher

25.

26. Make your own tweets too.

27. OPEN LETTER TO THE CANADIAN GOVERNMENT

28. We have watched as you have violated the very laws that guarantee your power. We have witnessed your fall from Representatives of the People to Representatives of Greed and Corruption.

29. We've been watching you systematically destroy the rights of your own people, one law at a time. No longer shall we stand by and watch you enslave our fellow citizens.

30. You have continued down this path of treason by creating acts such as the EU-Canada trade agreement C.E.T.A., Bill C-10, Bill C51, and more. You've tried to conceal the true purpose of these bills, and pass them without the consent of the Canadian people.

31. We are now here to undo your sordid life's work in its entirety. No longer will your transgressions go unnoticed. No longer will you enslave the people. The world will know of your violations against the rights of the citizens you were elected to represent.

32. The eyes of the people are open. We see your hunger for power, and money. You label those with voices that speak against you as terrorists, and vilify true freedom in the process.

33. This is a warning for anyone who thinks they can make a profit off the people without repercussions. We will not stand silently and allow you to enslave our country. We will not comply.

34. This is the Canadian Charter of Rights and Freedoms. Every time you violate this Charter we will ensure the people are aware of your actions. You may have previously succeeded in concealing your actions, but that time has come to an end. You were elected by us, and you will be removed by us.

35. See http://pastebin.com/6P3i40wb For Canadian Charter of Rights and Freedoms

36. We suggest printing off and sending to you local MP, or emailing it to them. This letter is open, to the Canadian Government, all sides whether Conservative, Liberal, NDP, Bloc Qbc, Green Party, or an independent politician, you do wrong by the people you were elected to represent and we will find you. To the police who are paid to Serve

and Protect the people and not the corporation, your corrupt ways will end. We are here, and we are many. You may have money, and power but we can see through the deceit and disinformation, this end now.

37. We are Anonymous,

38. We are Legion,

39. We do not Forgive,

40. We do not Forget,

41. Stephen Harper and the corrupt elite ruining Canada,

42. Expect Us.

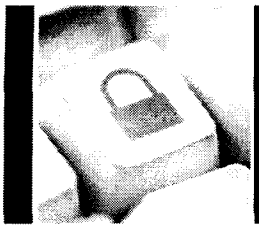
43. #OpPartyCrasher

44. #OpFuckHarper

////

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Public Safety Canada | Sécurité publique Canada



CCIRC
Canadian Cyber Incident Response Centre

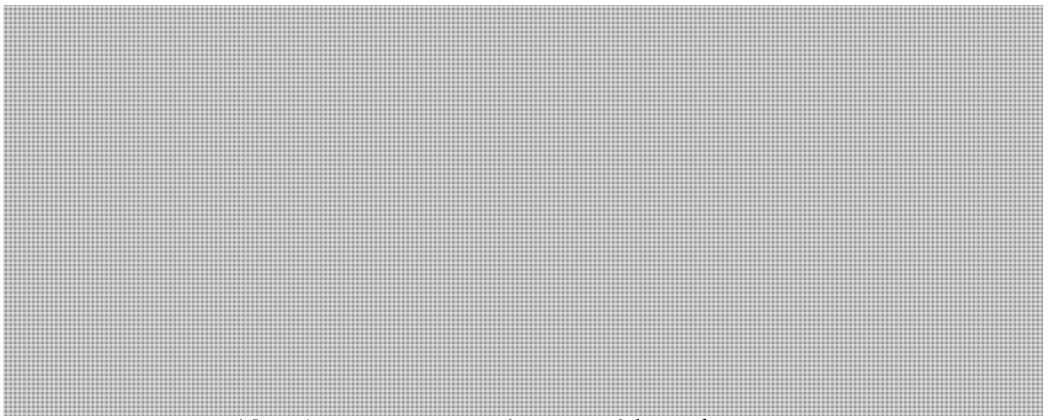
BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****
Date: 2 November 2012
CYBERDO: Vireak
****

[FOUO] NEW EVENTS:

1. Title: CE12-003907 [Notifications - Zeus]
- Summary: CCIRC was notified that the following organizations may contain hosts infected with Zeus related malware.
  Total IP count: 1567
  Number of affected organisations receiving a notification: 97
  Provincial:1
  Telecom: 68
  Energy:4
  Transportation: 1
  Manufacturing & Retail:3
  Health:1
  Academia(all): 19
- Action/Decision: Notifications sent to IT or technical contacts.
  - Owner: Steve
  - Status: Active

2. Title: CE12-003909 [SpyEye Command and Control]
- Summary: CCIRC was notified of a domain being used for SpyEye Command and Control.



- Action/Decision: Notification sent to Hosting Providers abuse contact.
  - Owner: Chris
  - Status: Active

Canada

3. Title: CE12-003910 [Notifications - Flashback]
- Summary: CCIRC was notified that the following organizations may contain hosts infected with Flashback related malware
  Total IP count: 588
  Number of affected organisations receiving a notification:54
  Provincial:2
  Municipal:
  Telecom: 37
  Academia(all): 15
- Action/Decision: Notifications sent to IT or technical contacts.
  - Owner: Steve
  - Status: Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. Title: CE12-003829 [BBB Complaint Form Malware]
- Summary: Energy sector company has identified infected hosts. They will provide CCIRC with updated malware samples.
- Action/Decision: Additional analysis pending receipt of malware sample.
  - Owner: Bruce
  - Status: Active

2. Title: CE12-003863 [#OpPartyCrasher Anonymous DDoS]
- Summary: Federal Partners are reviewing their monitoring and escalation processes in preparation for the weekend. As well, members from the Federal CSIRT will be on site to provide support. During recent analysis a Federal Partner noticed [redacted]
- Action/Decision: CCIRC will aid in anaylsis and assist Federal Partners where necessary.
  - Owner: Bruce
  - Status: Active

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. [redacted]

2. [redacted]

3. [redacted]

4. **ICS-CERT - ICSA-12-271-01—C3-ILEX EOSCADA MULTIPLE VULNERABILITIES**
   Dale Peterson of Digital Bond has identified multiple vulnerabilities in the C3-ilex's EOScada application that can result in data leakage and a denial-of-service

(DoS) condition. C3-ilex's has produced a patch that resolves these vulnerabilities.
Reference: http://www.us-cert.gov/control_systems/pdf/ICSA-12-271-01.pdf

PUBLICATIONS:

1. **CF12-017 - Better Business Bureau Phishing Emails Using P2P Zeus Malware Variant**

VULNERABILITY WATCH:

1. **Vulnerabilities in Apple Safari (Webkit)**
A security researcher reports that use-after-free and race condition vulnerabilities exist in webkit which may be exploited by luring an affected client to a crafted webpage to execute arbitrary code and compromise the system. The vendor has released a patch. CVE-2012-3748 CVE-2012-5112.
Reference: http://secunia.com/advisories/51157/
http://secunia.com/advisories/51157/
http://securitytracker.com/id/1027716
http://support.apple.com/kb/HT5568

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS:

1. **Malwasm – Malware Reverse Engineering Tool**
Malwasm is a tool based on Cuckoo Sandbox. Malwasm was designed to help people that do reverse engineering. Malwasm step by step:
•the malware to analyse is executed through Cuckoo Sandbox
•during the execution, malwasm logs all activites of the malware with pintool
•all activities are stored in a database (Postgres)
•a web service is available to visualize and manage the data stored in the database
Reference: http://code.google.com/p/malwasm/

CYBER NEWS:

1. **The shortcomings of anti-virus software**
No, this isn't about lousy detection rate. I think we're pretty much resigned to that, irrespective of the latest fancy marketing terms the industry uses to sell us the same failed concept. This is about the forensic quality, or rather lack thereof, of anti-virus. [...] Increasingly now, anti-virus alerts us (maybe) to a persistent threat that has been on the system for days, weeks, heck, even months. And deleting or quarantining such a threat causes a serious problem: It modifies or eradicates evidence. Yes, we get an alert, but then we are like the CSI guys who get called to a murder scene that doesn't have a body. Sure we can spend hours trying to lift DNA off cigarette stubs, but things would be so much easier if the caller could tell us what exactly he has seen where, and where the body was?
Reference: http://isc.sans.edu/diary.html?storyid=14437

2. **Feds need to add regulations to force Canadians to think about cyber-security, experts say**

One day after a top Tory senator suggested the government and Canadians didn't want more regulations on how we use cyberspace, a former British spy chief said that thinking needed to be deleted.

Governments need to possibly create more red tape to force companies and individuals to think about cyber-security because too few are doing enough to protect themselves and others from cyber-threats, Sir David Pepper told a security conference Wednesday in Ottawa.

Reference:
http://www.calgaryherald.com/news/national/Feds+need+regulations+force+Canadians+think+about+cyber/7478557/story.html

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒

Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION: NIL

Pages 981 to / à 984

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Page 985

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Page 986

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Page 987

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Page 988

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Page 989

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Page 990

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Page 991

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

From:
Sent: Friday, November 02, 2012 10:28 AM
To: 'CTEC <CTEC@CSE-CST.GC.CA> (CTEC@CSE-CST.GC.CA)'
Cc: CYBERDO
Subject: FW: CE12-003863 [Oppartycrasher)
Attachments:

-----Original Message-----
From: Bergeron, Dominic
Sent: November-02-12 10:19 AM
To: Clow, Patrick; Matsuno, Akira
Cc: Moore, Bruce; CYBERDO
Subject: RE: CE12-003863 [Oppartycrasher)

Hi

Please let me know if you have any questions.

Dom

-----Original Message-----
From:
Sent: November-02-12 10:06 AM
To: Clow, Patrick; Bergeron, Dominic; Matsuno, Akira
Cc: Moore, Bruce; CYBERDO
Subject: CE12-003863 [Oppartycrasher)

Pat, as promised,

Cheers,

Clow, Patrick

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Friday, November 02, 2012 4:38 PM
To: CTEC
Subject: Update 9: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 2 November 2012
==========

==========
Update 9: 2 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC .

ASSESSMENT
==========

Page 994

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

Departments should implement the mitigation advice in above listed Cyber Flashes as well as any other Cyber Flashes that are released.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Pages 997 to / à 999

are duplicates of

sont des duplicatas des

pages 993 to / à 995

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Friday, November 02, 2012 5:14 PM
To: CTEC
Subject: Update/Mise à jour no 8: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous – Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

(La version française suit)

==========
GC CTEC - Information Note IN12-002
Date: 1 November 2012
==========

==========
Update 8: 1 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC .

NEW HIGHLIGHTS
==========
Potential traces of have been detected.

ASSESSMENT
==========

[redacted]

SUGGESTED ACTION
==========

[redacted]

Departments should implement the mitigation advice in GCCF12-008: DDoS campaign against the GC.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

==========

==========
CECM-GC – Note d'information IN12-002
Date : 1er novembre 2012
==========

==========
Mise à jour no 8 : 1er novembre 2012
- Mise à jour de l'information sur l'évaluation ==========

==========
Anonymous – Attaque par déni de service distribué visant le GC ==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de la campagne de déni de service distribué visant le GC planifiée par Anonymous.

ÉVALUATION
==========

From: CFNOC@forces.gc.ca
Sent: Saturday, November 03, 2012 2:14 AM
To: CYBERDO
Subject: RE: OpPartyCrasher Initiated

No. The only info I received is what is stated below.

G. Trepanier
J.G.G. Trepanier
Sergeant/sergent
>24/7 Watch
>Canadian Forces Network Operations Centre | Centre d'opérations des
>réseaux des Forces canadiennes Information Management Group | Groupe de
>gestion de l'information National Defence | Défense nationale Ottawa,
>Canada K1A 0K2 CFNOC@forces.gc.ca Telephone | Téléphone 613-945-7777 /
[redacted] Facsimile | Télécopieur 613-945-7760
>Teletypewriter (National Defence) | Téléimprimeur (Défense nationale)
>1-800-467-9877 Government of Canada | Gouvernement du Canada
>
>View a Remedy Trouble Ticket at this site:
http://img-ggi.mil.ca/sd-cs/nsd-bsn/index-eng.asp s.16(2)(c)

-----Original Message-----
From: CYBERDO [mailto:[redacted]
Sent: Saturday, 3, November, 2012 02:03 AM
To: +CFNOC@ADM(IM) CFNOC@Ottawa-Hull
Cc: ++CFNOC_CD Ops@ADM(IM) CFNOC@Ottawa-Hull; ++CFNOC_CD Ops Fusion@ADM(IM) CFNOC@Ottawa-Hull; +CFNOC_Watch Officer@ADM(IM) CFNOC@Ottawa-Hull; +CFNOC_WATCH WO@ADM(IM) CFNOC@Ottawa-Hull
Subject: RE: OpPartyCrasher Initiated

Greetings,

Thank for the information.
Web site seems to works. Did you have any indicators that the web site is down?

Thanks,

Vireak Phlek
CDO
CCIRC

-----Original Message-----
From: CFNOC@forces.gc.ca [mailto:CFNOC@forces.gc.ca]
Sent: November-03-12 12:59 AM
To: CYBERDO
Cc: CFNOC_CDOps@forces.gc.ca; CFNOC_CDOpsFusion@forces.gc.ca; CFNOC_WatchOfficer@forces.gc.ca; CFNOC_WatchWO@forces.gc.ca

s.15(1) - Def

Subject: FW: OpPartyCrasher Initiated

FYI/A.

G. Trepanier
J.G.G. Trepanier
Sergeant/sergent
>24/7 Watch
>Canadian Forces Network Operations Centre | Centre d'opérations des
>réseaux des Forces canadiennes Information Management Group | Groupe de
>gestion de l'information National Defence | Défense nationale Ottawa,
>Canada K1A 0K2 CFNOC@forces.gc.ca Telephone | Téléphone 613-945-7777 /
[redacted] Facsimile | Télécopieur 613-945-7760
>Teletypewriter (National Defence) | Téléimprimeur (Défense nationale) s.16(2)
>1-800-467-9877 Government of Canada | Gouvernement du Canada
>
>View a Remedy Trouble Ticket at this site:
http://img-ggi.mil.ca/sd-cs/nsd-bsn/index-eng.asp

-----Original Message-----
From: [redacted]
Sent: Saturday, 3, November, 2012 00:16 AM
To: +CFNOC@ADM(IM) CFNOC@Ottawa-Hull; ++CFNOC_CD Ops Fusion@ADM(IM) CFNOC@Ottawa-Hull
Subject: OpPartyCrasher Initiated

Good evening watch,

[redacted]

You may want to pass this info to the CCIRC Duty Officer (CYBERDO) for their action. No further action is required from us.

Cheers

Sent from my wireless handheld device / Transmis de mon appareil portable

From: CYBERDO
Sent: Saturday, November 03, 2012 2:30 AM
To: Beaudoin, Luc; Anderson, Windy
Cc: CYBERDO
Subject: CE12-003863 [#OpPartyCrasher Anonymous DDoS]

Hello Luc, Wendy,

[redacted]

Received the info from DND.

[redacted]

Page 1006

is a duplicate of

est un duplicata de la

page 1011

From: CYBERDO
Sent: Saturday, November 03, 2012 3:08 AM
To: GOC-COG
Cc: CYBERDO
Subject: RE: OpPartyCrasher Initiated

[redacted]

Vireak

-----Original Message-----
From: GOC-COG
Sent: November-03-12 1:24 AM
To: CYBERDO
Subject: OpPartyCrasher Initiated

FYSA

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted] s.16(2)(c)

-----Original Message-----
From: CFNOC@forces.gc.ca [mailto:CFNOC@forces.gc.ca]
Sent: November-03-12 1:18 AM
To: GOC-COG
Subject: FW: OpPartyCrasher Initiated

FYI/A.

G. Trepanier
J.G.G. Trepanier
Sergeant/sergent
>24/7 Watch
>Canadian Forces Network Operations Centre | Centre d'opérations des
>réseaux des Forces canadiennes Information Management Group | Groupe de
>gestion de l'information National Defence | Défense nationale Ottawa,
>Canada K1A 0K2 CFNOC@forces.gc.ca Telephone | Téléphone 613-945-7777 /
>[redacted] Facsimile | Télécopieur 613-945-7760
>Teletypewriter (National Defence) | Téléimprimeur (Défense nationale)
>1-800-467-9877 Government of Canada | Gouvernement du Canada
>
>View a Remedy Trouble Ticket at this site:
http://img-ggi.mil.ca/sd-cs/nsd-bsn/index-eng.asp

-----Original Message-----
From: +CFNOC@ADM(IM) CFNOC@Ottawa-Hull

Sent: Saturday, 3, November, 2012 00:58 AM
To: [redacted]
Cc: ++CFNOC_CD Ops@ADM(IM) CFNOC@Ottawa-Hull; ++CFNOC_CD Ops Fusion@ADM(IM) CFNOC@Ottawa-Hull; +CFNOC_Watch Officer@ADM(IM) CFNOC@Ottawa-Hull; +CFNOC_WATCH WO@ADM(IM) CFNOC@Ottawa-Hull
Subject: FW: OpPartyCrasher Initiated

FYI/A.

s.15(1) - Def
s.16(2)
s.16(2)(c)

G. Trepanier
J.G.G. Trepanier
Sergeant/sergent
>24/7 Watch
>Canadian Forces Network Operations Centre | Centre d'opérations des
>réseaux des Forces canadiennes Information Management Group | Groupe de
>gestion de l'information National Defence | Défense nationale Ottawa,
>Canada K1A 0K2 CFNOC@forces.gc.ca Telephone | Téléphone 613-945-7777 /
[redacted] Facsimile | Télécopieur 613-945-7760
>Teletypewriter (National Defence) | Téléimprimeur (Défense nationale)
>1-800-467-9877 Government of Canada | *Gouvernement du Canada*
>
>View a Remedy Trouble Ticket at this site:
http://img-ggi.mil.ca/sd-cs/nsd-bsn/index-eng.asp

-----Original Message-----
From: [redacted]
Sent: Saturday, 3, November, 2012 00:16 AM
To: +CFNOC@ADM(IM) CFNOC@Ottawa-Hull; ++CFNOC_CD Ops Fusion@ADM(IM) CFNOC@Ottawa-Hull
Subject: OpPartyCrasher Initiated

Good evening watch,

[redacted]

You may want to pass this info to the CCIRC Duty Officer (CYBERDO) for their action. No further action is required from us.

Cheers

Sent from my wireless handheld device / Transmis de mon appareil portable

From: Beaudoin, Luc
Sent: Saturday, November 03, 2012 4:09 AM
To: CYBERDO; Anderson, Windy
Subject: Re: CE12-003863 [#OpPartyCrasher Anonymous DDoS]

Very well. Provide them with all the available technical information,

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----
From: CYBERDO
Sent: Saturday, November 03, 2012 02:29 AM
To: Beaudoin, Luc; Anderson, Windy
Cc: CYBERDO
Subject: CE12-003863 [#OpPartyCrasher Anonymous DDoS]

Hello Luc, Wendy,

Received the info from DND.

Page 1010

is a duplicate of

est un duplicata de la

page 665

From: CCIRC-CCRIC
Sent: Saturday, November 03, 2012 8:36 AM
To: toewsv1@parl.gc.ca
Cc:
Subject: CCIRC CE12-003885 [#OpPartyCrasher
Attachments:

Greetings,

CCIRC would like to share the following information in the attachment. It contains a declaration to the Minister and have indicators

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613- Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada

-----Original Message-----
From: CCIRC-CCRIC
Sent: November-03-12 3:03 AM
To: toewsv1@parl.gc.ca
Cc:
Subject: CCIRC CE12-003885 [#OpPartyCrasher

Greetings,

[redacted]

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-[redacted] Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada s.16(2)(c)

From: Phlek, Vireak
Sent: Saturday, November 03, 2012 8:48 AM
To: Anderson, Windy
Cc: CYBERDO; Beaudoin, Luc
Subject: Update : CE12-003863 [#OpPartyCrasher Anonymous DDoS]
Attachments: Update 9: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Good morning Windy,

CTEC sent their update 9 last night.

[redacted]

As of now the web site is still up and running.

Thanks,

Vireak

From: Anderson, Windy
Sent: Saturday, November 03, 2012 9:22 AM
To: Phlek, Vireak
Cc: CYBERDO; Beaudoin, Luc
Subject: Re: Update : CE12-003863 [#OpPartyCrasher Anonymous DDoS]

Thanks for the updates. Robert appreciates too.

Windy

----- Original Message -----
From: Phlek, Vireak
Sent: Saturday, November 03, 2012 08:47 AM
To: Anderson, Windy
Cc: CYBERDO; Beaudoin, Luc
Subject: Update : CE12-003863 [#OpPartyCrasher Anonymous DDoS]

Good morning Windy,

CTEC sent their update 9 last night.

[redacted]

As of now the web site is still up and running.

Thanks,

Vireak

Pages 1015 to / à 1020

are duplicates of

sont des duplicatas des

pages 1025 to / à 1030

From: Christopher Locke <Christopher.Locke@tpsgc-pwgsc.gc.ca>
Sent: Saturday, November 03, 2012 4:10 PM
To: SOMIPC - GOSCPI
Cc: CYBERDO; CTEC (CTEC@CSE-CST.GC.CA)
Subject: [redacted]

Importance: High

s.16(2)

[redacted]

Cheers,
Chris Locke

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Saturday, November 03, 2012 4:17 PM
To: CTEC
Subject: Update 10: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 10: 3 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC s.16(2)
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC. [redacted] 2012.

ASSESSMENT
==========

[redacted]

[redacted]

SUGGESTED ACTION
==========

[redacted]

GC-CTEC and SSC will have staff in place this weekend, during the announced attack times, monitoring the situation and providing general mitigation advice including new or updated Cyber Flashes as required. Information note updates will be released as required in order to inform the GC of any changes of attack schedule as well as any trending in DDoS activity observed.

Departments should implement the mitigation advice in above listed Cyber Flashes as well as any other Cyber Flashes that are released.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

From: Blackberry, GCCTEC2 <GCCTEC2@CSE-CST.GC.CA>
Sent: Saturday, November 03, 2012 5:24 PM
To: CTEC; Blackberry, GCCTEC1; CYBERDO
Subject: Re: [CE12012-1289] FW:

Hello Vireak,

----- Original Message -----
From: CTEC
Sent: Saturday, November 03, 2012 03:52 PM
To: Blackberry, GCCTEC1; Blackberry, GCCTEC2;
Subject: FW: [CE12012-1289] FW: New Version of www.victoews.com -> OpPartyCrasher

---
From: CYBERDO[SMTP:
Sent: November 3, 2012 3:51:42 PM
To: CTEC
Subject: RE: [CE12012-1289] FW:

Thank you CTEC.

Vireak

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: November-03-12 1:20 PM
To: CYBERDO; CTEC
Subject: [CE12012-1289] FW:

Classification: UNCLASSIFIED

Hello CyberDO,

For your consumption.

http://www.pastebay.net

Regards,

Pages 1026 to / à 1031

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

From: Blackberry, GCCTEC2 <GCCTEC2@CSE-CST.GC.CA>
Sent: Saturday, November 03, 2012 7:29 PM
To: CTEC; RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca; CYBERDO
Subject: More info on #OpPartyCrasher

Hello,

More info from a Trusted Partner.

Regards,

[redacted]

GC-CTEC, CDO

[redacted]

Pages 1033 to / à 1034
are duplicates of
sont des duplicatas des
pages 697 to / à 698

From: CCIRC-CCRIC
Sent: Sunday, November 04, 2012 12:57 AM
To: [redacted]
Cc:
Subject: CCIRC CE12-003885 [#OpPartyCrasher [redacted]
Attachments: [redacted]

Greetings,

CCIRC is aware of your web site was listed as a target [redacted] You will find the following Mitigation Guidelines for Denial-of-Service Attacks at http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Please consider the following:

Establish contact with your technical team or host provider.

Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.

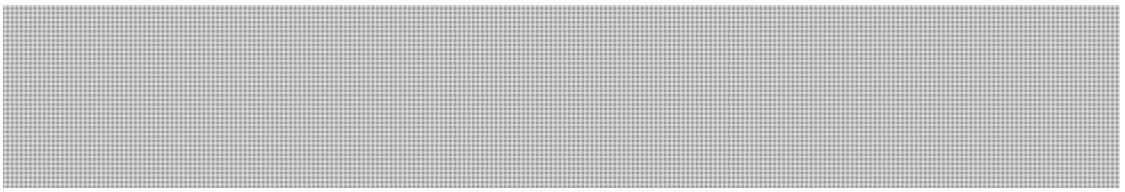
Establish 24/7 contact information for your ISP and alternate methods for communications.

[redacted]

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-[redacted] Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada s.16(2)(c)

From: Breault, Stephen
Sent: Sunday, November 04, 2012 2:59 PM
To: CYBERDO
Subject: #Oppartycrasher



From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Sunday, November 04, 2012 3:27 PM
To: CTEC
Subject: Update 11: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 11: 4 November 2012 s.16(2)
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC.

ASSESSMENT
==========

Page 1038

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

==========

GC-CTEC and SSC will have staff in place this weekend, during the announced attack times, monitoring the situation and providing general mitigation advice including new or updated Cyber Flashes as required. Information note updates will be released as required in order to inform the GC of any changes of attack schedule as well as any trending in DDoS activity observed.

Departments should implement the mitigation advice in above listed Cyber Flashes as well as any other Cyber Flashes that are released.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

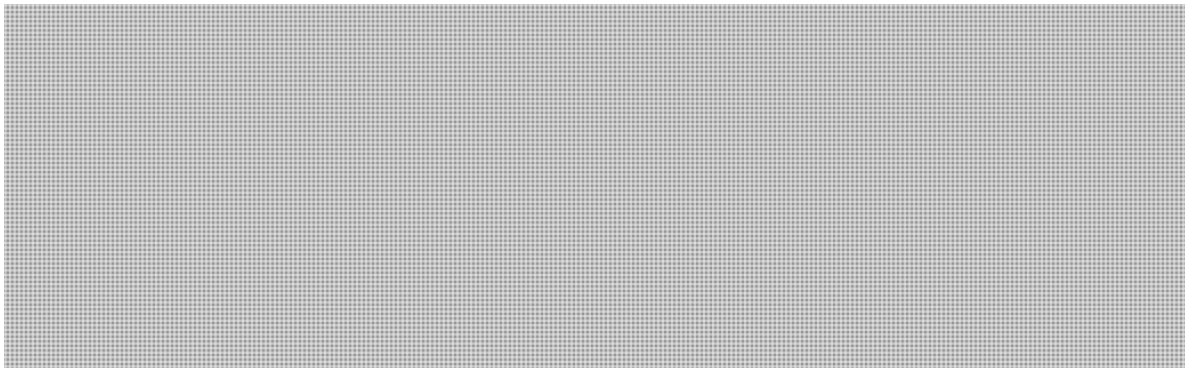
We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

From: RCN GPS CPI - NCR SMD IPC <RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca>
Sent: Sunday, November 04, 2012 8:08 PM
To: 'ctec@cse-cst.gc.ca'; CYBERDO; Lucie Levesque
Subject: Fw: Letter Writing

No biggie but this was posted 20 minutes ago
Chris
IPC Duty Analyst
819-956-1006
Sent from my BlackBerry Wireless Handheld

----- Original Message -----
From: Chris Locke [mailto:
Sent: Sunday, November 04, 2012 08:05 PM
To: RCN GPS CPI - NCR SMD IPC
Subject: Letter Writing



/c

From: CCIRC-CCRIC
Sent: Monday, November 05, 2012 9:38 AM
To:
Subject: CE12-003863 OpPartyCrasher, Anonymous DDOS threats
Attachments:

Greetings,

CCIRC is aware of that a website for which you are identified as the technical point of contact, was recently listed as a potential target by Anonymous.

Mitigation information can be found attached and on the following Public Safety Canada web site:
http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613- Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada

From:
To:
Sent: Monday, November 05, 2012 9:38 AM
Subject: Undeliverable: CE12-003863 OpPartyCrasher, Anonymous DDOS threats

Delivery has failed to these recipients or groups:

The e-mail address you entered couldn't be found. Please check the recipient's e-mail address and try to resend the message. If the problem continues, please contact your helpdesk.

Page 1044

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(d), 16(2)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 1045 to / à 1046
are duplicates of
sont des duplicatas des
pages 1047 to / à 1048

From: Cyber-Incident
Sent: Monday, November 05, 2012 2:09 PM
To: [redacted]
Subject: RE: CE12-003863 [redacted] OpPartyCrasher, Anonymous DDOS threats

Yes, as discussed.

Cheers

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-[redacted] Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada

From: [redacted]
Sent: November-05-12 1:42 PM
To: Cyber-Incident
Subject: FW: CE12-003863 [redacted] OpPartyCrasher, Anonymous DDOS threats

Dear Sir / Madam,

My name is [redacted] and I work as the Security Specialist for [redacted]

We have received the email below and just want to confirm its validity. Is this email sent out from your office?

Please advise. Thanks.

[redacted]

From: CCIRC-CCRIC [mailto:
Sent: November-05-12 6:38 AM
To:
Subject: CE12-003863 OpPartyCrasher, Anonymous DDOS threats

Greetings,

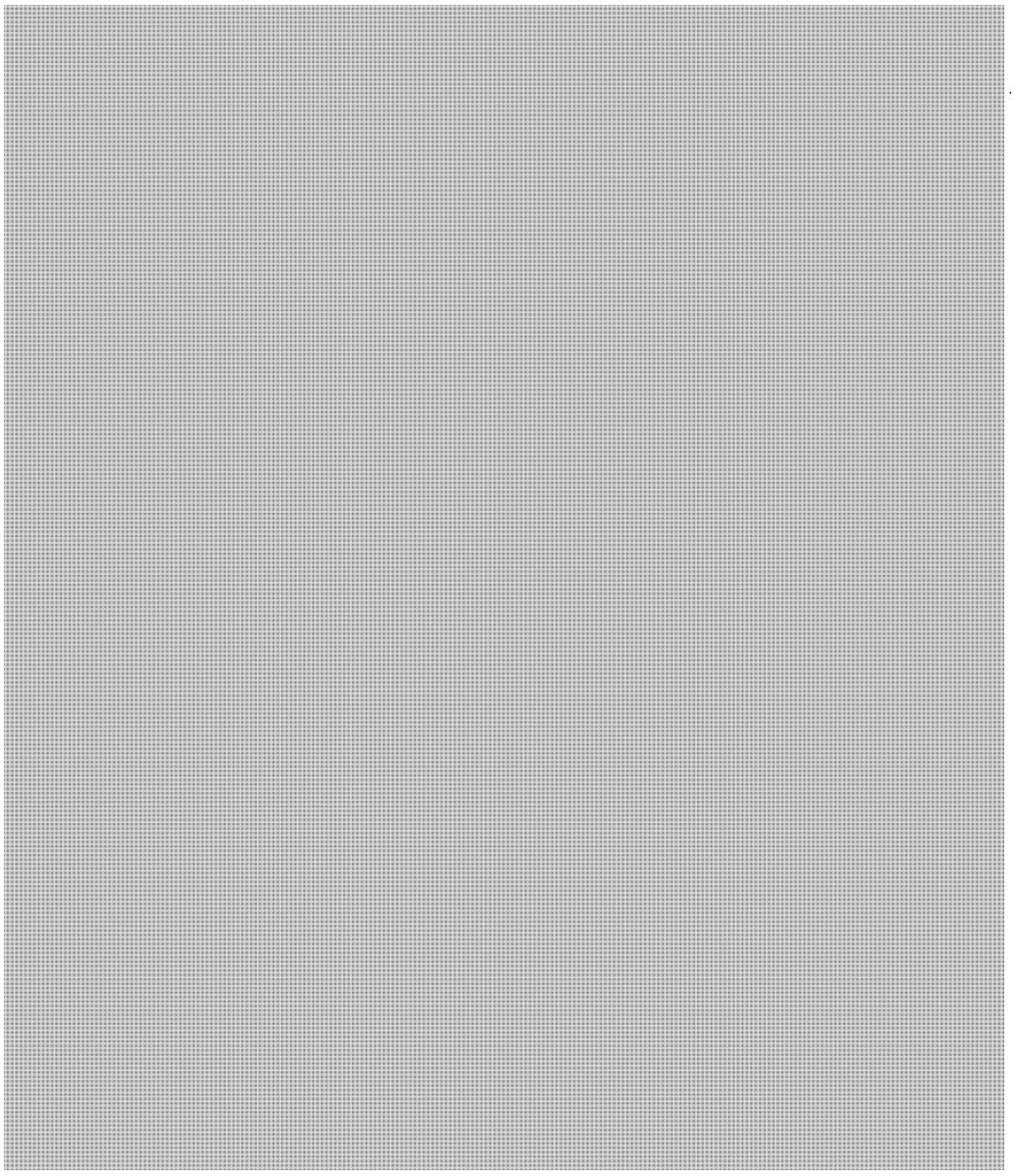
CCIRC is aware of that a website for which you are identified as the technical point of contact, was recently listed as a potential target by Anonymous.

Mitigation information can be found attached and on the following Public Safety Canada web site:
http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613- Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada

s.16(2)



Sincerely,

George E. Pelletier

-----Original Message-----
From: Pelletier, George E [NC]
Sent: Sat 11/3/2012 12:57 PM
To: Pelletier, George E [NC]; Rene Pariseau; CTEC
Cc: rcngpscpi.ncrsmdipc@ssc-spc.gc.ca; Snider, Mike [NC]; Surprenant, Jean-François [NC]; Tough, Dave [NC]; Young, Perry [NC]; Huard, Steve [NC]; Robillard, Jonathan [NC]; Pariseau, René [NC]
Subject: RE:

Hi Folks,

Just spotted this a few minutes ago. It appears to be a slightly modified version from this morning:

Pages 1050 to / à 1054
are withheld pursuant to section
sont retenues en vertu de l'article

16(2)

of the Access to Information
de la Loi sur l'accès à l'information

[redacted]

Sincerely,

George E. Pelletier

-----Original Message-----
From: Pelletier, George E [NC]
Sent: Sat 11/3/2012 4:09 AM
To: Rene Pariseau; CTEC
Cc: rcngpscpi.ncrsmdipc@ssc-spc.gc.ca; Snider, Mike [NC]; Surprenant, Jean-François [NC]; Tough, Dave [NC]; Young, Perry [NC]; Huard, Steve [NC]; Robillard, Jonathan [NC]; Pariseau, René [NC]
Subject: RE: [redacted]

Good Morning CTEC and SSC,

[redacted]

Pages 1056 to / à 1059
are withheld pursuant to section
sont retenues en vertu de l'article

16(2)

of the Access to Information
de la Loi sur l'accès à l'information

s.16(2)

s.19(1)

[redacted]

Sincerely,

George E. Pelletier

-----Original Message-----
From: Rene Pariseau [mailto[redacted]
Sent: Sat 11/3/2012 2:00 AM
To: CTEC
Cc: rcngpscpi.ncrsmdipc@ssc-spc.gc.ca; Snider, Mike [NC]; Surprenant, Jean-François [NC]; Pelletier, George E [NC]; Tough, Dave [NC]; Young, Perry [NC]; Huard, Steve [NC]; Robillard, Jonathan [NC]; Pariseau, René [NC]
Subject: [redacted]

Hello CTEC,

Sorry for sending this so late but you might want to look at this in the morning. [redacted]

Cheers.

--
Rene Pariseau, GCIH, GCFA
twitter: http://twitter.com/renepariseau

Public Safety Canada | Sécurité publique Canada

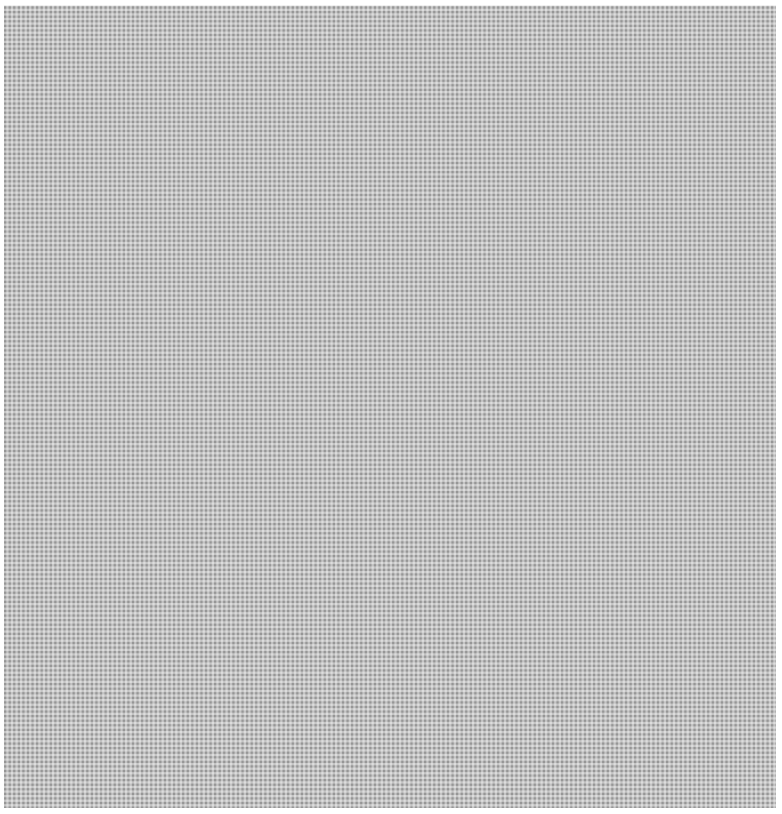
CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****
Date: 5 November 2012
CYBERDO: Vireak
****

[FOUO] NEW EVENTS:

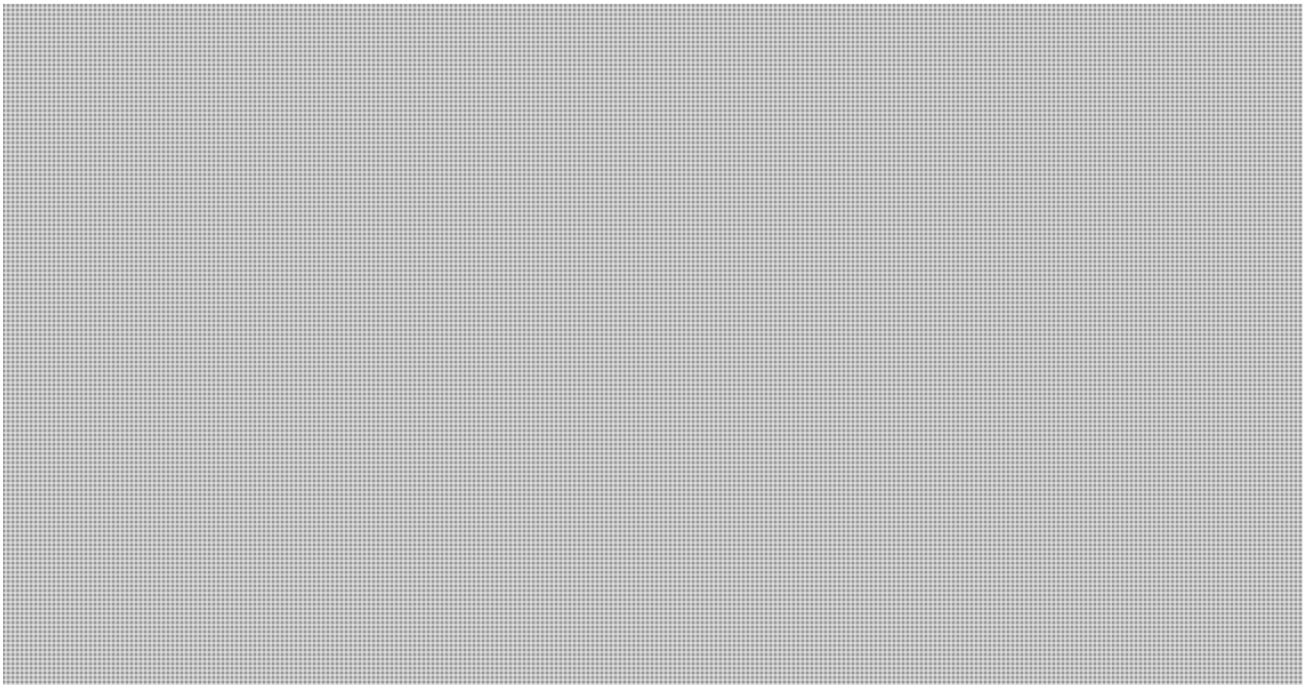
1. Title: CE12-003919 [Submission of malware: BBB and CF12-017]
- Summary: CCIRC received a [redacted] related to CF12-017.



- Owner: Bruce
- Status: Active

2. Title: CE12-003920 [CRR for Trojan on Canadian Site]
- Summary: Two trojans were confirmed originating from malc0de. Analysis done using virustotal.

Canada



- Action/Decision: CRR sent to hosting provider.

  - Owner: Ron
  - Status: Active

3. Title: CE12-003915 [Energy sector organization spear phishing to senior management]

- Summary: An energy sector organization submitted email samples appearing to be financial frauds. Email contacts from senior executives was leaked. Email using a senior official name appended to a yahoo webmail account was used as the email source to lure recipients. No malware or URLs appear in the email.

Email body description:

Morning ……(your name),

Hope you are having a nice time at work today, I have few transaction which I will want u to take care for me today, firstly I want to inform you that i need to complete some Wire transfer to another institution. What information you will need to process a Electronic wire transfer?

Please confirm the receipt of this email.

Similar campaigns reported here: http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Spam-Email-Scams-October-2012?OpenDocument

- Action/Decision: No further action required.

  - Owner: Steve
  - Status: Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE: NIL

1. Title: CE12-003863 [#OpPartyCrasher Anonymous DDoS]
- Summary: Anonymous threatens DDoS activity against Conservative party from Nov 3rd - Nov 15th. Event related to CE12-003854 and CE12-003848.

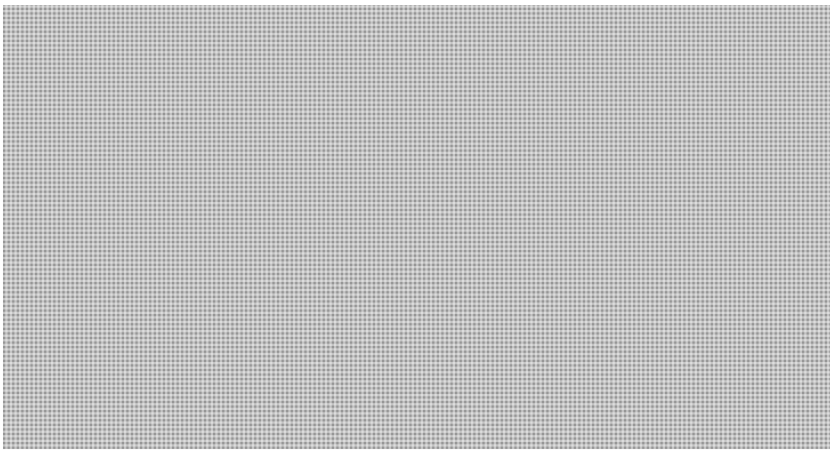
- Action/Decision:

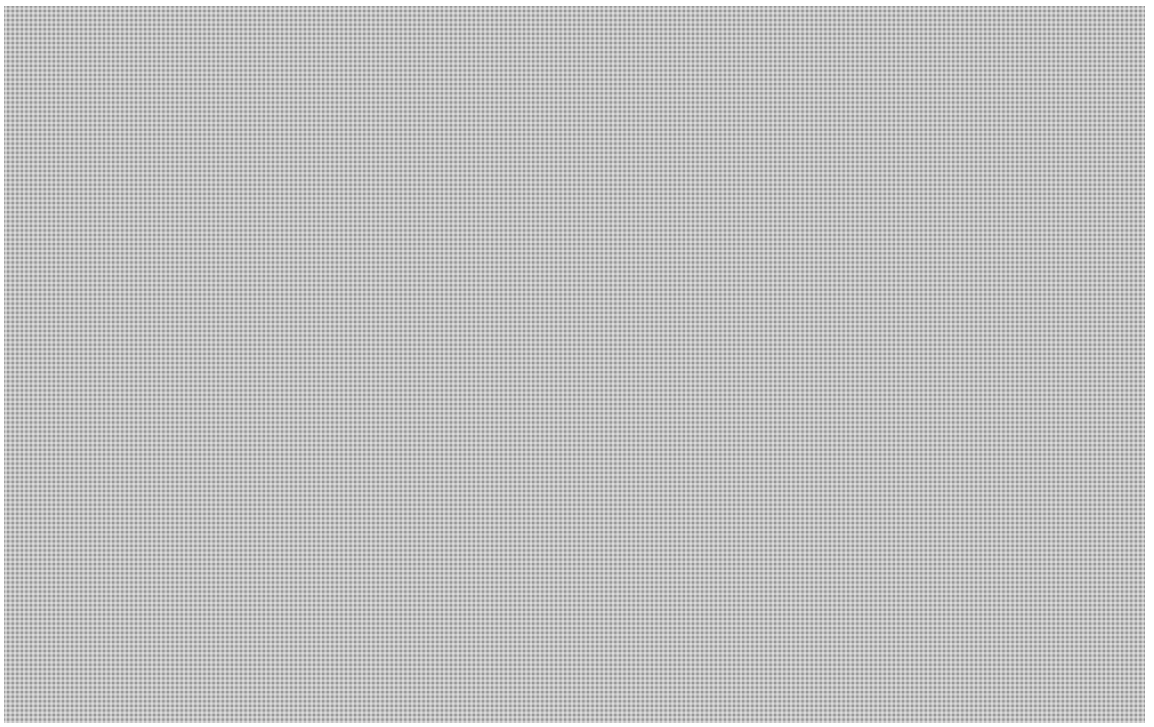
- Owner: Bruce
- Status: Active

2. Title: CE12-003897 [Air Canada Phishing]

Summary: CCIRC received a report of a live phishing email.

Link in the email:





- Action/Decision: Provide result to submitting party.
- Owner: Phlek
- Status: Active

[FOUO] ACTIVITIES:

1. Title: CE12-003914 [CloudFlare OpenResolver List]
- Summary: Cloudflare posted a summary of the threat posed by open DNS resolvers.

- Action/Decision: CCIRC requested Canadian IP list for action.

  - Owner: Chris
  - Status: Active

[FOUO] INTERNATIONAL PARTNERS:

1.
2.
3.

PUBLICATIONS: NIL

VULNERABILITY WATCH:NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS:

1. A guide on how to hack the iOS 6 Kernel

Reference: http://conference.hitb.org/hitbsecconf2012kul/materials/D1T2%20-%20Mark%20Dowd%20&%20Tarjei%20Mandt%20-%20iOS6%20Security.pdf

CYBER NEWS:

1. Malware protection firm **FireEye** has teamed up with EMC's RSA Security division through a new interoperability agreement that will leverage threat information from FireEye's Malware Protection System (MPS) and feed that data into RSA's **NetWitness** network monitoring platform.

Reference: http://www.securityweek.com/emcs-netwitness-platform-leverage-fireeyes-threat-data

2. VMware warns customers: Patch now as more stolen code leaks

VMware warned on Sunday that more of its source code for its ESX hypervisor technology could become public after another batch of code was released by a hacker.

The source code dates from 2004 and is related to other code released in April, wrote Iain Mulholland, VMware's director of platform security. He did not indicate what risk the current release poses to customers.

Reference: http://news.techworld.com/security/3409013/vmware-warns-customers-patch-now-as-more-stolen-code-leaks/

3. Attack of Team GhostShell against Russian Government

During last attack Team GhostShell leaked 2.5 millions of accounts belong to governmental, academic, political, research institutes, law enforcement, telecom and large corporations operating in different sectors such as energy and banking. "GhostShell is declaring war on Russia's cyberspace, in "Project BlackStar".

Reference: http://securityaffairs.co/wordpress/10036/hacking/attack-of-team-ghostshell-against-russian-government.html

4. For Internet Safety, Russia Most Dangerous In World

There are just 10 countries worldwide that host 86 percent of the web resources used to spread malware. For the second quarter in a row, this figure has climbed by a single percentage point.Yet, where it's climbed the most is Russia. Russia now hosts 23.2 percent of the world's malware, meaning most of the attacks on global computer systems — from PCs to networks to smartphones — originated by code writer in Russia. The U.S. came in second with 20.3 percent.

Reference: http://www.forbes.com/sites/kenrapoza/2012/11/02/for-internet-safety-russia-most-dangerous-in-world/

****

CYBER ENVIRONMENT SCANNING:
Websites
Malicious Activities and Incident Reports :
Atlas Canada Report (http://atlas.arbor.net/cc/CA)
ShadowServer Reports – previous day activity
Zeus Tracker (https://zeustracker.abuse.ch/index.php)
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)
XSSED (http://xssed.com/archive/special=1)
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)
Vulnerabilities:
Secunia (http://secunia.com/advisories/historic/)
TrendLabs Malware Blog (http://blog.trendmicro.com/)
Security Tracker (http://securitytracker.com/archives/summary/9000.html)
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)
Internet Storm Center – Sans (http://isc.sans.org)
Softpedia – Security (http://news.softpedia.com/cat/Security/)
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)
Websense Security Labs Blog
(http://community.websense.com/blogs/securitylabs/)
The H Security (http://www.h-online.com/security/)
Help Net Security (http://www.net-security.org/)
SecuriTeam (http://www.securiteam.com/)
News and Trends:
The Kaspersky Lab Security News Service (http://threatpost.com/)
Sucuri Research Blog (http://blog.sucuri.net/)
F-Secure (http://www.f-secure.com/weblog/)
Topix News (http://www.topix.net/tech/computer-security)

Krebs on Security (http://krebsonsecurity.com/)
Threat Level (http://www.wired.com/threatlevel/)
News Now
(http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)
Info Security News Mailing List (http://seclists.org/isn/)

[FOUO] GENERAL INFORMATION: NIL

Page 1068

is a duplicate of

est un duplicata de la

page 1069

From: Matsuno, Akira
Sent: Tuesday, November 06, 2012 12:19 PM
To: Moore, Bruce; CYBERDO
Cc: Turbide, Frank; Bergeron, Dominic; Clow, Patrick; Breault, Stephen
Subject: RE: CCIRC CE12-003863 OpPartyCrasher Anonymous DDoS - [redacted] TA12-5116

I'm getting Frank's help on this one. He was going to note some observations that he had for this.

Note that I am on course this week and we don't have good signal at the training centre. I will do my best to respond when I can.

Akira

-----Original Message-----
From: CYBERDO
Sent: Tuesday, November 06, 2012 11:33 AM
To: Matsuno, Akira
Subject: CCIRC CE12-003863 OpPartyCrasher Anonymous DDoS - [redacted] TA12-5116

Hi Akira;

Any idea when analysis will be completed on this file?

Bruce Moore
Incident Handler | Gestionnaire d'incident Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-7792
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Tuesday, November 06, 2012 12:51 PM
To: CYBERDO
Cc: CTEC; Denis.Patenaude@ssc-spc.gc.ca
Subject: RE: CE12-003863 [#OpPartyCrasher]

Classification: UNCLASSIFIED

Hello Stephen,

[redacted]

Regards,

[redacted]
GC-CTEC - Cyber Duty Officer
[redacted]

From: CYBERDO [mailto:[redacted]
Sent: November 6, 2012 9:40 AM
To: 'Denis Patenaude (Denis.Patenaude@ssc-spc.gc.ca)'; CTEC
Subject: CE12-003863 [#OpPartyCrasher]

Gents,

[redacted]

s.16(2)
s.16(2)(c)

Any of these look familiar,

Thanks for your time.

Cheers,

Stephen
Cyber Duty Officer | Officier de veille cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From:
Sent: Tuesday, November 06, 2012 12:53 PM
To: CCIRC-CCRIC
Cc:
Subject: RE: CE12-003863 OpPartyCrasher, Anonymous DDOS threats

Sensitivity: Confidential

From: CCIRC-CCRIC [mailto:
Sent: November-05-12 6:38 AM
To:
Subject: CE12-003863 OpPartyCrasher, Anonymous DDOS threats

Greetings,

CCIRC is aware of that a website for which you are identified as the technical point of contact, was recently listed as a potential target by Anonymous.

Mitigation information can be found attached and on the following Public Safety Canada web site:
http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613- Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada

s.16(2)(c)

Pages 1073 to / à 1074
are withheld pursuant to sections
sont retenues en vertu des articles

16(2), 16(2)(c), 21(1)(b)

of the Access to Information
de la Loi sur l'accès à l'information

Page 1075

is withheld pursuant to sections

est retenue en vertu des articles

16(2), 21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Page 1076

is withheld pursuant to sections

est retenue en vertu des articles

16(2), 16(2)(c), 21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Page 1077

is withheld pursuant to sections

est retenue en vertu des articles

16(2), 21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO
Sent: Tuesday, November 06, 2012 2:29 PM
To: Bendelier, Kenneth
Subject: RE: Please read now - Potential CRA to BD shutdown
Attachments:

Who is your BC contact ? I ll fire them a response.

Here is the email if you prefer sending it:
////
Greetings,

CCIRC is aware of a number of website being potential target of the hacktivist group Anonymous.

Mitigation information can be found attached and on the following Public Safety Canada web site:
http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

CCIRC is not aware of increase threats or risks associated with this activity for other government or vital system operators partners.

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613- Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada

\\\\

From: Bendelier, Kenneth
Sent: November-06-12 11:52 AM
To: CYBERDO
Cc: Beaudoin, Luc; Clow, Patrick; Anderson, Windy
Subject: FW: Please read now - Potential CRA to BD shutdown
Importance: High

I'll try asking again.

Are we (or our partners) aware of anything CRA related that is going on? CRA seems to have put an advisory out to their provincial partners (this is Ontario, BC asked the same question on Friday).....

I'd like to be able to say we know (or don't know) something (anything).....

This seems one of those odd ones where our current partners (provinces) are asking about something relating to our former partners (CRA) where another partner is the lead (GC CTEC) and we (CCIRC) should perhaps be a coordinator.

From: Lorenc, John (MGS) [mailto:John.Lorenc@ontario.ca]
Sent: November-06-12 9:50 AM
To: Bendelier, Kenneth
Subject: FW: Please read now - Potential CRA to BD shutdown

Hello Ken

Wondering if you have any more info on this?

John

John Lorenc, CISSP
Manager, Information Protection Centre
OCCIO, Corporate Security Branch
Ministry of Government Services
155 University Ave, 7th floor
Toronto, ON M5H 3B7
Office: 416.212.2839, Cell: [redacted]
Fax: 416.212.5375, john.lorenc@ontario.ca

s.19(1) s.16(2)

From: Samuels, Crystal (MGS)
Sent: November-05-12 9:57 AM
To: Tarsitano, Mario (MGS)
Subject: (Important Info): Potential CRA to BD shutdown

Hello Mario,

On Friday late afternoon Barry Edwards give me a call indicating that he is informing all his stakeholders of an anticipated malicious attempt to negatively impact the Government of Canada systems.

[redacted]

I will keep in close contact with Barry [redacted] and if require inform our partners [redacted]

Thank you,

Crystal Samuels, MBA
Manager, Business Directory
Business Improvement Division
ServiceOntario – ***making it easier***
Visit us at: www.ServiceOntario.ca

s.19(1)

T: 416-212-4960
B: [redacted]
E: crystal.samuels@ontario.ca

From: CCIRC-CCRIC
Sent: Tuesday, November 06, 2012 3:06 PM
To:
Subject: CE12-003863 OpPartyCrasher, Anonymous DDOS threats
Attachments:

Greetings,

As discussed, CCIRC is aware that the website for which you are identified as the technical point of contact, was recently listed as a potential target by Anonymous.

Mitigation information can be found attached and on the following Public Safety Canada web site:
http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613- Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada

From: Bendelier, Kenneth
Sent: Tuesday, November 06, 2012 3:46 PM
To: CYBERDO; Beaudoin, Luc; Clow, Patrick; Anderson, Windy
Subject: Re: CE12-003863 OpPartyCrasher Anonymous DDOS threat

Well well done.

Thank you.

From: CCIRC-CCRIC
Sent: Tuesday, November 06, 2012 03:37 PM
To: 'Rob.todd@gov.bc.ca' <Rob.todd@gov.bc.ca>
Cc: Bendelier, Kenneth
Subject: CE12-003863 OpPartyCrasher Anonymous DDOS threat

Greetings,

This is in response to a request for information you sent us. CCIRC is aware of a number of website being potential target of the hacktivist group Anonymous.

Mitigation information can be found attached and on the following Public Safety Canada web site:
http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-
s.16(2)(c)
Facsimile | Télécopieur +1 613-991-3574 Government of Canada | Gouvernement du Canada

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Tuesday, November 06, 2012 4:26 PM
To: CTEC
Subject: Update 13: Information Note IN12-002: Anonymous DDoS activity against GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 6 November 2012
==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

==========
Update 13: 6 November 2012
- Restructured assessment section
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Page 1084

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

SUGGESTED ACTION
==========

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here:
http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

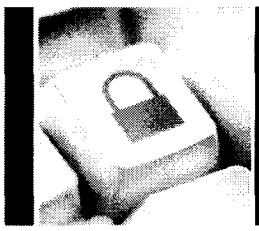
==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.



CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 6 November 2012
CYBERDO: Vireak
****

[FOUO] NEW EVENTS:

1. Title: CE12-003924 [CI Energy Submitted malware Sample]
- Summary:
  CCIRC received a malware sample from our CI Energy partner.
- Action/Decision:
  TAR was requested and an analyst is working on it
  - Owner: Luc
  - Status: Active

2. Title: CE12-003927 [Phishing Emails related to CF12-009]
- Summary:
  A Federal partner reported [redacted]
  They received [redacted]
  Indicators from CF12-009 Update 2 were hits.
- Action/Decision:
  N/A
  - Owner: Bruce
  - Status: Closed

s.16(2)
s.16(2)(c)

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. Title: CE12-003863 [#OpPartyCrasher Anonymous DDoS]
- [redacted]

Canada

[redacted]

- Owner: Bruce
- Status: Active

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. Item Description: [redacted]

2. Item Description: [redacted]

PUBLICATIONS: NIL

VULNERABILITY WATCH:

1. Item Description: **Symantec Endpoint Protection CAB File Processing**
   A remote user can send a specially crafted CAB formatted file to trigger a memory corruption error in 'dec_abi.dll' and execute arbitrary code on the target system. The code will run with System privilege. CVE-2012-4953. A vendor patch is available.

- Reference: http://www.kb.cert.org/vuls/id/985625

THREAT WATCH: NIL

1. Item Description:

- Reference:

UTILITIES/REPORTS/TIPS:

1. Item Description: **ITSG-33 (IT Security Risk Management: A Lifecycle approach)**
   The ITSG-33 publication has been developed to help government departments ensure security is considered right from the start. By following the principles within this publication, you not only help ensure predictability and cost-effectiveness, you also help ensure that there are no hidden surprises preventing you from obtaining authority to operate and maintaining continued authorization.
   Reference: http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng.html

2. Item Description: **Your malware shall not fool us with those anti analysis tricks**
   It is well known that a big amount of malware samples are aware of the execution environment. This means that a malware sample can change his behavior if it detects that the running environment is unwanted. There are resources, public source code, and even programs that detail how to bypass automatic malware analysis systems and make things awkward for malware researchers. Of course, these resources are quite useful for both researchers and malware developers.
   We are going to take a look at some of these tricks, all found in real malware samples. Also, just as they do, we have developed some yara signatures to detect these tricks that could be useful to differently process or classify these malware samples. We could classify anti analysis tricks in three big groups:
   - Anti Virtual Machine, that tries to detect if the execution environment is a known VM or emulator.
   - Anti Debugging, that tries to detect if the program is running under the surveillance of a debugger.
   - Anti Sandbox, that tries to detect known sandboxing products.
- Reference: http://labs.alienvault.com/labs/index.php/2012/your-malware-shall-not-fool-us-with-those-anti-analysis-tricks/

CYBER NEWS:

1. Item Description: **Citadel: a cyber-criminal's ultimate weapon?**
   In old times, a citadel was a fortress used as the last line of defense. For cyber criminals it is a powerful and state-of-the-art toolkit to both distribute malware and manage infected computers (bots). Citadel is an offspring of the (too) popular Zeus crimekit whose main goal is to steal banking credentials by capturing keystrokes and taking screenshots/videos of victims' computers. Citadel came out circa January 2012 in the online forums and quickly became a popular choice for criminals. A version of Citadel (1.3.4.5) was leaked in late October and although it is not the latest (1.3.5.1),

it gives us a good insight into what tools the bad guys are using to make money. In this post, I will show you how criminals operate a botnet. This is not meant as a tutorial and I do want to stress that running a botnet is illegal and could send you to jail.

- Reference: http://blog.malwarebytes.org/intelligence/2012/11/citadel-a-cyber-criminals-ultimate-weapon/

2. Item Description: **Coke Gets Hacked And Doesn't Tell Anyone**
FBI officials quietly approached executives at Coca-Cola Co. (KO) on March 15, 2009, with some startling news.
Hackers had broken into the company's computer systems and were pilfering sensitive files about its attempted $2.4 billion acquisition of China Huiyuan Juice Group (1886), according to three people familiar with the situation and an internal company document detailing the cyber intrusion. The Huiyuan deal, which collapsed three days later, would have been the largest foreign takeover of a Chinese company at the time.
- Reference: http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-tell.html?utm_source=Sinocism+Newsletter&utm_campaign=7b539f90bbThe_Sinocism_China_Newsletter_For_11_05_2012&utm_medium=email

3. Item Description: **Hacking of Tax Records Has Put States on Guard**
The theft of tax information from a South Carolina computer system appears to have been the largest cyberattack ever on a state government and has put other states on high alert, computer security experts say.
- Reference: http://www.nytimes.com/2012/11/06/us/south-carolina-tax-hacking-puts-other-states-on-alert.html?hp

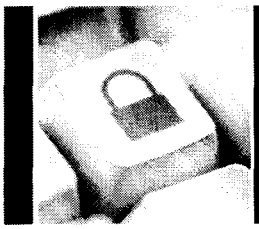
****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒

Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION: New Cyberdo - Bruce



CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 7 November 2012
CYBERDO: Bruce
****

[FOUO] NEW EVENTS:

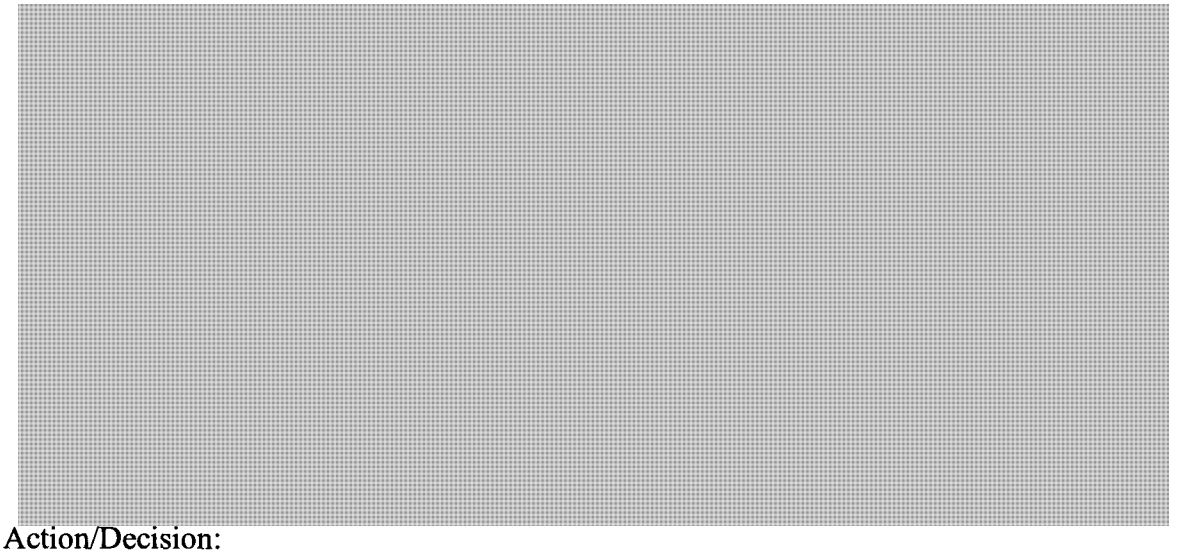
1. Title: CE12-003931 - RBC Phishing
- Summary:
  CCIRC received a report of a live phishing email.
  Link in the email:
  [redacted]
- Action/Decision:
  Report sent to the organization phishing intake and a partner for URL blocking.

  - Owner: Bruce
  - Status: Closed

2. Title: CE12-003932 - CI-Telecom - Target Phishing Email
- Summary:
  [redacted]
- Action/Decision:

  - Owner: Bruce
  - Status: Closed

3. Title: CE12-003934 [Potential Brobot sites]
- Summary:



- Action/Decision:

  - Owner: Luc
  - Status: Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. Title: CE12-003863 [#OpPartyCrasher Anonymous DDoS]
- Update:
  Target #4 identified. CCIRC notified the affected site administrator.
- Action/Decision:

  - Owner: Bruce
  - Status: Active

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. Item Description:
2. Item Description:

PUBLICATIONS:

1. Item Description: AV12-0044 - Security Updates for Adobe Flash

VULNERABILITY WATCH:

1. Item Description: **Google Chrome Multiple Vulnerabilities**
   Multiple vulnerabilities have been reported in Google Chrome. Most of these have to do with built in plugins packages with the application allowing remote code execution. 21 CVEs are affected. A vendor patch is available
   - Reference: http://googlechromereleases.blogspot.dk/2012/11/stable-channel-release-and-beta-channel.html

2. Item Description: **Adobe Flash Player Multiple Vulnerabilities**
   Adobe Flash Player Multiple Vulnerabilities - Multiple vulnerabilities have been reported in Adobe Flash Player and Adobe AIR allowing users to remotely cause buffer overflow and memory corruption. CVE-2012-5274 to 5280. A vendor patch is available.
   - http://www.adobe.com/support/security/bulletins/apsb12-24.html

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS:

1. Item Description: **Virtual machine used to steal crypto keys from other VM on same server**
   Piercing a key defense found in cloud environments such as Amazon's EC2 service, scientists have devised a virtual machine that can extract private cryptographic keys stored on a separate virtual machine when it resides on the same piece of hardware. The technique, unveiled in a research paper published by computer scientists from the University of North Carolina, the University of Wisconsin, and RSA Laboratories, took several hours to recover the private key for a 4096-bit ElGamal-generated public key using the libgcrypt v.1.5.0 cryptographic library. The attack relied on "side-channel analysis," in which attackers crack a private key by studying the electromagnetic emanations, data caches, or other manifestations of the targeted cryptographic system.
   - Reference: http://arstechnica.com/security/2012/11/crypto-keys-stolen-from-virtualmachine/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+arstechnica%2Findex+%28Ars+Technica+-+All+content%29
     http://www.cs.unc.edu/~reiter/papers/2012/CCS.pdf

CYBER NEWS:

1. Item Description: **Trojan horse designed to steal your photos**

   When it comes to data theft there seems to be no limit to the types of files that might be stolen if your system becomes compromised.

   The latest, Troj/PixSteal-A, is designed to take all of the images, photos and even memory dumps from your hard drive.

   The malware starts out by scouring your C: D: and E: drives on Windows for any files ending in .JPG, .JPEG and .DMP.

- Reference: http://nakedsecurity.sophos.com/2012/11/06/trojan-horse-designed-to-steal-your-photos/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+nakedsecurity+%28Naked+Security+-+Sophos%29

2. Item Description: **New Backdoor DDoS Malware Co-Existing on Gh0stRAT-Infected Machines**

   Gh0st RAT has a new roommate. A new backdoor called ADDNEW has been discovered on machines infected with the Gh0st remote access Trojan, adding new distributed denial of service attack capabilities, as well as a feature that targets passwords and credentials stored on the Firefox browser.

   Gh0st RAT is a notorious piece of malware having been used in the Aurora attacks on Google, Adobe and other large manufacturers and technology companies. Most recently, new variants of Gh0st were present in water-holing attacks called VOHO analyzed by RSA Security's FirstWatch research team.

- Reference: https://threatpost.com/en_us/blogs/new-backdoor-ddos-malware-co-existing-gh0strat-infected-machines-110612

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒

Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION:

[redacted] s.16(2)(c)

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Wednesday, November 07, 2012 4:43 PM
To: CTEC
Subject: Mise à jour no 10: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

English version previously sent.

==========
CECM-GC – Note d'information IN12-002
Date : 25 octobre 2012
==========

==========
Mise à jour no 10: 3 novembre 2012
- Mise à jour de l'information sur l'évaluation ==========

==========
Anonymous – Attaque par déni de service distribué visant le GC ==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de la campagne de déni de service distribué visant le GC planifiée par Anonymous.

ÉVALUATION
==========

[redacted]

À mesure qu'il découvrira des activités malveillantes touchant le GC, le CECM-GC diffusera des cybercapsules contenant des conseils d'atténuation technique connexes.

Depuis la diffusion de la première note d'information IN12-002, le CECM-GC a publié les documents suivants :
- GCCF12-008 : « Campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre au niveau du réseau en vue de remédier à l'activité inhabituelle du port « 0 ». On ignore toujours si cette activité est liée à la campagne #OpPartyCrasher d'Anonymous.
- GCCF12-009 : « Utilisation possible de [redacted] dans le cadre de la campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre au niveau du réseau et du serveur en vue de remédier au trafic [redacted] inhabituel qui est probablement lié à la campagne #OpPartyCrasher d'Anonymous.
- GCCF12-010 : « Mesures d'atténuation pour la campagne visant les formulaires de sites Web du GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre au niveau du serveur en vue de remédier aux attaques visant les formulaires Web qui ne sont probablement pas liés à la campagne #OpPartyCrasher d'Anonymous.

MESURES RECOMMANDÉES
==========

[redacted]

Des membres du personnel du CECM-GC et de SPC surveilleront la situation au cours de la fin de semaine, pendant les heures d'attaque annoncées, et fourniront des conseils généraux d'atténuation, dont de nouvelles cybercapsules ou mises à jour, au besoin. Le CECM-GC diffusera également au besoin des mises à jour de la note d'information IN12-002

pour informer les ministères du GC des changements concernant l'horaire des attaques et des tendances dans les activités observées de déni de service distribué.

On vous recommande de mettre en œuvre les conseils d'atténuation énoncés dans les cybercapsules susmentionnées et dans celles qui seront diffusées ultérieurement.

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

==========

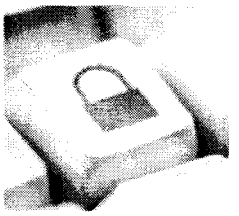
Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

OPERATIONAL SUMMARY
CCIRC Cyber Awareness Product



Weekly Technical Report

Issued: 07 November 2012

Volume 2012 - 44

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flash marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information, or Technical
- **Operational Summary**: Daily, Weekly, Monthly

NOTE TO READERS

CCAPs are available at the following website: http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx. If you have any questions, please contact the Public Safety Cyber Duty Officer @ [redacted] s.16(2)(c)

Traffic Light Protocol: RED: Designated for a specific audience/Non-sharable
AMBER: Sharable within organization on a need-to-know basis/Non-publishable
GREEN: Sharable within organization or community/Non-publishable
WHITE: Free to distribute

Table of Contents

Executive Summary

During the reporting period, the Canadian Cyber Incident Response Centre (CCIRC) handled 13 incidents, affecting partners in public and private sector organizations. The threat of action by the group Anonymous on political institutions [redacted] continued and was reported in the media.

CCIRC sent victim notifications to its partners in public and private organizations who were found to have hosts infected with Conficker, Fake Anti-Virus (i.e. rogueware), Zeus, SpyEye, Flashback, and/or Nitol malware; and to organizations which were found to be operating with open domain name system (DNS) resolvers. CCIRC also handled several phishing attempts, including the impersonation of Canada Post, the Better Business Bureau, and a European energy company.

CCIRC regularly issues information products to inform its partners of potential, imminent or actual cyber threats. During the reporting period, CCIRC issued one cyber flash (*CF12-017 – Better Business Bureau Phishing Emails Using [peer-to-peer] P2P Zeus Malware Variant*) to its partners in public and private sector organizations.

Threat and vulnerability monitoring identified new vulnerabilities in Apple Safari and Symantec Endpoint Protection – both of which have vendor patches released – and new ransomware which impersonates the hacktivist group Anonymous. Additionally, the United States Department of Homeland Security's Industrial Control Systems Computer Emergency Response Team (ICS-CERT) reported an application vulnerability used by the owners and operators of electrical, water, sewage, and gas industrial control systems.

This week's noteworthy news included phishing emails imitating an update to Windows 8, as well as hacking researchers funded by the Government of France who claim to have defeated the new security features of Windows 8. The increasing sophistication and prevalence of Citadel malware, which is a version of the pervasive Zeus crimekit developed in early 2012, was also highlighted.

s.16(2)
s.16(2)(c)

Incident Reporting

This section contains information related to incidents affecting Critical Infrastructure in Canada.

1. CE12-003863 [redacted] Anonymous DDoS]

[redacted]

CCIRC notified site administrators and provided some mitigation advice. The impact to these sites has been minimal/nil to our knowledge.

2. CE12-003891 [Notifications – Conficker]

Notifications to multiple organizations. Hosts within these organizations were infected with Conficker botnet malware.
Total IP count: 3831
Number of affected organisations receiving a notification: 135
Federal: 1
Provincial: 3
Municipal: 1
Telecom: 104
Energy: 2
Manufacturing & Retail: 1
Health: 4
Academia: 19
Notifications sent to IT security or technical contacts at affected organizations.

3. CE12-003893 [European Energy Company Phishing]

CCIRC was notified of a phishing website targeting a European energy company hosted on a Canadian website.

[redacted]

Deactivation request sent to the hosting provider.

4. CE12-003895 [Malware hosted [redacted]

[redacted]

[redacted]

5. CE12-003901 [FakeAV Malware]

CCIRC received a FakeAV malware sample that attempted connections to:
[redacted]
Additional research indicated this IP address was associated with FakeAV malware activity since at least 2009. CRR sent to the hosting provider.

6. CE12-003902 [Notifications – Open DNS Resolvers]

Notifications to multiple organizations. Hosts within these organizations were operating open DNS resolvers. Potential implications from operating systems as open resolvers are:

- They allow outsiders to consume resources that do not belong to them.
- Attackers may be able to poison the cache of an open resolver.
- Open resolvers could be used in DDoS attacks.

Notifications sent to IT Security or technical contacts in the following sectors:
Fed: 1
Provincial: 2
Academia: 3

7. CE12-003903 [Notifications – Zeus]

Notifications to multiple organizations. Hosts within these organizations were infected with ZeuS malware.
Total IP count: 3425
Number of affected organisations receiving a notification: 116
Provincial: 4
Telecom: 99
Finance: 1
Energy: 2
Transportation: 1
Academia: 16
Other Industries: 2
Notifications sent to IT security or technical contacts at affected organizations.

8. CE12-003902 [Notifications – Generic Botnet Malware]

Notifications to multiple organizations. Hosts within these organizations were infected with various botnet related malware.
Total IP count: 3133
Number of affected organisations receiving a notification: 109
Provincial: 4
Telecom: 82
Finance: 1
Energy: 2
Health: 1
Academia: 19
Notifications sent to IT security or technical contacts at affected organizations.

s.16(2)
s.16(2)(c)

9. CE12-003907 [Notifications – ZeuS Malware]

Notifications to multiple organizations. Hosts within these organizations were infected with ZeuS malware.
Total IP count: 1567
Number of affected organisations receiving a notification: 97
Provincial: 1
Telecom: 68
Energy: 4
Transportation: 1
Manufacturing & Retail: 3
Health: 1
Academia: 19
Notifications sent to IT security or technical contacts at affected organizations.

10. CE12-003909 [SpyEye Command and Control]

CCIRC was notified of a domain being used for SpyEye Command and Control.

[redacted]

CRR sent to the hosting provider.

11. CE12-003910 [Notifications – Flashback Malware]

Notifications to multiple organizations. Hosts within these organizations were infected with Flashback malware.
Total IP count: 588
Number of affected organisations receiving a notification: 54
Provincial: 2
Municipal:
Telecom: 37
Academia: 15
Notifications sent to IT security or technical contacts at affected organizations.

12. CE12-3917 [Malware hosted on [redacted]]

CCIRC identified malware files hosted on this server (Generic Trojan).

[redacted]

Detection ratio: 20 / 44

[redacted]

Detection ratio: 19 / 44

CRR sent to the hosting provider.

Federal Government

1. CE12-003900 [Nitol Infection – Federal Department]

CCIRC received information from a trusted source that hosts within a Federal department may be infected with Nitol related malware. CCIRC sent a notification to the Federal CSIRT for evaluation and notification to the affected department.

Provincial and Territorial Government

NIL

Municipal Government

NIL

Information and Communication Technology

NIL

Finance

NIL

Energy and Utilities

NIL

Transportation

1. CE12-003897 [Air Canada Phishing]

URL in phishing email downloaded Zeus malware.

CCIRC analysis found that an infected host would make connections to IP: (This domain/IP were listed as indicators in CF12-009 Update 3)

Manufacturing

NIL

Health

NIL

Food

NIL

Water

NIL

Other (Academia)

NIL

Other Organizations

NIL

Partners

Watch List

NIL

Malware Indicators

*IMPORTANT: These indicators must be silently dropped if implemented in defensive technologies. Many security products perform dynamic pulling of malicious sites/IPs. The indicators below are sensitive and may be associated with on-going investigations. Active probing could disrupt such efforts.

Indicator	Malware	Reference
Email Indicators: Sender: Subject: Attachment Name: **File Indicators:** Filename: MD5 Hash Filename: MD5 Hash **Domain(s) and IP(s):** HTTP (Port 80) traffic to:	BBB Phishing / Zeus	Trusted Partner

[redacted] **HTTP URI Indicators:** [redacted]		
Domain(s) and IP(s): TCP Port 8080 traffic to: [redacted] TCP Port 80 and 8080 traffic to: [redacted] **HTTP URI Indicators:** [redacted]	Trojan	Trusted Partner
Domain(s) and IP(s): [redacted] **HTTP URI Indicators:** [redacted]	SpyEye	Trusted Partner
Email Indicators: Sender: [redacted] Subject: Attachment: [redacted]	Phishing / Trojan	Trusted Partner

s.16(2)

s.19(1)

Sender: [redacted] Subject: **Domain(s) and IP(s):** [redacted] **HTTP URI Indicators:** [redacted]		
HTTP URI Indicators: [redacted]	Sopelka Botnet / Citadel	Trusted Partner
Email Indicators: Sender: [redacted] Subject: Attachment name: Sender : [redacted] Subject: **Domain(s) and IP(s):** [redacted]	Blackhole Exploit Kit v2.0	Trusted Partner
Email Indicators: Sender: [redacted] Subject: Sender : Subject:	Phishing	Trusted Partner

Domain(s) and IP(s):		
Pre-Infection Indicators **Email Indicators:** Sender: Subject: **File Indicators:** Filename: MD5 Hash: Filename: MD5 Hash: **HTTP URI Indicators:** ***Post-Infection Indicators*** **File Indicators:** Filename: MD5 Hash: **Domain(s) and IP(s):** HTTP (Port 80) traffic to: **HTTP URI Indicators:**	Phishing	Trusted Partner
Email Indicators: Subject: Attachment Name: Subject: Attachment(s): Subject: Attachment(s) Subject: Attachment(s): Subject: Attachment(s):	Spear Phishing	Trusted Partner

Subject: Attachment(s): Subject (multiple variants): • • • • • • • • • • • **File Indicators:** Filename MD5 Hash: Filename: MD5 Hash: Filename: MD5 Hash: Filename: MD5 Hash: Filename: MD5 Hash Filename: MD5 Hash Filename: MD5 Hash **Domain(s) and IP(s):** **HTTP URI Indicators:**		
Domain(s) and IP(s):	Ransomware	Trusted Partner
Domain(s) and IP(s):	Zitmo (Zeus-in-the-Mobile) malware	Trusted Partner

[redacted]		
File Indicators: MD5 Hash: [redacted] MD5 Hash: MD5 Hash: MD5 Hash: **Domain(s) and IP(s):** [redacted]	Nuclear Exploit Kit	Trusted Partner

CCIRC Cyber Awareness Products

Alerts

NIL

Advisories

1. AV12-044: Security Updates for Adobe Flash Player

http://www.publicsafety.gc.ca/prg/em/ccirc/2012/av12-044-eng.aspx

Information Notes

NIL

Technical Reports

NIL

Cyber Flashes

2. CF12-017 - Better Business Bureau Phishing Emails Using P2P Zeus Malware Variant

Threat and Vulnerability Monitoring

This section contains threats and vulnerabilities that did not meet the publication criteria for CCIRC products other than operational summaries. It is not meant to be an exhaustive list but rather a heads-up on potentially significant threats and vulnerabilities affecting technologies available to CCIRC communities of interest.

Vulnerabilities

1. Vulnerabilities in Apple Safari (Webkit)

A security researcher reports that use-after-free and race condition vulnerabilities exist in webkit which may be exploited by luring an affected client to a crafted webpage to execute arbitrary code and compromise the system. The vendor has released a patch. CVE-2012-3748 CVE-2012-5112.
References: http://secunia.com/advisories/51157/
http://secunia.com/advisories/51157/
http://securitytracker.com/id/1027716
http://support.apple.com/kb/HT5568

2. Symantec Endpoint Protection CAB File Processing

A remote user can send a specially crafted CAB formatted file to trigger a memory corruption error in 'dec_abi.dll' and execute arbitrary code on the target system. The code will run with System privileges (CVE-2012-4953). A vendor patch is available.
Reference: http://www.kb.cert.org/vuls/id/985625

Threat Watch

1. Ransomware Pretends to be Anonymous

Your computer has been hacked by the Anonymous Hackers Group and locked for the moment. All files have been encrypted. You need to pay a ransom of £100 within 24 hours to restore the computer back to normal…
Associated C&C: [redacted]

SCADA/ICS

1. ICS-CERT - ICSA-12-271-01-C3-ILEX EOSCADA MULTIPLE VULNERABILITIES

Multiple vulnerabilities in the C3-ilex's EOScada application can result in data leakage and a Denial of Service condition. C3-ilex has produced a patch that resolves these vulnerabilities.
Reference: http://www.us-cert.gov/control_systems/pdf/ICSA-12-271-01.pdf

Noteworthy News

1. Phishing Email Hijacks Windows 8 Launch

A new round of emails tries to dupe unsuspecting users to "update" to Windows 8 for free.
Reference: http://www.zdnet.com/phishing-email-hijacks-windows-8-launch-7000006606/

2. Government-Funded Hackers Say They've Already Defeated Windows 8's New Security Measures

On Tuesday the French firm Vupen, whose researchers develop software hacking techniques and sell them to government agency customers, announced that it had already developed an exploit that could take over a Window 8 machine running Internet Explorer 10, in spite of the many significant security upgrades Microsoft built into the latest version of its operating system.
Reference: http://www.forbes.com/sites/andygreenberg/2012/10/31/government-funded-hackers-say-theyve-already-defeated-all-of-windows-8s-new-security-measures/

3. Can the Nuclear exploit kit dethrone Blackhole?

The Nuclear exploit pack has been present for a while now, and its author has recently released version 2.0. He (or she?) advertises it on its own page, likely linked to from a number of underground forum entries. [...]But what differentiates this offer from others is that the cybercriminal is determined not to be blamed for the criminal actions performed by his customers, and he tries to achieve this by introducing Terms of Service that everyone must agree to before using the kit.
Reference: http://www.net-security.org/malware_news.php?id=2308

4. Feds need to add regulations to force Canadians to think about cyber-security, experts say

One day after a top Tory senator suggested the government and Canadians didn't want more regulations on how we use cyberspace, a former British spy chief said that thinking needed to be deleted. Governments need to possibly create more red tape to force companies and individuals to think about cyber-security because too few are doing enough to protect themselves and others from cyber-threats, Sir David Pepper told a security conference Wednesday in Ottawa.
Reference:
http://www.calgaryherald.com/news/national/Feds+need+regulations+force+Canadians+think+about+cyber/7478557/story.html

5. Citadel: a cyber-criminal's ultimate weapon?

In old times, a citadel was a fortress used as the last line of defense. For cyber criminals it is a powerful and state-of-the-art toolkit to both distribute malware and manage infected

computers (bots). Citadel is an offspring of the (too) popular Zeus crimekit whose main goal is to steal banking credentials by capturing keystrokes and taking screenshots/videos of victims' computers. Citadel came out circa January 2012 in the online forums and quickly became a popular choice for criminals. A version of Citadel (1.3.4.5) was leaked in late October and although it is not the latest (1.3.5.1) it gives us a good insight into what tools the bad guys are using to make money. In this post, I will show you how criminals operate a botnet. This is not meant as a tutorial and I do want to stress that running a botnet is illegal and could send you to jail.
Reference:
http://blog.malwarebytes.org/intelligence/2012/11/citadel-a-cyber-criminals-ultimate-weapon/

6. Hacking of Tax Records Has Put States on Guard

The theft of tax information from a South Carolina computer system appears to have been the largest cyberattack ever on a state government and has put other states on high alert, computer security experts say.
Reference:
http://www.nytimes.com/2012/11/06/us/south-carolina-tax-hacking-puts-other-states-on-alert.html?hp

From: Pacha, Tomasz
Sent: Thursday, November 08, 2012 3:02 PM
To: CYBERDO
Cc: Bendelier, Kenneth; Klassen, Nathan; Proulx, Véronique
Subject: RE: CTEC Cyber Report
Attachments: CTA Report - Anonymous.pdf

Thanks Stephen -- much appreciated.

Tom Pacha
Canadian Cyber Incident Response Centre
613-991-3415

-----Original Message-----
From: CYBERDO
Sent: November-08-12 2:59 PM
To: Pacha, Tomasz
Subject: FW: CTEC Cyber Report

Tom,
FYI, Just in case you get other questions.....

Stephen
Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-[redacted] Facsimile | Télécopieur +1 613-991-3574 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: GOC-COG
Sent: Thursday, November 08, 2012 2:42 PM
To: CYBERDO
Subject: CTEC Cyber Report

Cyber DO,

Just in case you don't know of this report. Our DG sent it to GOC Ops Cen as a FYI.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted] <mailto:[redacted]>

From: Oldham, Craig
Sent: November-08-12 2:37 PM
To: GOC-COG; Paquet, Alain; Duschner, Gabrielle; Livingstone, Shane; McLeod, Tim; Mattioli, Mary-Ann
Subject: Fw: CTEC Cyber Report

Info - do not know if GOC is aware.

S. Craig Oldham

Director General / Directeur général

Government Operations Centre / Centre des opérations du gouvernement

613-991-7728 (T) [redacted] (C) [redacted] (S)Craig.Oldham@opscen.gc.ca <mailto:Craig.Oldham@opscen.gc.ca>

From: CTEC [mailto:CTEC@CSE-CST.GC.CA] <mailto:[mailto:CTEC@CSE-CST.GC.CA]>
Sent: Thursday, November 08, 2012 02:34 PM
Subject: CTEC Cyber Report

Classification: UNCLASSIFIED

Dear Cyber Security Stakeholder,
The Cyber Threat Evaluation Centre (CTEC) is an important component of CSEC that analyzes and assesses cyber security threats across the Government of Canada (GC). Accordingly, CTEC produces a wide variety of situational awareness reports on key cyber threats facing the GC. As a member of the Government of Canada IT management community, we believe that this information is imperative to your operations. CTEC is pleased to release a new report for your benefit:

* Cyber Threat Actor Report (CTA) – Anonymous Update

The Cyber Threat Actor Report documents and analyzes the most relevant cyber threat actors affecting the Government of Canada at present. This information is based on recent activity affecting various GC departments in order to better understand the nature of the threat actor. The CTA is a tool to protect government information going forward by identifying the groups likely to target systems of importance to the GC.

CSEC requests that the above mentioned report remains in cryptologic channels; further, we ask that you contact us prior to disseminating to other Government of Canada stakeholders.

CTEC continues to evolve our reporting lines and we welcome any suggestions on how we can better serve the information needs of your department or agency. Attached, please find a feedback form to be completed at your convenience.

We look forward to collaborating with you in the future, Cyber Threat Evaluation Team (CTEC) ctec@cse-cst.gc.ca <mailto:ctec@cse-cst.gc.ca>

Attachments: 1

* Cyber Threat Actor Report (CTA) – Anonymous Update

Please contact ctec@csc-cst.gc.ca <mailto:ctec@csc-cst.gc.ca> should you require the French version of the above documents.

<<CTA Report - Anonymous.pdf>>

Public Safety Canada | Sécurité publique Canada

CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 8 November 2012
CYBERDO: Bruce
****

[FOUO] NEW EVENTS:

1. Title: CE12-003942 - Foreign Government Website Defacement
- Summary:
  CCIRC observed that a website registered by a Forgeign Governement was recently defaced. This was a homepage defacement. The homepage was replaced with an ideological message of an Islamic nature.
- Action/Decision:
  Notification sent to the national CSIRT for that country.
  - Owner: Bruce
  - Status: Closed

2. Title: CE12-003943 [University Website Defacement]
- Summary:
  CCIRC observed that a website registered by a University was recently defaced.
- Action/Decision:
  Notification sent to the technical contact for the university.
  - Owner: Bruce
  - Status: Closed

3. Title: CE12-003944 -DDoS on CI Telecom Client from a [redacted] Source
- Summary:
  Report received from a CI Telecom of an on-going DNS DDoS attack originating from [redacted] targeting the CI Telecom client host. Attack ongoing since 25 Oct 2012. CI Partner requested CCIRC assitance in contacting [redacted] for mitigation.
- Action/Decision:
  CCIRC requested the telecom company provide a short snippet of logs to provide to [redacted] for substantiation.
  - Owner: Bruce
  - Status: Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. Title: CE12-003863 - #OpPartyCrasher Anonymous DDoS
- Update:
  A trusted partner released Update 14: Information Note IN12-002: Anonymous DDoS activity.
-
  - Owner: Bruce
  - Status: Active

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. Item Description: CERT Australia – Update "35 Strategies to Mitigate Targeted Cyber Intrusions" The first 4 of these strategies haven't changed and still mitigate at least 85% of targeted cyber intrusions, however the order has now changed, with Application Whitelisting now the number one strategy in terms of effectiveness. That said, DSD have stated that the first 4 of the 35 strategies should ideally be implemented as a package, with a risk managed approach for the remainder. Reference: http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

PUBLICATIONS: NIL

VULNERABILITY WATCH:NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS:NIL

CYBER NEWS:

1. Item Description: **Adobe, now 'married' to Microsoft, moves Flash updates to Patch Tuesday**

   Adobe on Tuesday announced that it will pair future security updates for its popular Flash Player with Microsoft's Patch Tuesday schedule.

   At the same time, Adobe issued an update that patched seven critical Flash vulnerabilities, and Microsoft shipped fixes for Internet Explorer 10 (IE10), which includes an embedded copy of Flash.

   But the move to synchronize Flash Player updates with Microsoft's monthly patch schedule was the bigger news. "Starting with the next Flash Player security update, we plan to release regularly-scheduled security updates for Flash Player on 'Patch Tuesdays,'" Adobe said in a statement yesterday.

- Reference: http://www.computerworld.com/s/article/print/9233342/Adobe_now_married_to_Microsoft_moves_Flash_updates_to_Patch_Tuesday

2. Item Description: **How to report a computer crime: malware by email**

   Do you know how to report a computer crime? Or even who you would report it to?

   We looked at unauthorised email account access in the first of our series of articles on how to report a computer crime. Now we turn our heads to malware by email.

   We'll look at what offences are committed in different countries when a crime like this happens, how you should report the crime, and what evidence you can preserve.

   ...

   The legal bit

   We've focused on the UK, USA, Canada and Australia, but each country has its own legislation, though the relevant statute often exists to accommodate the same offences in each country.

   ...

   Canada

   The Criminal Code of Canada contains sections that specifically cater for cybercrime, including:

   Unauthorised Use of Computer

   Possession of Device to Obtain Computer

   Mischief in Relation to Data

   Identity Theft and Identity Fraud

   In this case, both Section 342.1 Canadian Criminal Code (CCC) - Unauthorised Use

of a Computer - and Section 430(1.1) CCC - Mischief in Relation to Data (damaging data) - were contravened.

...

Reporting the crime

Reporting the crime

Canada

The Royal Canadian Mounted Police (RCMP) are the main agency with regard to the investigation of federal statutes, but they also have policing responsibility for a number of the Canadian provinces and all 3 territories, as well as some local police services in towns and cities.

A computer crime victim, like Andre, should report their incident to their local police service. If appropriate, it will be escalated for the attention of the agency with federal responsibility, the RCMP.

- Reference: http://nakedsecurity.sophos.com/2012/11/07/how-to-report-a-computer-crime-malware-by-email/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+nakedsecurity+%28Naked+Security+-+Sophos%29

3. Item Description: Experts Warn of Zero-Day Exploit for Adobe Reader
Software vendor Adobe says it is investigating claims that instructions for exploiting a previously unknown critical security hole in the latest versions of its widely-used PDF Reader software are being sold in the cybercriminal underground.

   The finding comes from malware analysts at Moscow-based forensics firm Group-IB, who say they've discovered that a new exploit capable of compromising the security of computers running Adobe X and XI (Adobe Reader 10 and 11) is being sold in the underground for up to $50,000. This is significant because — beginning with Reader X– Adobe introduced a "sandbox" feature aimed at blocking the exploitation of previously unidentified security holes in its software, and so far that protection has held its ground.

- Reference: http://krebsonsecurity.com/2012/11/experts-warn-of-zero-day-exploit-for-adobe-reader/#more-17437

****

CYBER ENVIRONMENT SCANNING:

Websites	Checked
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION:

Page 1124

is a duplicate of

est un duplicata de la

page 1131

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Friday, November 09, 2012 3:00 PM
To: CYBERDO
Cc: CTEC
Subject: FW: www.conservative.ca site [redacted] #OpPartyCrasher
Attachments: Screen Shot 2012-11-09 at 2.09.26 PM.png; Screen Shot 2012-11-09 at 2.12.58 PM.png

Classification: UNCLASSIFIED

Pse see attached if you haven't already been notified or are aware.

Cheers,

[redacted]

[redacted]
Incident Handler
Cyber Threat Evaluation Centre
[redacted]
ctec@cse-cst.gc.ca

To report incidents affecting GC infrastructures contact GC-CTEC at ctec@cse-cst.gc.ca. Any government department suspecting cyber incidents should provide a written report to GC-CTEC.

-----Original Message-----
Good Afternoon,

I just saw the following #OpPartyCrasher [redacted]

[redacted]

Page 1126

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

From: Beaudoin, Luc
Sent: Friday, November 09, 2012 4:49 PM
To: Bendelier, Kenneth; CYBERDO
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Cyberdo, can you forward to ken the email in this event folder which was sent from CCIRC-CCRIC, with attachments and start with "this is in response to your request for information"....

----- Original Message -----
From: Bendelier, Kenneth
Sent: Friday, November 09, 2012 04:42 PM
To: Beaudoin, Luc
Subject: Re: CCIRC CE12-003863 [redacted]Anonymous DDoS - Update]

Will do...can u resend one of those to me please :-D

----- Original Message -----
From: Beaudoin, Luc
Sent: Friday, November 09, 2012 04:36 PM
To: Bendelier, Kenneth; CYBERDO
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Of course. If you do, add all content which also sent to ON and AB.

----- Original Message -----
From: Bendelier, Kenneth
Sent: Friday, November 09, 2012 03:53 PM
To: CYBERDO
Cc: Beaudoin, Luc
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Merci IH.

May I share with NCSIP?

----- Original Message -----
From: CYBERDO
Sent: Friday, November 09, 2012 03:51 PM
To: Bendelier, Kenneth
Cc: Beaudoin, Luc
Subject: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Good Evening Ken;

Update received from GC/CTEC on current Op Party Crasher activity.

[redacted]

[redacted]

Bruce Moore
Incident Handler | Gestionnaire d'incident Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-7792
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: NCSIP@lists.gov.ns.ca
Sent: Friday, November 09, 2012 5:11 PM
To: Listserver NCSIP
Cc: Beaudoin, Luc
Subject: Fw: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]
Attachments:

Importance: High

This message sent from: PS - Ken Bendelier <Kenneth.Bendelier@ps-sp.gc.ca>

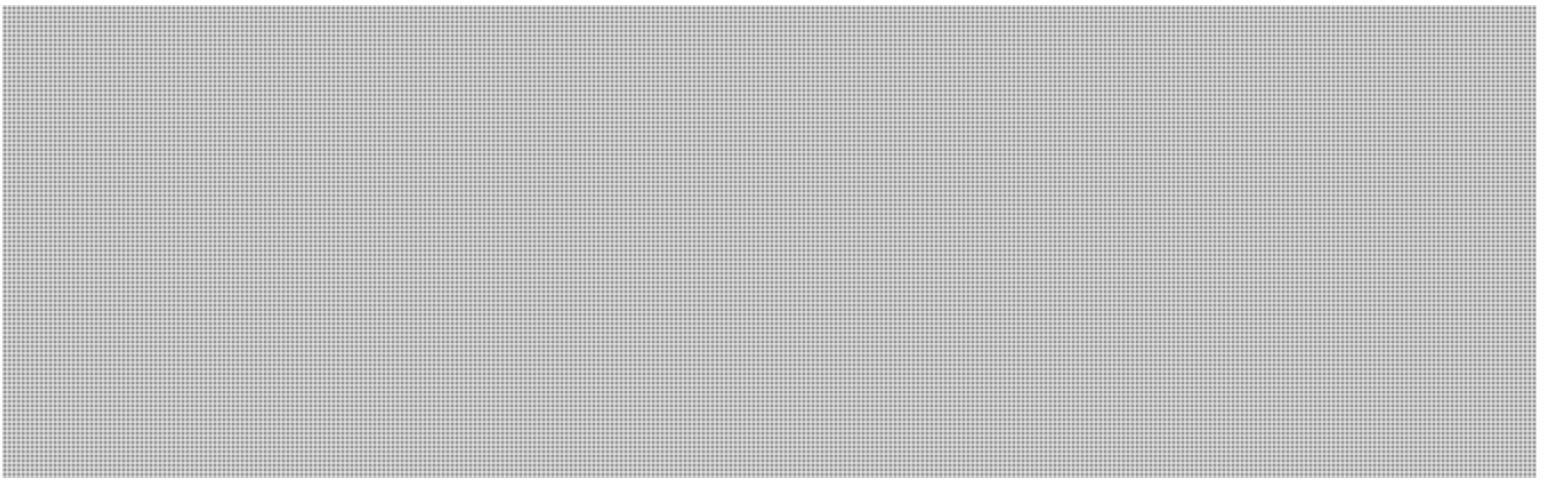
FYI. A second message with indicators will follow.

For internal use for awareness and defensive measures only please.

----- Original Message -----
From: CYBERDO
Sent: Friday, November 09, 2012 03:51 PM
To: Bendelier, Kenneth
Cc: Beaudoin, Luc
Subject: CCIRC CE12-003863

Good Evening Ken;

Update received from GC/CTEC on current Op Party Crasher activity.



Bruce Moore
Incident Handler | Gestionnaire d'incident Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-7792
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

---

NCSIP Sharepoint Site: https://cdms.ext.gov.ab.ca

You are currently subscribed to ncsip@lists.gov.ns.ca as: [redacted]
To unsubscribe click here:
[redacted] s.16(2)(c)
or send a blank email to [redacted]

From: NCSIP@lists.gov.ns.ca
Sent: Friday, November 09, 2012 5:12 PM
To: Listserver NCSIP
Subject: Fw: CE12-003863 [#OpPartyCrasher - www.conservative.ca]
Attachments:

This message sent from: PS - Ken Bendelier <Kenneth.Bendelier@ps-sp.gc.ca>

The second message.

Please advise as to relevance to your needs at your convenience.

----- Original Message -----
From: CYBERDO
Sent: Friday, November 09, 2012 05:04 PM
To: Bendelier, Kenneth
Subject: FW: CE12-003863 [#OpPartyCrasher - www.conservative.ca]

This is the email sent earlier today to See attachments and comments below.

Bruce

-----Original Message-----
From: CCIRC-CCRIC
Sent: November-09-12 6:52 AM
To:
Cc:
Subject: CE12-003863 [#OpPartyCrasher - www.conservative.ca]

Greetings,

In the immediate follow the step below;

- Establish contact with your technical team or host provider.

- Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.

- Establish 24/7 contact information for your ISP and alternate methods for communications.

- Finally CCIRC would like to have the server logs if possible for our future analysis.

Note: find attached analysis of the potential tools and the pastebay post referencing conservative.ca.

Cyber Duty Officer | Officier de veille cybernétique

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-

Facsimile | Télécopieur +1 613-991-3574

Government of Canada | Gouvernement du Canada

NCSIP Sharepoint Site: https://cdms.ext.gov.ab.ca

s.16(2)

s.16(2)(c)

You are currently subscribed to ncsip@lists.gov.ns.ca as:

To unsubscribe click here:

or send a blank email to

From: Beaudoin, Luc
Sent: Friday, November 09, 2012 11:25 PM
To: 'GCCTEC3.Blackberry@CSE-CST.GC.CA'; 'CTEC@CSE-CST.GC.CA'
Cc: CYBERDO
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

That sounds like the first comment I heard but they mixed it with anonymous making it impossible to understand.

Tx. We have clarity at last !

Luc

----- Original Message -----
From: Blackberry, GCCTEC3 [mailto:GCCTEC3.Blackberry@CSE-CST.GC.CA]
Sent: Friday, November 09, 2012 09:29 PM
To: CTEC <CTEC@CSE-CST.GC.CA>; Beaudoin, Luc
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Hi Luc,

Is this the article that relates?

http://www.cbc.ca/m/rich/canada/story/2012/11/09/pol-cp-cyber-attacks-canada-host-public-safety.html

Do you know if there is a transcript of the 17h00 french broadcast.

Cheers

----- Original Message -----
From: CTEC
Sent: Friday, November 09, 2012 04:57 PM
To: Blackberry, GCCTEC1; Blackberry, GCCTEC2; Blackberry, GCCTEC3
Subject: FW: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

From: Beaudoin, Luc[SMTP:LUC.BEAUDOIN@PS-SP.GC.CA]
Sent: November 9, 2012 4:57:22 PM
To: CTEC; Bendelier, Kenneth; CYBERDO
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update] Auto forwarded by a Rule

Agreed. Wasn t in 1630h news, so waiting for the hour one but the statement from the announcer was really odd and was referring to a PS statement... Maybe in the news later. We ll see. Tx.

----- Original Message -----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, November 09, 2012 04:49 PM

To: Beaudoin, Luc; Bendelier, Kenneth; CYBERDO
Cc: CTEC <CTEC@CSE-CST.GC.CA>
Subject: RE: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Classification: UNCLASSIFIED

Hi Luc,

This angle does not make any sense from CTEC's perspective. The only information we released was in the update that you received.

Regards,

Cyber Threat Evaluation Centre
CTEC@CSE-CST.GC.CA


-----Original Message-----
From: Beaudoin, Luc [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: November 9, 2012 4:21 PM
To: Bendelier, Kenneth; CYBERDO
Cc: CTEC
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

The news are announcing right now (CBC radio French, 1630h news) that PS is concerned that gov websites may be used in these attacks, and not only as targets. This is really odd.

Bruce or vireak, we need to check we comdo is PS is making a public announcement on this and ensure it is accurate. Also check with CTEC if this makes any sense (did they release anything that could be interpreted as such?)

Luc

----- Original Message -----
From: Bendelier, Kenneth
Sent: Friday, November 09, 2012 03:58 PM
To: CYBERDO
Cc: Beaudoin, Luc
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Thanks.

If we do share, it may be better coming from the CCIRC e-mail so we reinforce that as our unified distribution point.

If we don't share, understandable. This info will help a lot in case I get a question.

At any rate, thanks Bruce. You rock, as always.

----- Original Message -----
From: CYBERDO
Sent: Friday, November 09, 2012 03:54 PM
To: Bendelier, Kenneth; CYBERDO
Cc: Beaudoin, Luc
Subject: RE: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

I don't see why not unless the Ops Manager disagrees.

Bruce

-----Original Message-----
From: Bendelier, Kenneth
Sent: November-09-12 3:53 PM
To: CYBERDO
Cc: Beaudoin, Luc
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

s.16(2)

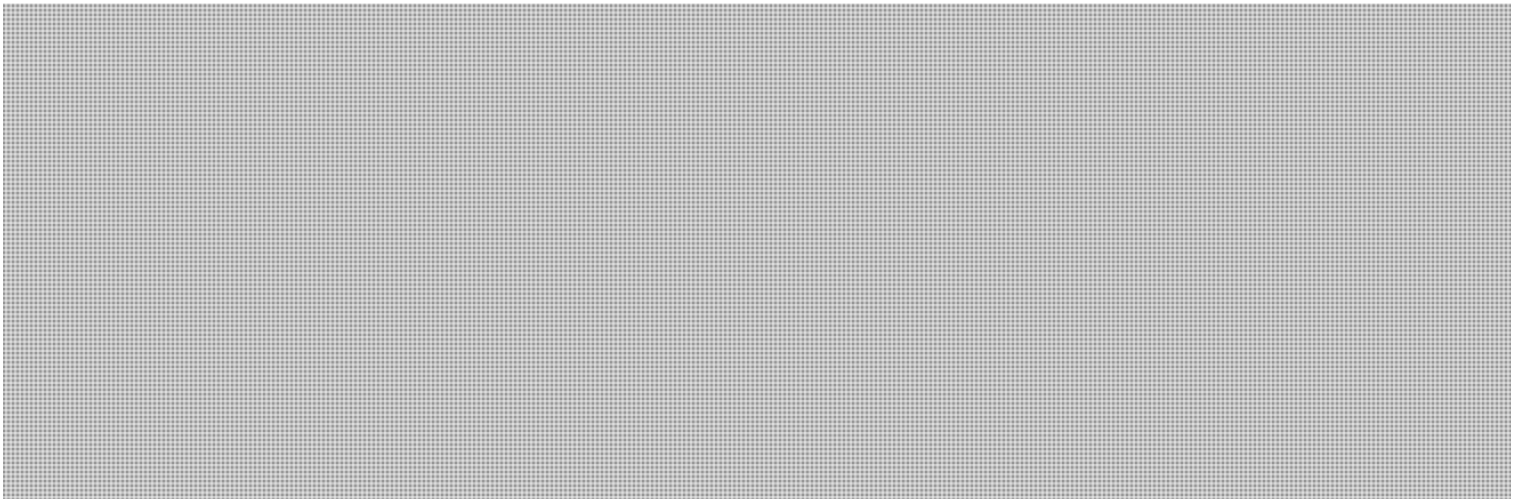
Merci IH.

May I share with NCSIP?

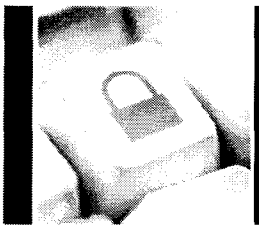
----- Original Message -----
From: CYBERDO
Sent: Friday, November 09, 2012 03:51 PM
To: Bendelier, Kenneth
Cc: Beaudoin, Luc
Subject: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Good Evening Ken;

Update received from GC/CTEC on current Op Party Crasher activity.



Bruce Moore
Incident Handler | Gestionnaire d'incident Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-7792
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada



CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 10 November 2012
CYBERDO: Bruce
****

[FOUO] NEW EVENTS:

1. Title: CE12-003953 - Conficker notifications
- Summary:
  Canada Drone Report: 2012-11-07 notifications to multiple organizations. Hosts within these organizations were infected with Conficker botnet malware.
  Number of affected organisations receiving a notification: 150
    - Provincial: 4
    - Telecom: 110
    - Energy: 3
    - Transportation: 1
    - Manufacturing & Retail: 1
    - Health: 3
    - Academia(all): 28
- Action/Decision:
  Notifications sent to IT security or technical contacts.
  - Owner: Steve
  - Status: Active

2. Title: CE12-003954 - Zeus notifications
- Summary:
  Trusted partner data source report: notifications to multiple organizations. Hosts within these organizations were infected with Zeus malware.
    - Provincial:1
    - Municipal:1
    - Telecom: 66
    - Energy:3
    - Transportation:1
    - Manufacturing & Retail:1
    - Health:1
    - Academia(all):16
- Action/Decision:
  Notifications sent to IT security or technical contacts

- Owner: Steve
- Status: Active

3. Title: CE12-003956 - Code Injecton Attack against Foreign Government Website
- Summary:
  CCIRC received a report from a Foreign Government CSIRT regarding a code injection attack against their Government's website that involved several Canadian IP addresses.
- Action/Decision:
  CCIRC sent a message to the CSIRT requesting additional technical details, logs or analysis that they may have related to this event. After discussion with our tech team, there is no sufficient evidence, without additional context and technical documentation, that these IP addresses were involved.
  - Owner: Bruce
  - Status: Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. Title: CE12-003863 [#OpPartyCrasher Anonymous DDoS]
- Update:
  Message sent to the targeted(identified by Anonymous) website hosting provider regarding the Tweets posted by Anonymous containing crafted links that are being used to take advantage of a minor flaw in the targeted website. (Sample URL provided)
- Action/Decision:

  - Owner: Bruce
  - Status: Active

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS: NIL

PUBLICATIONS: NIL

VULNERABILITY WATCH:NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS:

1. Item Description: **Remote Diagnostics with PSR**
   Have you ever been in this situation? Someone calls you for help and tries to explain their problem. They do such a poor job of explaining what they are seeing that you aren't even sure what OS they are using much less how to fix their problem. You wish you had some way of remotely seeing their desktop, but the user is incapable of following instructions required for you to remotely connect to and administer their machine. This is especially frustrating when you are in the identification or containment phase of an incident. Communications is an essential element of handling incidents effectively. When you are in a pinch, here is a new tool to add to your tool belt.
   Microsoft Windows 7 has a tool called PSR (Problem Sequence Recorder). PSR will capture screen images, mouse clicks and some keyboard input and put in into a zip file that can be emailed back to you. The information is recorded in the sequence that the user sees it. You can see what they clicked and the order in which they clicked it. You can see what was on their screen and to a very limited extent what they typed. If you just run PSR.EXE it will bring up a GUI (graphical user interface). It is really easy to use. It has a start button and a stop button. When you click stop it prompts you to save a file. It produces a zip file containing the diagnostic information that the user can email to you (assuming that they have SOME connectivity).
- Reference: https://isc.sans.edu/diary/Remote+Diagnostics+with+PSR/14485

CYBER NEWS:

1. Item Description: **New Dead drop techniques used by Security Agencies**
   What is a dead drop? It is methods that spies use or have used to communicate with associates who have information for them. The dead drop allows them to exchange information without having actual physical contact with each other. The person leaving the information can leave it under a rock or a can or bush. A special type of empty spikes that can be dropped into holes has also been used drop information. The person leaving the information also leaves some kind of signal the drop was made. The signal could be a chalk marks on a tree or pavement. Someone views the signal and retrieves information.
- Reference: http://thehackernews.com/2012/11/new-dead-drop-techniques-used-by.html#sthash.nsvMUb2b.dpbs

2. Item Description: **Out of date, vulnerable browsers put users at risk**
   Is your browser up to date? According to the results of a new survey from Kaspersky—a security software vendor—nearly a quarter of the browsers currently in use are out of date. Surfing the Web with a vulnerable browser is a recipe for disaster.
   The Web browser has evolved to become the primary software used on many PCs.

People access their email, surf websites, create documents and spreadsheets, access cloud-based file storage and sharing sites, and share with others on social networking sites—all through the browser. Attackers no this as well, which is why it is exceptionally risky to use a browser with known vulnerabilities.

- Reference: http://www.pcworld.com/article/2013737/out-of-date-vulnerable-browsers-put-users-at-risk.html

3. Item Description: **Trusted computing for industrial control systems and infrastructure**

Beyond the Stuxnet worm that targeted industrial software and equipment, supervisory control and data acquisition (SCADA) attacks are becoming increasingly common.

In an article for the Wall Street Journal on taking the cyber attack threat seriously, Barack Obama noted: "Last year, a water plant in Texas disconnected its control system from the internet after a hacker posted pictures of the facility's internal controls.

"More recently, hackers penetrated the networks of companies that operate our natural gas pipelines. Computer systems in critical sectors of our economy – including the nuclear and chemical industries – are being increasingly targeted."

- Reference: http://www.computerweekly.com/opinion/Trusted-computing-for-industrial-control-systems-and-infrastructure

4. Item Description: **Persistent Threat Detection on a Budget**

If there's one simple – high impact – thing you could do to quickly check whether your network has been taken over by a criminal entity, or uncover whether some nefarious character is rummaging through your organizations most sensitive intellectual property out of business hours, what would it be? In a nutshell, I'd look to my DNS logs.

Whenever an electronic intruder employs their tools to navigate your network, tries to connect back to their command and control server, or attempts to automatically update the malicious binaries they've installed upon the system they have control over (or wish to control), those victim devices tend to repeatedly resolve the domain names that that attacker is operating from.

- Reference: https://blog.damballa.com/archives/1834

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒

SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION: NIL

From: Beaudoin, Luc
Sent: Saturday, November 10, 2012 10:25 AM
To: Swift, Andrew; Champoux, Martin; Bendelier, Kenneth; CYBERDO
Cc: Anderson, Windy; 'CTEC@CSE-CST.GC.CA'
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Yes, CTEC sent me that story found here: http://www.cbc.ca/m/rich/canada/story/2012/11/09/pol-cp-cyber-attacks-canada-host-public-safety.html

There were 2 stories. One on the latter and one on anonymous threat to the GC referring to a CSEC note probably. The problem is that the 2 stories were mixed together into a single story which made no sense in the 17h radio bulletin from radio-canada yesterday. They stated something along the line that GC was targeted and these attacks generally came from south africa, eastern europe etc. And they attributed part of it to CSEC. Didn t sound very good (ie point to other countries).

Probably not a big deal.

Cheers

Luc

----- Original Message -----
From: Swift, Andrew
Sent: Saturday, November 10, 2012 09:38 AM
To: Champoux, Martin; Beaudoin, Luc; Bendelier, Kenneth; CYBERDO
Cc: Anderson, Windy; 'CTEC@CSE-CST.GC.CA' <CTEC@CSE-CST.GC.CA>
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Martin,
Only story I saw yesterday was the following, based on an ATI.
Andrew

Canada becoming 'host' country for cyber attackers, government fears November 9, 2012, 15:59 ET Canadian Press, By: Jim Bronskill

OTTAWA _ The Public Safety Department worries Canada is becoming a digital launching pad for _ not just a target of _ malicious cyber-activities, confidential briefing notes reveal.

Traditionally, most cyber-criminals are known for plotting their online schemes in places like Eastern Europe, East Asia and Africa, say departmental notes prepared for a closed-door meeting of the Cross-Cultural Roundtable on Security.

``This may be shifting to more developed countries such as Canada, the U.S. and France _ countries with good reputations,'' say the notes, obtained by The Canadian Press under the Access to Information Act.

``Plainly said, we may be moving from being mostly 'targets' of organized cyber-crime hosted in outside jurisdictions, to 'hosts' of online cyber-crime operations and activities.''

The notes were drafted for an introductory discussion by Brett Kubicek, Public Safety's manager of research and academic relations, at the roundtable's June meeting.

The roundtable, which comprises members of various ethnic backgrounds, tries to foster dialogue on security issues between government officials and minority communities.

``When it comes to cyberspace, it's likely that the flow of questions facing policy-makers will continue to outpace readily available and clear solutions for the foreseeable future,'' say Kubicek's notes.

His comments followed an explicit warning from the Canadian Security Intelligence Service about homegrown websites that support and incite terrorist violence.

They also echoed findings of digital security company Websense, which singled out Canada as a breeding ground for Internet nastiness in its two latest annual surveys.

Last spring, Websense said Canada ranked No. 2 in the world _ ahead of prime offenders Egypt and Russia _ for hosted phishing sites that lure unsuspecting people into providing personal information like credit card numbers.

It also noted a 39-per-cent increase in Canadian-hosted ``bot networks,'' the command-and-control centres for cyber-criminals, as well as a 239-per-cent jump in potentially infectious and otherwise dangerous Canadian websites.

``Across the board, we're seeing all types of malicious content coming out of the Great White North,'' the company said in May.

``Even after last year's discovery, we still have not seen any big takedowns of malicious sites in Canada. In fact, malicious sites seem to stay up longer than in other countries.''

In July it was reported that Farsi-speaking hackers used four cyber-bases in Canada to steal confidential materials from hundreds of government officials and businesspeople in Afghanistan, Iran and Israel.

The roundtable proceedings clearly indicate Canadian officials are just beginning to grapple with a problem that will only grow.

In his remarks, Kubicek noted the ``ever-expanding mismatch'' between the growing online dimension of Canadian lives and the body of laws, regulations and policies developed largely for an ``offline'' world.

A Justice Department briefing prepared for the June roundtable meeting says challenges include the appropriateness of existing laws for criminal behaviour and the need for new ones to address the changing environment.

``Cyberspace presents challenges for Canadian legislation and for law enforcement as technology evolves rapidly,'' says the presentation. ``Legal frameworks and investigative practices are challenged to keep pace with this evolution.''

Since technological shifts happen much faster than legislative change, the preferred strategy is to draft technology-neutral laws to the extent possible, the department adds.

Other considerations include combating cyber-crime without eroding privacy and co-operating with other countries to tackle the global nature of illicit online activities.

Federal Auditor General Michael Ferguson recently found the government had been slow to mount an effective response to the rapidly growing threat of cyber-attacks on key systems.

The government has made only limited progress in shoring up computer networks and lags in building partnerships with other players, Ferguson said. The federal cyber-incident response centre doesn't even operate around the clock, he added.

Following the report's release, Public Safety Minister Vic Toews acknowledged that cyber-threats were not considered a priority until recently.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

----- Original Message -----
From: Champoux, Martin
Sent: Saturday, November 10, 2012 09:30 AM
To: Beaudoin, Luc; Bendelier, Kenneth; CYBERDO
Cc: Anderson, Windy; 'CTEC@CSE-CST.GC.CA' <CTEC@CSE-CST.GC.CA>; Swift, Andrew
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Only just saw this e-mail. Will do some digging on it on Monday.

----- Original Message -----
From: Beaudoin, Luc
Sent: Friday, November 09, 2012 05:22 PM
To: Bendelier, Kenneth; Champoux, Martin; CYBERDO
Cc: Anderson, Windy; 'CTEC@CSE-CST.GC.CA' <CTEC@CSE-CST.GC.CA>
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Ok, it was in the 17h news. A 20 second segment just quoting CSEC as saying cyber attacks may be targeting federal systems in the upcoming days, and that such attacks often come from France, south africa and asia...

Which product makes that link with source countries ? Definitely not a good public statement as these countries could easily say just the same about Canada...

Nothing on gov being the source. That was the announcer s own interpretation, mistaken.

Luc

----- Original Message -----
From: Beaudoin, Luc
Sent: Friday, November 09, 2012 04:32 PM
To: Bendelier, Kenneth; Champoux, Martin; CYBERDO
Cc: Anderson, Windy
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

News now. I am listening to it and I ll report on details... I hope I misunderstood the lady pre-announcing it....

----- Original Message -----
From: Beaudoin, Luc
Sent: Friday, November 09, 2012 04:27 PM
To: Bendelier, Kenneth; Champoux, Martin

Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Martin, as tu une idee ?

----- Original Message -----
From: Bendelier, Kenneth
Sent: Friday, November 09, 2012 04:23 PM
To: Beaudoin, Luc
Subject: Re: CCIRC CE12-003863 [Anonymous DDoS - Update]

Ask Champeaux

----- Original Message -----
From: Beaudoin, Luc
Sent: Friday, November 09, 2012 04:20 PM
To: Bendelier, Kenneth; CYBERDO
Cc: 'CTEC@CSE-CST.GC.CA' <CTEC@CSE-CST.GC.CA>
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

The news are announcing right now (CBC radio French, 1630h news) that PS is concerned that gov websites may be used in these attacks, and not only as targets. This is really odd.

Bruce or vireak, we need to check we comdo is PS is making a public announcement on this and ensure it is accurate. Also check with CTEC if this makes any sense (did they release anything that could be interpreted as such?)

Luc

----- Original Message -----
From: Bendelier, Kenneth
Sent: Friday, November 09, 2012 03:58 PM
To: CYBERDO
Cc: Beaudoin, Luc
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Thanks.

If we do share, it may be better coming from the CCIRC e-mail so we reinforce that as our unified distribution point.

If we don't share, understandable. This info will help a lot in case I get a question.

At any rate, thanks Bruce. You rock, as always.

----- Original Message -----
From: CYBERDO
Sent: Friday, November 09, 2012 03:54 PM
To: Bendelier, Kenneth; CYBERDO
Cc: Beaudoin, Luc
Subject: RE: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

I don't see why not unless the Ops Manager disagrees.

Bruce

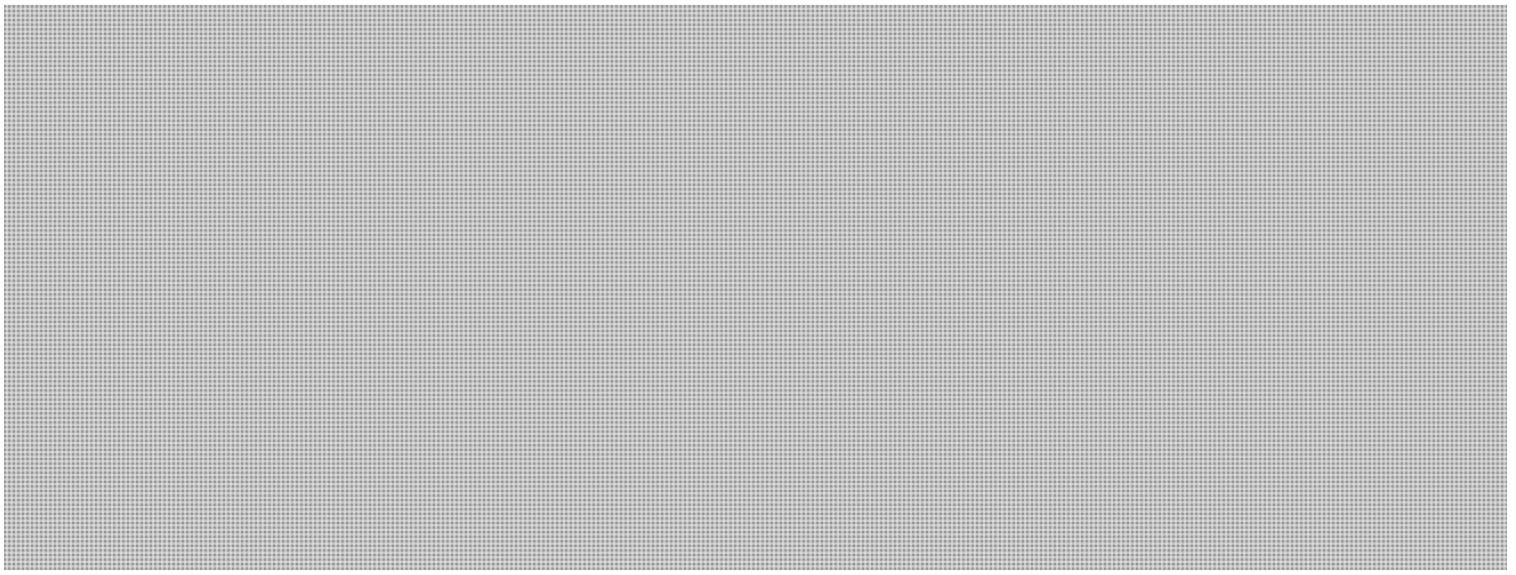
-----Original Message-----
From: Bendelier, Kenneth
Sent: November-09-12 3:53 PM
To: CYBERDO
Cc: Beaudoin, Luc
Subject: Re: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Merci IH.

May I share with NCSIP?

----- Original Message -----
From: CYBERDO
Sent: Friday, November 09, 2012 03:51 PM
To: Bendelier, Kenneth
Cc: Beaudoin, Luc
Subject: CCIRC CE12-003863 [OpPartyCrasher Anonymous DDoS - Update]

Good Evening Ken;



Bruce Moore
Incident Handler | Gestionnaire d'incident Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-7792
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: Mail Delivery System <MAILER-DAEMON@
To:
Sent: Monday, November 12, 2012 5:08 PM
Subject: Undeliverable: CE12-003863 [- www.conservative.ca]

Delivery has failed to these recipients or groups:

A problem occurred during the delivery of this message to this e-mail address. Try sending this message again. If the problem continues, please contact your helpdesk.

The following organization rejected your message: [.

Page 1149

is withheld pursuant to sections

est retenue en vertu des articles

16(2), 16(2)(c)

of the Access to Information

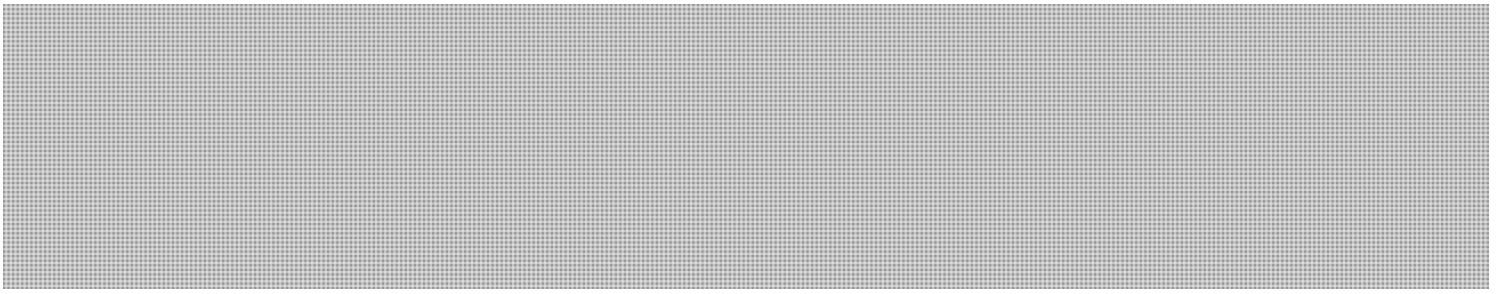
de la Loi sur l'accès à l'information

From: Bendelier, Kenneth
Sent: Tuesday, November 13, 2012 3:47 PM
To: Beaudoin, Luc; CYBERDO; Dick, Robert
Subject: Re: DDoS

Merci Luc,

IH, as always, rocks!

----- Original Message -----
From: Beaudoin, Luc
Sent: Tuesday, November 13, 2012 03:44 PM
To: Bendelier, Kenneth; CYBERDO
Subject: RE: DDoS



Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Bendelier, Kenneth
Sent: Tuesday, November 13, 2012 3:34 PM
To: Beaudoin, Luc; CYBERDO
Subject: Fw: DDoS

Help please.

----- Original Message -----
From: Dick, Robert
Sent: Tuesday, November 13, 2012 03:32 PM
To: Bendelier, Kenneth; [redacted]@CSE-CST.GC.CA' <[redacted]@CSE-CST.GC.CA>
Subject: DDoS

Our M.O. is asking for an update re Govt and the November campaign in general.

Nothing fancy: please let me know if there's anything new and if so what, or all is fine / quiet.

Thx

From: Breault, Stephen
Sent: Wednesday, November 14, 2012 2:53 PM
To: Bendelier, Kenneth; CYBERDO
Subject: RE: Update 18: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Yes that is correct...

-----Original Message-----
From: Bendelier, Kenneth
Sent: Wednesday, November 14, 2012 2:50 PM
To: CYBERDO
Subject: Re: Update 18: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Thanks.

The non-GC targets were advised they were potential targets?

----- Original Message -----
From: CYBERDO
Sent: Wednesday, November 14, 2012 02:44 PM
To: Bendelier, Kenneth
Subject: FW: Update 18: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

FYSA.

Chris

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 14, 2012 2:44 PM
To: CTEC
Subject: Update 18: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC
Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 14 November 2012
==========

NOTICE:

==========

Update 18: 14 November 2012

- Updated assessment information

==========

==========

Anonymous DDoS activity against GC

==========

AUDIENCE

========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE

=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT

==========

Page 1154

is withheld pursuant to section

est retenue en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

s.16(2)

SUGGESTED ACTION
==========

[redacted]

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here:
http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Thursday, November 15, 2012 2:50 PM
To: CTEC
Subject: Update 19: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 15 November 2012
==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

==========
Update 19: 15 November 2012
- Updated assessment information and suggested action
==========

s.16(2)

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

[redacted]

[redacted]

SUGGESTED ACTION
==========

GC-CTEC coordinated the incident response and the threat evaluation for this event. Shared Services Canada led the mitigation effort [redacted]

Departments should ensure that their Business Continuity Plans are updated and current.

If a department is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps

ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

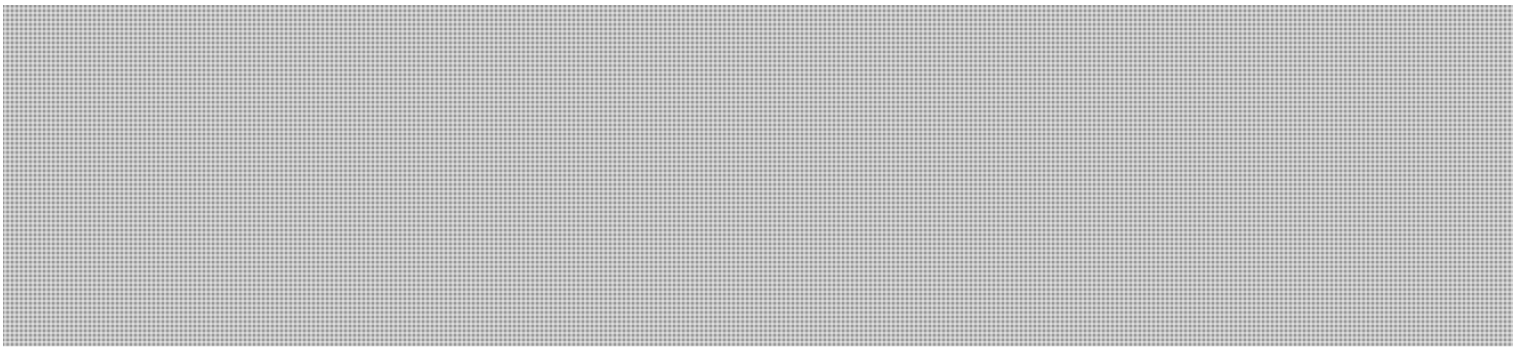
From: Mattioli, Mary-Ann
Sent: Friday, November 16, 2012 10:47 AM
To: Pacha, Tomasz
Cc: Bendelier, Kenneth; Proulx, Véronique; CYBERDO; Klassen, Nathan
Subject: RE: CCIRC Weekly Technical Report 07 Nov 2012

Thank you.

s.16(2)

-----Original Message-----
From: Pacha, Tomasz
Sent: November-16-12 10:04 AM
To: Mattioli, Mary-Ann
Cc: Bendelier, Kenneth; Proulx, Véronique; CYBERDO; Klassen, Nathan
Subject: RE: CCIRC Weekly Technical Report 07 Nov 2012

Good morning Mary-Ann,



Tom Pacha
Canadian Cyber Incident Response Centre
613-991-3415

-----Original Message-----
From: Bendelier, Kenneth
Sent: November-16-12 9:29 AM
To: Mattioli, Mary-Ann; Klassen, Nathan
Cc: Proulx, Véronique; Pacha, Tomasz
Subject: Re: CCIRC Weekly Technical Report 07 Nov 2012

Neither one of us are here...

Vero or tom

----- Original Message -----
From: Mattioli, Mary-Ann
Sent: Friday, November 16, 2012 09:27 AM
To: Bendelier, Kenneth; Klassen, Nathan

Subject: RE: CCIRC Weekly Technical Report 07 Nov 2012

[redacted]

Thanks!

-----Original Message-----
From: Bendelier, Kenneth
Sent: November-14-12 3:01 PM
To: Klassen, Nathan; Mattioli, Mary-Ann
Subject: Re: CCIRC Weekly Technical Report 07 Nov 2012

s.16(2)

Let's be careful on wording and slippery slope things here. An MP's personal website is not an attack on a government entity anymore than an attack on CUPE would be. [redacted] is a valid government entity. The others.....

----- Original Message -----
From: Klassen, Nathan
Sent: Wednesday, November 14, 2012 02:55 PM
To: Mattioli, Mary-Ann
Subject: RE: CCIRC Weekly Technical Report 07 Nov 2012

Yes to [redacted] Anonymous has claimed responsibility for the majority of the attacks. Few suggested edits below.

[redacted]

-----Original Message-----
From: Mattioli, Mary-Ann
Sent: Wednesday, November 14, 2012 1:18 PM
To: Klassen, Nathan
Subject: FW: CCIRC Weekly Technical Report 07 Nov 2012

Hi Nate,

Hi Nate,

In this report, did Anonymous attack the [redacted] as well? Also, did Anonymous claim responsibility for all of the attacks?

[redacted]

Thanks, Mary-Ann

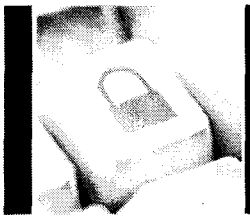
-----Original Message-----
From: GOC-COG
Sent: November-09-12 6:47 PM
To: * GOC-SOO / COG-APO; * GOC-Analysis / COG-Analyse
Subject: CCIRC Weekly Technical Report 07 Nov 2012

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

-----Original Message-----
From: CCIRC-CCRIC
Sent: November-09-12 6:28 PM
Subject: CCIRC Weekly Technical Report 07 Nov 2012

Incident Handler | Gestionnaire d'incident Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-7792 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

Public Safety Canada | Sécurité publique Canada



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CCIRC CYBER OPERATIONAL SUMMARY

REPORTING PERIOD: NOVEMBER 25 – DECEMBER 8, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-020

PURPOSE

This product is intended to provide cyber information to partners and operators of vital systems in public and private sectors, in order to support operational and security decision-making in these organizations. It is based on information reported to and researched by the Canadian Cyber Incident Response Centre (CCIRC), and may not be indicative of the cyber environment in Canada.[1] This report also provides background information on the technical products released by CCIRC over the reporting period.

Highlights

- Spear phishing targets Canadian power generating organization.

- Canadian organization successfully coerced with a denial-of-service attack.

In the news:

- Cyber attack reporting could boost defence capability.

- Contact information of United Nations agency scientists released by hackers.

OVERVIEW

During this reporting period, CCIRC handled 49 incidents. Some of those reported to CCIRC included:

- An oil and gas organization reports a significant compromise;
- Hacktivists reportedly targeting the Canadian critical infrastructure sector organizations; and
- A provincial organization's website hosted malvertising.

PRODUCTS RELEASED

CCIRC regularly issues information products to inform its partners of potential, imminent or actual cyber threats. During the reporting period, CCIRC issued an update to a previously released cyber flash (*CF12-009 Update 4: Airline Company Email Phishing Campaign*) after it received new reports of ongoing phishing campaigns falsely representing an airline company in order to deliver malware to recipients.

[1] Additional reporting by partners would help CCIRC contribute to a more accurate Canadian picture.

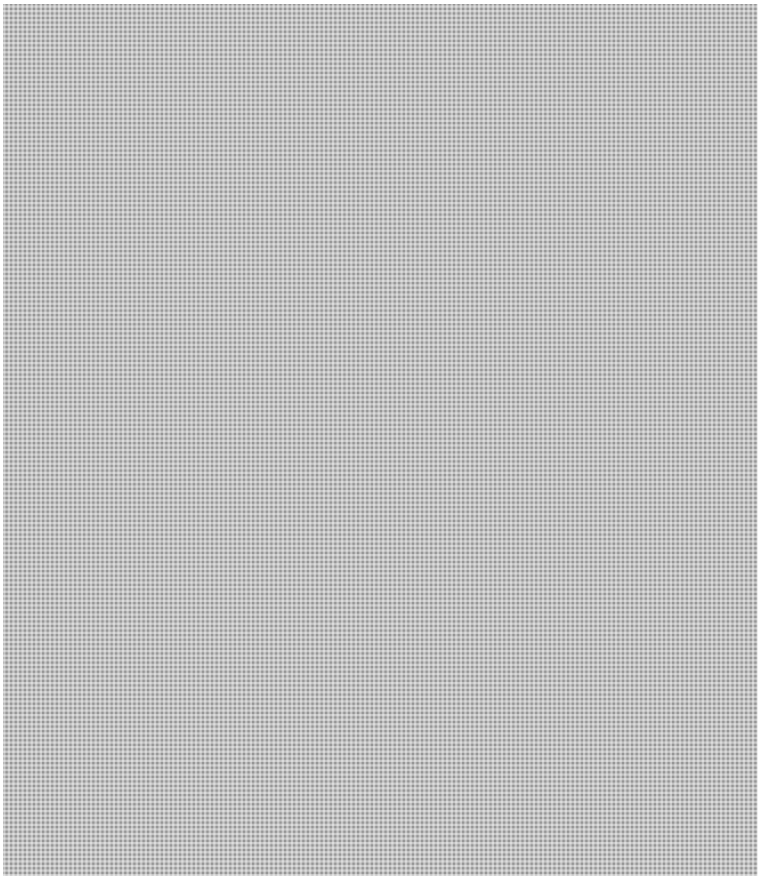
Canada

NEW INCIDENTS

Private Sector

Canadian energy company reports compromise – Trusted sources informed CCIRC of a potential compromise at a large Canadian oil and gas company. CCIRC notified the company and provided them with initial information to help them assess and mitigate this incident.

> *Comment: As of this writing, this incident is ongoing. CCIRC is collaborating with federal partners and with the affected company to assess and, if required, mitigate the situation.*



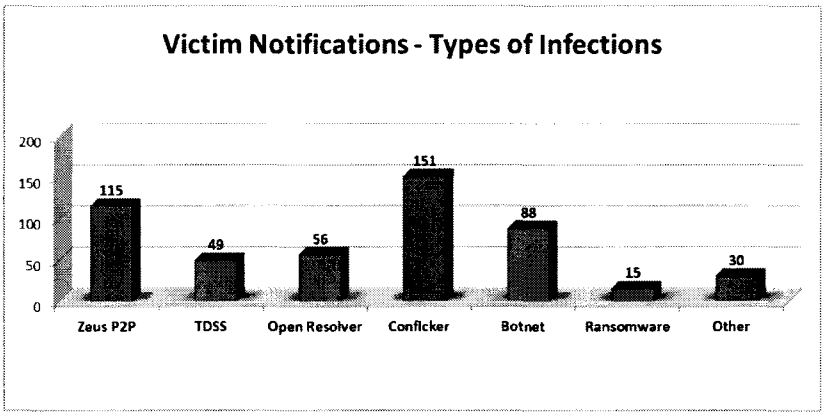
Canadian electric power organization targeted by spear phishing – As a result of the organization's defensive posture, the malware contained within these targeted emails was detected prior to exploitation, and the organization was not impacted by this malware. The organization provided malware samples to CCIRC, and CCIRC's analysis revealed that the malware was designed to give its authors network access commensurate with the rights of the victim.

Anonymous campaign reportedly targeting Canadian critical infrastructure – The hacktivist group Anonymous announced several targets in the Canadian energy and utilities, information and communication technology (ICT), manufacturing, and food sectors in a continuation of its #OpPartyCrasher.

> *Comment: CCIRC notified the targeted organizations but is not aware of any impact on these organizations at this time, and continues to collaborate with federal partners to monitor the situation. In November 2012, open sources indicated that Anonymous' #OpPartyCrasher had targeted Canadian government entities with distributed denial-of-service (DDoS) attacks.*

Canadian organization successfully coerced with denial-of-service (DoS) attack – A trusted partner informed CCIRC that a Canadian organization had been coerced with a DoS attack. The victim organization had refused to pay the hacking group initially as the threat was not taken seriously, but subsequently did so after their website was affected by a DoS attack.

> *Comment: CCIRC encourages partners and operators of vital systems who find themselves coerced or blackmailed through cyberspace to contact CCIRC or law enforcement. They are also encouraged to consult CCIRC's Mitigation Guidelines for Denial-of-Service Attacks.*



Victim notifications – During the reporting period, CCIRC sent a total of 504 notifications to some of its partners in Canadian public and private sector organizations whose computers were found to be infected with Zeus peer-to-peer (P2P), TDSS, and/or Conficker malware. Notifications were also sent to organizations that were found to be operating with open Domain Name System (DNS) resolvers, and who had computer devices found to be infected with various ransomware and/or which were a part of a botnet. CCIRC's victim notifications also typically contain detection indicators and mitigation advice.

> *Comment: P2P is a newer delivery method for the existing Zeus banking Trojan which involves spreading the malware between unsuspecting victims. As a result, the malware's author always retains access to their botnet through the P2P network, and is thereby precluded from establishing a command and control server.*

Public Sector

Federal Government

vulnerability found on federal organization's website – CCIRC notified the organization and the federal computer security incident response team (CSIRT), the latter of which provided mitigation advice to the affected organization.

In all instances, CCIRC notified the federal CSIRT which provided mitigation advice to the affected organizations.

Provincial Government

Provincial government organization website hosted malvertising – A trusted partner informed CCIRC of an advertisement banner on a provincial organization's website which was redirecting users to a malicious Java Archive (JAR) file. CCIRC notified the organization that their advertisement banners were redirecting users to a malicious website. The incident was mitigated by the affected organization and contributed to CCIRC's recent cyber flash (*CF12-019: Java Exploits Leveraging Compromised OpenX Ad Servers*).

Phishing campaign targeted provincial government organization – A provincial Information Protection Centre (IPC) notified CCIRC that several employees at a department had been the victims of a phishing campaign. The IPC mitigated the issue by resetting these employees' credentials, blocking the IP address and URL of the phishing website, and blocking the source of the phishing emails. As CCIRC's analysis uncovered that the phishing emails originated from a foreign critical infrastructure organization, CCIRC notified that country's computer emergency readiness team (CERT).

NOTEWORTHY ITEMS IN THE NEWS

Cyber attack reporting could boost defence capability – The European Commission (EC) is considering making it mandatory for companies to report cyber attacks. Adoption of cloud infrastructure, an economic development goal of the EC, is dependent on the security of cloud infrastructure. The details of whom may have to report cyber attacks, and to which authority, are expected to be included in the EC's forthcoming inaugural cyber security strategy.

Data on International Atomic Energy Agency scientists grabbed in purported hack – Hackers leaked the contact information of 167 scientists, including several Canadians, belonging to the United Nations' International Atomic Energy Agency (IAEA).

Syrian Internet Outage – The outage occurred on November 29-30, 2012. During this event, all of Syria's international communications cables were disconnected, effectively removing the country of 22,530,000 (July 2012 population estimate) people from the Internet.

Best Practices
Blackhole Exploit Kit Mitigation

Exploit kits inspect a potential victim's system for vulnerabilities and then automatically exploit these by inserting malware. This malware then calls home to a command and control server before carrying out its malicious function.

Blackhole is currently one of the most prevalent exploit kits affecting Canada, and the following defence-in-depth security best practices should be considered:

- Patch operating systems and applications in a timely manner;
- Disable vulnerable systems (e.g. Java, Flash) whenever these are not needed;
- Block compromised legitimate websites through the use of reputation filtering;
- Maintain up-to-date spam filters; and
- Educate users about the threat.

For additional mitigation guidelines and detection indicators, please consult CCIRC's Cyber Flash *CF12-018 Blackhole Exploit Kit Version 2 Indicators*.

The best practices above are based on Sophos' Security Threat Report 2013.

DNS change puts 284 Pakistani websites at mercy of hackers – In one of the biggest cyber security events of the year in Pakistan, the websites of Google, eBay, and Microsoft were among those completely taken down and/or defaced.

PUBLISHED INTERNET THREAT REPORTS

Sophos Security Threat Report 2013 – Sophos reports that the growing demand to be able to access data from anywhere, and the subsequent diversification and growth of the technologies (e.g. cloud infrastructure) which meet this demand, has provided malicious actors with plenty of new targets to exploit. The report also highlighted the distributed denial-of-service (DDoS) attack campaign that targeted U.S. financial institutions (September – October 2012), and the prevalence of spear phishing attacks against critical infrastructure organizations.

While Sophos has observed a growth of advanced persistent threats campaigns, it lists Canada as the eighth least targeted country in this regard. In closing, Sophos called for "a renewed focus on layered security and detection across the entire threat lifecycle, not just the point of entry."

Study finds spear phishing at heart of most targeted attacks – Spear phishing refers to targeting key personnel within an organization because only one conduit into a network is required to conduct malicious activity, such as data theft. In this research paper, TrendMicro reports that advanced persistent threats (APT) constitute a growing part of the threat landscape and that meticulously engineered spear phishing is a prevalent infiltration technique for APT actors.

> *Comment: CCIRC has observed an increase in the number of advanced persistent threat attacks throughout 2012. CCIRC partners and operators of vital systems are encouraged to consult CCIRC's Mitigation Guidelines for Advanced Persistent Threats.*

FEEDBACK

Your feedback is appreciated and critical to making this product useful for you. Please email any feedback you have to Ken Bendelier, Manager, Operational Analysis and Support Section, at kenneth.bendelier@ps-sp.gc.ca.

From: Blackberry, GCCTEC1 <GCCTEC1@CSE-CST.GC.CA>
Sent: Thursday, December 06, 2012 7:16 PM
To: CYBERDO; CTEC
Subject: Fw: [redacted]
Attachments: [redacted]

Hello CyberDO,

FYI/FYA

[redacted]

Regards,

[redacted] s.16(2)
GC-CTEC

From: CTEC
Sent: Thursday, December 06, 2012 07:06 PM
To: Blackberry, GCCTEC1; Blackberry, GCCTEC2; Blackberry, GCCTEC3
Subject: FW: [redacted]

From: [redacted]
Sent: December 6, 2012 7:06:01 PM
To: CTEC
Subject: [redacted]
Auto forwarded by a Rule

Hello CTEC,

[redacted]

cheers
--
Rene Pariseau, GCIH, GCFA
twitter: http://twitter.com/renepariseau

From: CYBERDO
Sent: Thursday, December 06, 2012 8:28 PM
To: [redacted]
Cc: CYBERDO
Subject: CE12-004178 [Anynomous #OpPartyCrasher [redacted]
Attachments: [redacted]

Good day,
The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

[redacted]

You will find the following Mitigation Guidelines for Denial-of-Service Attacks at http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx.

In the immediate follow the step below;

- Establish contact with your technical team or host provider.
- Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.
- Establish 24/7 contact information for your ISP and alternate methods for communications.
- Finally CCIRC would like to have the server logs if possible for our future analysis.

Note: find attached analysis of the potential tools and the post referencing Irving oil.

Cyber Duty Officer | Officier de veille cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613[redacted]
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: Beaudoin, Luc
Sent: Thursday, December 06, 2012 8:58 PM
To: CYBERDO
Subject: Re: CE12-004178 [Anynomous #OpPartyCrasher -

Hmm. Pretty sure there is another template. I sent a number of them. Look at the email sent to

----- Original Message -----
From: CYBERDO
Sent: Thursday, December 06, 2012 08:44 PM
To: Beaudoin, Luc; CYBERDO
Subject: RE: CE12-004178 [Anynomous #OpPartyCrasher -

Got it....That's the template that was used in the last party crasher operation.

-----Original Message-----
From: Beaudoin, Luc
Sent: Thursday, December 06, 2012 8:41 PM
To: CYBERDO
Subject: RE: CE12-004178 [Anynomous #OpPartyCrasher - s.16(2)

Good. Tx.

Consider the following when providing advice:

``

In the immediate follow the step below;
``

Instead say:

``

In the immediate, please consider the following mitigation steps; ``

Remember that you are the government. If you give directives, you may be accountable. Also, in our field, some steps may cause more harm than good if they are not required. Have you considered they may not even be seeing any attack and we are asking for logs ?

-----Original Message-----
From: CYBERDO
Sent: December-06-12 8:35 PM
To: Beaudoin, Luc
Subject: FW: CE12-004178 [Anynomous #OpPartyCrasher -

FYI ,
In case you get a call, we got a heads up from CSE and ...see below.
Steve

s.16(2)(c)
s.19(1)

-----Original Message-----
From: CYBERDO
Sent: Thursday, December 06, 2012 8:28 PM
To:
Cc: CYBERDO
Subject: CE12-004178 [Anynomous #OpPartyCrasher -

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

You will find the following Mitigation Guidelines for Denial-of-Service Attacks at http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx.

In the immediate follow the step below;

- Establish contact with your technical team or host provider.
- Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.
- Establish 24/7 contact information for your ISP and alternate methods for communications.
- Finally CCIRC would like to have the server logs if possible for our future analysis.

Note: find attached analysis of the potential tools and the post referencing

Cyber Duty Officer | Officier de veille cybernétique

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-

Facsimile | Télécopieur +1 613-991-3574

PublicSafety.gc.ca | securitepublique.gc.ca

Government of Canada | Gouvernement du Canada

From: Breault, Stephen
Sent: Friday, December 07, 2012 7:31 AM
To: CYBERDO
Subject: #OpPartyCrasher

http://www.pastebay.net/[redacted]

1.
A Very Merry Canadian Christmas for the 99%
2.
3.
Greetings World,
4.
5.
We are Anonymous, This is a message to the Capitalist 1 % of Canada and to the People of Canada. We have been watching you, and it has come to our attention that YOUR

Greed is responsible for the downfall of this great country we call home.
6.
7.
Your greed and selfishness have bred a brainwashed consumeristic society in Canada. Now we have come to Crash teh Capitalist Party. We Won't Be the Consumer You want Us

to be. Your tactics against education and truth in our country are dumbing down the generations, WE won't be the complacent workers, or the sheep you want us to be.
8.
9.
No more, will you be able to lobby for bills and policies that protect and insure your Financial gain, or infringe on the Freedom and Privacy of the People. No more,

will you buy OUR politicians. No More, will your companies receive Bailouts and Tax Subsidies made up of OUR hard earned Money. No More Breaks, No More Capitalism, No More

Consumerism.
10.
We warned you before, and you should have #ExpectedUs.
11.
12.
To The People of Canada.
13.
THIS is OUR Home, and it's time we take it seriously. for far too long we have sat and watched in complacency as the Global Banking Cartel rapes our Country of its

resource and our people of their Rights and Freedoms. Its time we stop being complacent in their demands. it's time we stand up and take our country back. Stephen Harper is

denouncing the Arab Spring as a ballot grab, and says "it doesn't matter". What he doesn't see, is Canada has watched and learned from our brothers and sisters of the middle

east, and WE, Canadians are just as angry. We want this change, this revolution just as bad. It's time Canada becomes the change we want to see, it's time Canada for

Revolution. This is OUR Canada, These are OUR Streets, and This is OUR Internet.

14.

15.

#OpPartyCrasher ReEngaged

16.

17.

18.

Continue to write #OpPartyCrasher and #ExpectUs on either side of Canadian Currency

19.

20.

Let's Give the 99% the Justice Deserved, to the 1% of CANADA!

21.

#ExpectUs

22.

23.

CanAnons it's time to unite all Canadians against Corruption and Tyranny.

24.

Canadians it`s time to unite all CanAnons against Corruption and Tyranny.

25.

26.

This time Targets will not Focus on the Government in Power but the 1% who influence the powers at hand. The 1% of Canada believe they are safe, they think we haven't

been watching. These are the five richest corporations in Canada.

27.

These are the lobbyists, these are the people pushing for things like Bill c30, for FIPA and CETA. These are the people, that we as Canadians must let know this, is OUR

Canada. We have returned to crash your Capitalist Party yet again. Your ignorance and inhumanitarian ways of life, the hoarding of money, and your blatant disregard for Canada

as a whole, ends now! Canada is awakening to your injustice and Canada is angry. Canada it's time we

28.

take Canada back. #OpPartyCrasher ReEngaged

29.

30.

31.

#Op will begin on December 5 2012 and Commence on December 10 2012

32.

as 12/12/12 is the Launch of #TYLER #PM2012

33.

On December 20 2012 we will rerun the op,this will then commence on December 25 2012

34.

Merry Christmas to the 99% of Canada

35.

36.

#OpPartyCrasher Message to teh Capitalists
http://www.youtube.com/watch?v=sy00W1qQAWo&feature=youtu.be
37.
38.
also check out #OpFuckHarper http://pastebin.com/BfrN6jws
39.
40.
41.
Richest Canadians:
42.
THIS IS NOT ORDER OF ATTACK.
43.
Booster Scripts will be Released Midnight the Day of Attack.
44.
No. 1: Thomson family
45.
NET WORTH: $23.36B, ?6.2%
46.
HOME: Toronto COMPANIES: Thomson Reuters, Woodbridge Co.
47.
48.
Claim to fame: David Thomson (pictured), chairman of Thomson Reuters, is known for giving his billionaire U.S. rival, Michael Bloomberg,
49.
a real run for his money in the battle to dominate the electronic information-services market. As head of the nation's most enduring media dynasty,
50.
which owns a controlling stake in The Globe and Mail, the third Baron Thomson of Fleet also plays a major role in the ongoing evolution of printed news.
51.
http://thomsonreuters.com/
52.
http://www.woodbridgegroup.com
53.
54.
55.
56.
No. 2: Galen Weston
57.
Age: 70
58.
NET WORTH: $8.5B, ?31.3%
59.
HOME: Toronto COMPANIES: George Weston Ltd., Loblaws Cos. Ltd., Holt Renfrew
60.
61.
Brush with royalty: The grocery and retail magnate has been known to play polo with Prince Charles, which helps explain
62.
why many consider him the head of Canada's royal family. Weston's high-profile philanthropic wife, Hilary, is a former lieutenant-governor of Ontario,
63.

and son Galen G. is executive chair and public pitchman for the Loblaws supermarket chain.

64.

http://www.weston.ca/en/Home.aspx

65.

http://www.loblaw.ca/

66.

http://www.holtrenfrew.com/

67.

68.

69.

No. 3: Arthur, James and estate of John Irving

70.

Ages: 79 and 82

71.

NET WORTH: $7.46B,

72.

HOME: Saint John, N.B. COMPANIES: Irving Oil Ltd., J.D. Irving Ltd.

73.

74.

Family in flux: Under the direction of Kenneth Colin Irving, one of the leading industrialists of the 20th century, the Irving family expanded its initial

75.

sawmill business into a diversified empire before passing the torch to his three sons, James, Arthur (pictured) and Jack. But future succession plans are in question.

76.

Jack passed away in July, and his nephew, Kenneth, the rising star of the next generation, recently retired after an unnamed health setback.

77.

http://www.irvingoil.com/

78.

http://www.jdirving.com/

79.

80.

81.

No. 4: Rogers family

82.

NET WORTH: $6.02B, ?28%

83.

HOME: Toronto COMPANIES: Rogers Communications Inc.

84.

85.

Passing the torch: Ted Rogers died peacefully at home in 2008, but his entrepreneurial spirit lives on in family members who still serve shareholders. Edward Rogers,

86.

who cut his corporate teeth working in the U.S. cable and wireless sector, is the Toronto-based firm's deputy chairman and executive vice-president of emerging

87.

business and corporate development. Melinda Rogers (pictured), a Rotman MBA grad, is a director and senior vice-president of strategy and development.

88.

http://www.rogers.ca

89.

90.
91.

No. 5: Jimmy Pattison

92.

Age: 82

93.
94.

NET WORTH: $5.53B, ?9.1%

95.

HOME: Vancouver COMPANIES: Jim Pattison Group

96.
97.

Big secret: Having long disavowed leaving the Jim Pattison Group to his children, the octogenarian has many wondering what happens when he can no longer run his

98.

$7 billion private conglomerate like a tight ship.

99.

http://www.jimpattison.com/

Submit a correction or amendment below (click here to make a fresh posting <http://www.pastebay.net/pastebay.php>) After submitting an amendment, you'll be able to view the

differences between the old and new posts easily .

Cyber Duty Officer | Officier de veille cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-[redacted] s.16(2)(c)
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC
Sent: Friday, December 07, 2012 10:41 AM
Subject: CE12-004178 [Anonymous #OpPartyCrasher]
Attachments:

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

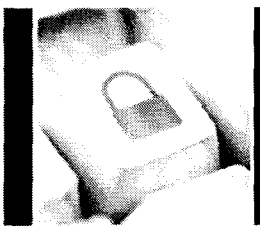
Mitigation information can be found attached and on the following Public Safety Canada web site:

http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Regards,

Cyber Duty Officer | Officier de veille cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613- s.16(2)(c)
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

Public Safety Canada | Sécurité publique Canada



CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 7 December 2012
CYBERDO: Patrick
****

[FOUO] NEW EVENTS:

1. Title: CE12-004174 [Notifications - TDSS]
   - Summary: Hosts within these organizations were infected with TDSS related malware.
     Total IP count: 124
     Number of affected organisations receiving a notification: 8
     Provincial: (1)
     Telecom: (5)
     Academia:(2)
   - Action/Decision: : Notifications sent to IT security or technical contacts.
     - Owner: Ian
     - Status: Active

2. Title: CE12-004175 [RBC Phishing Website]
   - Summary: CCIRC received a report of a live phishing website.
     [redacted]
   - Action/Decision: CCIRC submitted sample to RBC and to the phishing intake portal.
     - Owner: Allen
     - Status: Active

3. Title: CE12-004176 [RBC Phishing Website]
   - Summary: CCIRC received a report of a live phishing website.
     [redacted]
   - Action/Decision: CCIRC submitted sample to RBC and to the phishing intake portal.
     - Owner: Allen
     - Status: Active

4. Title: CE12-004170 [Financial sector data]
   - Summary: CCIRC received Zeus/Citadel data from a research and trusted security partner concerning foreign financial information. The data contained the following information ;

Username:
Password:
Name:
Primary E-mail:
Address:
Phone Numbers:
Paypal Balance:
Credit card: Number: | Exp date: | CVV:
Account type:
Status:
Last log in:
Country:
Check date:
IP address:
User-agent:

- Action/Decision: Called the foreign national CSIRT and forwarded the data.
  - Owner: Steve
  - Status: Active

5. Title: CE12-004178 [Anonymous #OpPartyCrasher – Energy Sector]
- Summary: CCIRC received a report indicating that #OpPartyCrasher has expressed intentions to target an energy sector company on the 6th Dec 2012.
- Action/Decision: CCIRC forwarded notification to IT security technical contact
  - Owner: Steve
  - Status: Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE: NIL

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1) **IWWN ICSA-12-341-01P** - GE Proficy HMI/SCADA Cimplicity Integer Overflow
2) [redacted]

PUBLICATIONS: NIL

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. **Patch Tuesday: Five critical bulletins, Exchange Server fix expected**
   "Microsoft will address 11 vulnerabilities this month, fixing flaws in Internet Explorer, Microsoft Office and Microsoft Exchange Server."
   Reference: http://searchsecurity.techtarget.com/news/2240174035/Patch-Tuesday-Five-critical-bulletins-Exchange-Server-fix-expected

2. **Air Canada Scam Alert: Your Order Processed**
   "Spam campaigns that leverage the name of some popular airline have been around for quite some time now. In order to bring something new to these operations, cybercriminals don't only change the pieces of malware they attach to the fake notifications, but also the name of the company."
   Reference: http://news.softpedia.com/news/Air-Canada-Scam-Alert-Your-Order-Processed-312534.shtml

3. **ZeuS Hackers Spoof Top US Banks to Infect New Victims**
   "Dell SecureWorks' Counter Threat Unit (CTU) has discovered that the hackers behind the Gameover ZeuS banking Trojan (the largest botnet targeting financial institutions) is in the midst of launching several malicious spam campaigns using the Cutwail botnet. When the attachment is clicked on, the user is executing the Pony downloader, which in turn installs the infamous Gameover ZeuS banking Trojan."
   Reference: http://www.secureworks.com/cyber-threat-intelligence/blog/trojans/zeus-hackers-spoof-top-us-banks-infect-victims/

4. **Finnish Website Attack via Rogue Ad**
   "An advertising network used by one of Finland's most popular websites, suomi24.fi, was compromised during the December time period. And according to Suomi24, all of that malware traffic was pushed by a single ad from a third-party advertiser's network."
   Reference: http://www.f-secure.com/weblog/archives/00002468.html

****

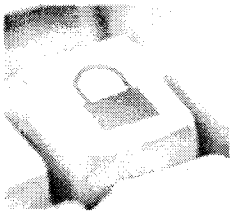
CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒

Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION:

OPERATIONAL SUMMARY
CCIRC Cyber Awareness Product



Weekly Technical Report

Issued: 12 December 2012

Volume 2012 - 49

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flash marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information, or Technical
- **Operational Summary:** Daily, Weekly, Monthly

NOTE TO READERS

CCAPs are available at the following website: http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx. If you have any questions, please contact the Public Safety Cyber Duty Officer @ [redacted] s.16(2)(c)

Traffic Light Protocol: RED: Designated for a specific audience/Non-sharable
AMBER: Sharable within organization on a need-to-know basis/Non-publishable
GREEN: Sharable within organization or community/Non-publishable
WHITE: Free to distribute

Table of Contents

Executive Summary

During the reporting period, the Canadian Cyber Incident Response Centre (CCIRC) handled 26 incidents, which affected partners in the finance, and energy and utilities sectors, and in federal, provincial, and foreign governments.

A noteworthy incident during this reporting period consisted of CCIRC being notified by an international partner of open domain name system resolvers which were amplifying distributed denial-of-service (DDoS) attacks targeting a wide range of Canadian sites. CCIRC is still investigating. Another noteworthy incident involved CCIRC notifying affected Canadian organizations of their corporate information being posted online by hacktivist group TeamGhostShell.

During the reporting period, CCIRC sent victim notifications to its partners in public and private organizations who were found to have hosts infected with Zeus, TDSS, and/or Gamaruel malware; and to organizations which were found to be operating with open domain name system (DNS) resolvers.

CCIRC regularly issues information products to inform its partners of potential, imminent or actual cyber threats. CCIRC did not release any such products during the reporting period.

ICS-CERT released two advisories related to Rockwell programmable logic controllers and Tropos wireless mesh routers.

This week's noteworthy news included the publication of the Sophos *Security Threat Report 2013*, TrendMicro's 'Deep Discovery' technology, and an increase in attacks involving malware on Apple OS X.

CCIRC'S INDUSTRIAL CONTROL SYSTEMS CYBER SECURITY BEST PRACTICES

In recognition of the risks facing industrial control systems, CCIRC recently published Technical Report (TR12-002) *Industrial Control System (ICS) Cyber Security: Recommended Best Practices* to its website. This Technical Report is a summary of CCIRC's *Industrial Control Systems Security Best Practice Guide*, which was published to CCIRC's secure Community Portal in October 2012 and is also available upon request.

The purpose of TR12-002 is to provide SCADA and ICS IT professionals and managers with a list of technical and administrative industry best practices to help address cyber security challenges faced by owners and operators of industrial facilities using networked control system technologies.

Incident Reporting

This section contains information related to incidents affecting Critical Infrastructure in Canada.

1. CE12-004145 [Notifications - Open Resolvers]

Hosts within these organizations had open DNS resolvers.
Notifications sent to IT security or technical contacts in the following CI sector organizations:
Total IP Count: 32
Affected organisations receiving a notification: 10
Trusted Security Partners: 1
Telecom: 4
Academia: 5

2. CE12-004146 [Notifications - Zeus Botnets]

Hosts within these organizations were infected with Zeus.
Notifications sent to IT security or technical contacts in the following CI sector organizations:
Total IP count: 138
Affected organisations receiving a notification: 15
Federal: 1
Provincial: 1
Telecom: 3
Academia: 10

3. CE12-004174 [Notifications - TDSS]

Hosts within these organizations were infected with TDSS.
Notifications sent to IT security or technical contacts in the following CI sector organizations:
Total IP count: 124
Affected organisations receiving a notification: 8
Provincial: 1
Telecom: 5
Academia: 2

4. CE12-004189 [Notifications - Zeus p2p]

Hosts within these organizations were infected with Zeus p2p.
Notifications sent to IT security or technical contacts in the following CI sector organizations:
Total IP count: 1731
Affected organisations receiving a notification: 114
Provincial: 1
Telecom: 96
Finance: 1
Energy: 4
Academia:11
Food:1

5. CE12-004206 [Notifications - Open Proxy]

Hosts within these organizations were found to have open proxy.
Notifications sent to IT security or technical contacts in the following CI sector organizations:
Total IP count: 10
Affected organisations receiving a notification: 3
Telecom: 2
Information and Technology: 1

Federal Government

1. CE12-004149 [Domain Registration Scam]

CCIRC received a report of a likely domain registration scam.
Email content:

"Dear Sir or Madam, We are a senior domain registrar in Hong Kong. 1.On Dec. 03, 2012, a company named Sliveruey Co. applied for registering the following Top-Level-Domains with us. [dept code].asia ps-sp.cn [dept code].com.cn ps-sp.com.hk [dept code].com.tw [dept code].hk [dept code].tw 2. Whether did you consign Sliveruey to register these Domains? Or are they your subbranch? Should you have any questions, pls do not hesitate to contact me. Tks & br, Candy Zhang Tel: +852_3050 _6765 Fax: +852_3069 _7409 czh@hkbweb[.]hk hxxp:// www[.]hkcreating[.]hk/"

This is a known practice that in most cases is attempting to receive payment from the target organization.

2. CE12-004155 [Phishing]

CCIRC received a CRA phishing email sample.
Embedded URL:

Federal CSIRT has been notified.

3. CE12-004165 [Unsecure Proxy Notification]

CCIRC received indication that a federal host is identified as potentially having an unsecured internet proxy.

Federal CSIRT has been notified.

4. CE12-004203 [Gamaruel Infection]

CCIRC was notified that hosts within a Federal Department may be infected with Win32/Gamaruel*.

Microsoft: Win32/Gamarue is a family of malware that may be distributed by exploit kits, spammed emails or other malware, and has been observed stealing information from an affected user.

Federal CSIRT has been notified.

Provincial and Territorial Government

1. CE12-004148 [Malware Samples]

CCIRC received different samples from our partner, ranging from Cycbot/Kazy to Jar file that exploit CVE-2012-0507 (AtomicReferenceArray). Details of indicators are provided below on the Malware indicators section.

Municipal Government

NIL

Information and Communication Technology

NIL

Finance

1. CE12-004175, CE12-004176 [RBC Phishing Website]

CCIRC received a report of a live phishing website.
Embedded URL link:

Embedded URL link:

CCIRC sent notification to IT security or technical contacts and trusted partner for URL blocking

Energy and Utilities

1. CE12-004173 [Anonymous #OpPartyCrasher]

CCIRC received a report indicating that #OpPartyCrasher has expressed intentions to target an energy sector company on the 6th Dec 2012.

CCIRC notified the IT security technical contacts.

2. CE12-004190 [Phishing Email]

CCIRC was informed by an Energy sector CI that executive level management had received phishing mail, it was determined that the same message was received twice within 10 minutes, targeting some twice, while others only once.
Email from
Subject :
Body:

"Hi,

May I have the direct number to reach you?

Regards,
Arthur Ganson"

No malicious code was discovered, this could possibly be an attempt at social engineering.

3. CE12-004191 [Possible Malware Compromise]

CCIRC obtained information from a trusted security partner indicating that an Energy sector company was likely compromised with a malware as a result of a targeted attack. CCIRC has reached out to the organization to notify and provide assistance as required.

More detail related to the indicators provided in the Malware Indicators section below.

4. CE12-004212 [Possible C2 IP Address]

CCIRC obtained information that three separate malware types were attempting to contact an IP address that is owned by a CI organization.

CCIRC notified the IT security technical contact.

Transportation

NIL

Manufacturing

NIL

Health

NIL

Food

NIL

Water

NIL

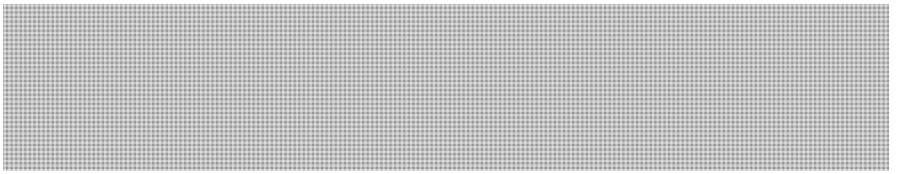
Other (Academia)

NIL

Other Organizations

1. CE12-004152 [Phishing site hosted in Canada]

CCIRC was notified of a phishing website, targeting an international organization which was hosted in Canada.



Code Removal Request was sent to the abuse contact.

2. CE12-004161 [Serbia TLD - Corruption]

CCIRC was notified by a trusted source of a corrupted TLD for Serbia.

3. CE12-004163 [Compromised Local Community Group Website]

CCIRC was notified that a Canadian website hosted malicious php code that redirected users to a phishing site located

CCIRC sent notification to IT security or technical contacts.

4. CE12-004167 [Accounts Compromised by Citadel Malware]

CCIRC was notified by a trusted partner that 39 E-mail accounts were compromised by the Citadel Malware.

CCIRC sent notification to IT security or technical contacts.

5. CE12-004170 [Foreign Financial sector data]

CCIRC received Zeus/Citadel data from a research and trusted security partner concerning foreign financial information. The data contained the following information;
Username, Password, Name, Primary E-mail, Address
Phone Numbers, Paypal Balance
Credit card Number, Exp date, CVV
Account type, Status, Last log in, Country, Check date
IP address, User-agent

CCIRC notified the foreign CSIRT.

6. CE12-004179 [DDOS – DNS Amplifications]

CCIRC was notified by International partner of open resolvers used to DDOS a wide range of Canadian sites.

CCIRC is still investigating the matter.

7. CE12-004194 [Zeuz p2p/Zbot– Victim Mentioned in Blog]

CCIRC were aware through open source of a Canadian host that appeared to be infected with Zeus P2P related malware mentioned in a blog.

CCIRC sent notification to IT security or technical contacts.

8. CE12-004198 [Canadian Hosts- Default credentials]

CCIRC obtained data containing publically accessible routers still configured with default credentials. This list contained Canadian hosts.

CCIRC sent notification to IT security or technical contacts.

9. CE12-004208 [Phishing]

CCIRC was notified by a trusted partner of phishing hosted on:
IP:
URL:
URL2:

URL:
IP:

Code Removal Request was sent to abuse contacts.

10. CE12-004209 [Zeus Notification - ISP]

CCIRC is aware of the following: Zeus config/command and control being hosted on
IP Address:
ZeuS Config URL:
ZeuS Drop URL:

CCIRC sent notification to IT security or technical contacts.

11. CE12-004210 [TeamGhostShell - ProjectWhitefox]

CCIRC was notified of a posting by TeamGhostShell that supposedly contains database information, from various organizations, containing user credentials.

CCIRC is analyzing the data for Canadian victims and notifying the affected organizations.

Partners

Watch List

NIL

Malware Indicators

*IMPORTANT: These indicators must be silently dropped if implemented in defensive technologies. Many security products perform dynamic pulling of malicious sites/IPs. The indicators below are sensitive and may be associated with on-going investigations. Active probing could disrupt such efforts.

Reference: Trusted Partner

Malware: Targeted Attack

Post-Infection

Domain Indicator(s)

File Indicator(s)

Filename:
MD5 Hash

IP Indicator(s)

[redacted]

Reference: CCIRC Analysis

Malware: Cycbot / Kazy

Post-Infection

File Indicator(s)

Filename: [redacted]
MD5 Hash: [redacted]
Filename: [redacted]
MD5 Hash: [redacted]
Filename: [redacted]
MD5 Hash: [redacted]

Malware: Java Exploit / CVE-2012-0507

Pre-Infection

Domain Indicator(s)

[redacted]

File Indicator(s)

Filename: [redacted]
MD5 Hash: [redacted]
Filename: [redacted]
MD5 Hash: [redacted]
Filename: [redacted]
MD5 Hash: [redacted]

HTTP URI Indicator(s)

[redacted]

IP Indicator(s)

[redacted]

Malware: Java Exploit / CVE-2012-1723

Pre-Infection

Domain Indicator(s)

[redacted]

File Indicator(s)

Filename: [redacted]
MD5 Hash [redacted]
Filename: [redacted]
MD5 Hash: [redacted]

HTTP URI Indicator(s)

[redacted]

IP Indicator(s)

[redacted]

Post-Infection

Domain Indicator(s)

[redacted]

HTTP URI Indicator(s)

[redacted]

Malware: Medfos Trojan

Pre-Infection

File Indicator(s)

Filename: [redacted]

MD5 Hash: [redacted]

Post-Infection

Domain Indicator(s)

[redacted]

File Indicator(s)

Filename [redacted]

MD5 Hash: [redacted]

IP Indicator(s)

[redacted]

Registry Indicator(s)

Key: [redacted]

Value: [redacted]

Reference: Trusted Partner

Malware: Multi-threaded RAT

Pre-Infection

File Indicator(s)

Filename: [redacted]

MD5 Hash: [redacted]

Post-Infection

File Indicator(s)

Filename: [redacted]

MD5 Hash [redacted]

IP Indicator(s)

[redacted]

Malware: Targeted Attack

Pre-Infection

Email Indicator(s)

From:
Subject:
Attachment:

From:
Subject:
Attachment:

From:
Subject:
Attachment:

Sender:
Subject

Post-Infection

Domain Indicator(s)

IP Indicator(s)

Infection

File Indicator(s)

File:
MD5:

Awareness Products

Alerts

NIL

Advisories

NIL

Information Notes

NIL

Technical Reports

1. TR12-002- Industrial Control System (ICS) Cyber Security: Recommended Best Practices

Link: http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-002-eng.aspx

Cyber Flashes

NIL

Threat and Vulnerability Monitoring

This section contains threats and vulnerabilities that did not meet the publication criteria for CCIRC products other than operational summaries. It is not meant to be an exhaustive list but rather a heads-up on potentially significant threats and vulnerabilities affecting technologies available to CCIRC communities of interest.

Vulnerabilities

1. Symantec Endpoint Protection Management Console Code Execution Vulnerabilities

The vulnerabilities are caused due to unspecified errors within the management console and should not be exposed to the network. Could lead to remote code execution. CVE-2012-4348 and CVE-2012-4349. A vendor patch is available.
Reference:http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20121210_00

Threat Watch

NIL

SCADA/ICS

1. ICSA-12-342-01 – Rockwell Allen-Bradley MicroLogix

Reference: http://www.us-cert.gov/control_systems/pdf/ICSA-12-342-01.pdf

2. ICSA-12-297-01 – TROPOS WIRELESS MESH ROUTERS INSUFFICIENT ENTROPY VULNERABILITY

Reference: http://www.us-cert.gov/control_systems/pdf/ICSA-12-297-01.pdf

Noteworthy News

1. Security Threat Report 2013

"IT security is evolving from a device-centric to a user-centric view, and the security requirements are many. A modern security strategy must focus on all the key components—enforcement of use policies, data encryption, secure access to corporate networks, productivity and content filtering, vulnerability and patch management, and of course threat and malware protection."
Reference: http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx

2. Trend Micro's Ottawa team readies 'Deep Discovery' offensive to root out authors of security threats

"A crack team of Ottawa programmers is quietly toiling away on revolutionary security technology that could change the way governments around the globe combat computer hackers."
Reference: http://www.vancouversun.com/technology/tech-biz/Trend+Micro+Ottawa+team+readies+Deep+Discovery/7649720/story.html

3. Android devices in U.S. face more malware attacks than PCs

"Android devices are now attacked more often by malware than PCs, according to a report released today by Sophos, a cyber security software maker. It said that almost 10 percent of Android devices in the U.S. have experienced a malware attack over a three-month period in 2012, compared to about 6 percent of PCs."
Reference: http://www.infoworld.com/d/security/android-devices-in-us-face-more-malware-attacks-pcs-208462

4. Beware 'Irreversible Malware, Increased Attacks On Apple OS X

"Cybercriminals using ransomware to extort money from computer users have raised their game by adding highly complex encryption to their methods used to lock down their victims' data."
Reference: http://www.crn.com/news/security/240143096/beware-irreversible-malware-increased-attacks-on-apple-os-x.htm

5. Why Anti-Virus is not a waste of money

"It has happened before, it just happened again and it will happen in the future. It is inevitable! Some company that needs to get some press coverage or public visibility will release yet another statement on how worthless Anti-Virus is, based on its own dysfunctional test."
Reference: http://blog.eset.com/2012/12/04/why-anti-virus-is-not-a-waste-of-money

6. Twitter and Facebook get called out for SMS exploit

"A security researcher has called out Twitter and Facebook for a SMS vulnerability capable of sending out unauthorized messages through the social networks."
Reference: http://www.v3.co.uk/v3-uk/news/2230029/twitter-and-facebook-get-called-out-for-sms-exploit

7. Rogue Yahoo! Messenger Cashes In on Latest YM Update

"On the heels of Yahoo!'s recent announcement of upcoming updates for the Messenger platform, certain bad guys are already taking this chance to release their own, malicious versions of Yahoo! Messenger."
Reference: http://blog.trendmicro.com/trendlabs-security-intelligence/rogue-yahoo-messenger-cashes-in-on-latest-ym-update/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trendlabs+Security+Intelligence+Blog%29

8. Nationwide Security Breach Raises Priority of IT Security

"Nearly a million Nationwide customers' personal information was compromised, but the fact that businesses report that cyber risk is their biggest concern shows that hackers present both threat and opportunity to the industry."
Reference: http://www.insurancetech.com/security/nationwide-security-breach-raises-priori/240143850

9. ZeuS Hackers Spoof Top US Banks to Infect New Victims

"Dell SecureWorks' Counter Threat Unit (CTU) has discovered that the hackers behind the Gameover ZeuS banking Trojan (the largest botnet targeting financial institutions) is in the midst of launching several malicious spam campaigns using the Cutwail botnet. When the attachment is clicked on, the user is executing the Pony downloader, which in turn installs the infamous Gameover ZeuS banking Trojan."
Reference: http://www.secureworks.com/cyber-threat-intelligence/blog/trojans/zeus-hackers-spoof-top-us-banks-infect-victims/

10. Finnish Website Attack via Rogue Ad

"An advertising network used by one of Finland's most popular websites, suomi24.fi, was compromised during the December time period. And according to Suomi24, all of that malware traffic was pushed by a single ad from a third-party advertiser's network."
Reference: http://www.f-secure.com/weblog/archives/00002468.html

11. 80% of malware attacks in 2012 were redirects from legitimate sites

"A new Sophos threat report signals that modern malware is taking advantage of new platforms. A recent Sophos threat report, Security Threat Report 2013, has found that 80% of malware attacks in 2012 were redirects from legitimate sites."
Reference: http://www.computerworlduk.com/news/security/3415472/80-of-malware-attacks-in-2012-were-redirects-from-legitimate-sites/?olo=rss

12. Necurs Rootkit Infections Way Up

"Infections from a nasty bit of malware, generally delivered by the Black Hole Exploit Kit, surged in November, hitting more than 83,000 machines.Microsoft's Malware Protection Center rates the Necurs rootkit threat as severe. Dubbed a rootkit by Kaspersky Lab, Necurs has many dimensions to it. Like most rootkits, it can hide its components from detection while also being capable of downloading additional malware, disabling a long list of security software and installing a backdoor. Attackers can maintain remote access to a machine this way in order to monitor activity, send spam or install scareware."
Reference: http://threatpost.com/en_us/blogs/necurs-rootkit-infections-way-120712

13. New Accounting System Hack Could Cause 'Mayhem'

"Dell SecureWorks' Counter Attacks against massive and proprietary enterprise accounting systems, in particular financial software such as SAP and Oracle, have been few and far between. That changed at this week's Black Hat Abu Dhabi conference where a pair of researchers presented proof-of-concept code that could change the dynamic of the financially motivated attack landscape."
Reference: http://threatpost.com/en_us/blogs/new-accounting-system-hack-could-cause-mayhem-120712

14. Metasploit Pro 4.5 Released

"Rapid7 released a new version of Metasploit Pro, which introduces advanced capabilities to simulate social engineering attacks. With Metasploit 4.5, security professionals can now gain visibility into their organization's exposure to phishing attacks through user-based and technical threat vectors, and introduce the necessary controls to manage the risk."
Reference: http://www.net-security.org/secworld.php?id=14083

15. Government Security News Names Entrust as a Winner in the Best Certificate Management Solution

"At a gala dinner that drew hundreds of government officials and industry executives to the Washington Convention Center on Nov. 29, Government Security News (GSN)(http://www.gsnmagazine.com/) magazine announced the winners — including Entrust— in 42 different categories in its fourthannual Homeland Security Awards competition.
GSN recognized Entrust as a winner in the"Best Certificate Management Solution" category. All winners were honored at a festive banquet hosted by GSN in a ballroom at the Washington, D.C. Convention Center."
Reference: http://www.i-newswire.com/government-security-news-names/205856

16. Tor network used to command Skynet botnet

"Security researchers have identified a botnet controlled by its creators over the Tor anonymity network. It's likely that other botnet operators will adopt this approach, according to the team from vulnerability assessment and penetration testing firm Rapid7."
Reference: http://news.techworld.com/security/3415592/tor-network-used-command-skynet-botnet/

17. Aramco Hack Aimed at Curbing Oil Production

"An August attack on the Saudi Arabian national oil company, Aramco, was reportedly launched in order to hinder oil production at the world's most valuable company, according to a report published in the New York Times yesterday.
The attack damaged some 30,000 company workstations but failed to achieve it primary goal, which, according to Abdullah al-Saadan, the company's vice president of corporate planning, was to stop the flow of oil and gas from Aramco to local and international markets."
Reference: http://threatpost.com/en_us/blogs/aramco-hack-aimed-curbing-oil-production-121012

18. Latest on Police Ransomware – It Speaks!

"These days, this new breed of ransomware notifies users of the fee (or ransom) under the guise of the victim's local law enforcement agencies. Thus, a user with a ransomware-

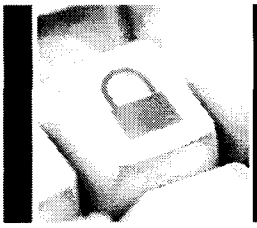
infected system from France will get a notification from the Gendarmerie Nationale, while a US-based one will likely receive a message from the FBI.
To level up the ante, we received a report that a new police Trojan variant even has a "voice". Detected as TROJ_REVETON.HM, it locks the infected system but instead of just showing a message, it now urges users to pay verbally. The user won't need a translator to understand what the malware is saying – it speaks the language of the country where the victim is located."
Reference: http://blog.trendmicro.com/trendlabs-security-intelligence/latest-on-police-ransomware-it-speaks/

19. No password is safe from this new 25-GPU computer cluster

"Your really, really strong password just became a little bit easier to break.
Jeremi Gosney, founder and CEO of Stricture Consulting Group, a company that handles password-cracking, has unveiled a computer cluster boasting 25 AMD Radeon graphics cards. The cluster's horsepower allows it to make 350 billion password guesses per second against the NT Lan Manager (NTLM) security protocol Microsoft has used in Windows Server since 2003."
Reference: http://news.cnet.com/8301-1009_3-57558223-83/no-password-is-safe-from-this-new-25-gpu-computer-cluster/?part=rss&subj=news&tag=title

20. Anonymous to Leak "Unprecedented Amounts of Data" Starting with December 10 – Video

"Starting with December 10 and until December 21, Anonymous hacktivists plan on leaking "an unprecedented amount" of corporate, financial, military and state data as part of the campaign called Project Mayhem 2012."
Reference: http://news.softpedia.com/news/Anonymous-to-Leak-Unprecedented-Amounts-of-Data-Starting-with-December-10-Video-313551.shtml



CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 14 December 2012
CYBERDO: Vireak
****

[FOUO] NEW EVENTS:

1. Title: CE12-004248 [New Ransomware Information]
- Summary: CCIRC received an analysis of a purportedly new Trojan from a private sector partner. The partner indicates that Canada and US are specifically targeted by this new Trojan. Partner is sharing with us for our review and situational awareness. Appears that the Trojan will encrypt the hard drive contents and prompt victim to send money via a money transfer service to have the files decrypted.
- Action/Decision: Analysis is ongoing.
  - Owner: Gregg
  - Status: Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. Title: CE12-004178 [Anonymous #OpPartyCrasher – Energy Sector]
- Summary: CCIRC received a report indicating that #OpPartyCrasher has expressed intentions to target an energy sector company on the 6th Dec 2012.
- Update: One of the targeted companies has requested assistance from CCIRC.
- Action/Decision: CCIRC provided analysis documents on [redacted] to assist with mitigation.
  - Owner: Vireak
  - Status: Active

2. Title: CE12-004191 [Compromised in Oil and Gaz Sector]
- Update: Organization has so far confirms 5 infections and those workstations were isolated from the network. The organization asked for more Indicators.
- Action/Decision: CCIRC provided 3 cyberflash, cf11-205, cf12-03 update 4 and the last cf12-020[the drafted version]. CCIRC also requested for the sample of the malware [if possible]).
  - Owner: Vireak
  - Status: Active

[FOUO] ACTIVITIES:

1. Title: CE12-004246 [Financial Partner Information Request]
- Summary: CCIRC received an information request from a financial partner. Would like to know if CCIRC has any information regarding cyber threat levels or recent attacks on Canadian financial partners.
- Action/Decision: CCIRC is reviewing request.
  - Owner: Sharique
  - Status: Active

[FOUO] INTERNATIONAL PARTNERS:

1. **ICSA-12-348-01** - Siemens ProcessSuite_Invensys InTouch Poorly Encrypted Passwords.
http://www.us-cert.gov/control_systems/pdf/ICSA-12-348-01.pdf

PUBLICATIONS:

1. **CF12-020: Indicators for Recent Targeted Attacks**

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. **Project Blitzkrieg e-banking heist is a credible threat, McAfee says**
"Project Blitzkrieg, a coordinated attack against U.S. banking customers allegedly planned for the spring of 2013, is a real and credible threat, security researchers at McAfee have said."
Reference:
http://www.computerworld.com/s/article/9234694/Project_Blitzkrieg_e_banking_heist_is_a_credible_threat_McAfee_says?taxonomyId=85

2. **UK cops: How we sniffed out convicted AnonOps admin 'Nerdo'**
"Analysis of IRC logs and open source intelligence played a key role in the successful police prosecution that led up the conviction of a member of Anonymous for conspiracy to launch denial of service attacks against PayPal and other firms.
Weatherhead, 22, was studying at Northampton University when he allegedly took part in "Operation Payback", the DDoS campaign launched by the hacktivists in defence of whistle-blowing site WikiLeaks. Targets included the entertainment industry and later financial services firms that had suspended

payment processing of donations to WikiLeaks after it controversially published leaked US diplomatic cables in late 2010."
Reference: http://www.theregister.co.uk/2012/12/14/uk_anon_investigation/

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒
SecuriTeam (http://www.securiteam.com/)	☒
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION: NIL

From: Phlek, Vireak
Sent: Friday, December 14, 2012 1:24 PM
To: CYBERDO
Subject: CE12-004178 [Anonymous #OpPartyCrasher]
Attachments:

If Wayne reply with the contact, please sent the above email with the attachment.

Vireak

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

Were impacted by that event?

Mitigation information can be found attached and on the following Public Safety Canada web site:

http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Regards,

Cyber Duty Officer | Officier de veille cybernétique

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613- s.16(2)(c)

Facsimile | Télécopieur +1 613-991-3574

PublicSafety.gc.ca | securitepublique.gc.ca

Government of Canada | Gouvernement du Canada

From: CYBERDO
Sent: Friday, December 14, 2012 2:32 PM
To: [redacted]
Subject: FW: CE12-004178 [Anonymous #OpPartyCrasher]
Attachments: [redacted]

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

[redacted]

Were impacted by that event?

Mitigation information can be found attached and on the following Public Safety Canada web site:

http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

[redacted]

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-[redacted] Facsimile | Télécopieur +1 613-991-3574 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

Pages 1207 to / à 1219

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)

of the Access to Information

de la Loi sur l'accès à l'information

From: Robert Lafrance <robert.lafrance@rcmp-grc.gc.ca>
Sent: Thursday, December 20, 2012 11:24 AM
To: Lise Robichaud
Cc: [redacted] CCIRC-CCRIC; Timothy O'Neil
Subject: Re: CE12-004178 [Anynomous #OpPartyCrasher - [redacted]
Attachments: [redacted]

Can you follow up on this when you get a chance as I am otherwise engaged with the FN protests currently going on in the division.

Thanks,

Rob

>>> CCIRC-CCRIC <[redacted]> 2012-12-20 11:37 >>>
Good Morning [redacted]

[redacted]

[redacted]

Regards,

Cyber Duty Officer
Public Safety Canada
CCIRC
613-[redacted]
www.publicsafety.gc.ca

Subject: CE12-004178 [Anynomous #OpPartyCrasher

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

You will find the following Mitigation Guidelines for Denial-of-Service Attacks at http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx.

In the immediate follow the step below;

- Establish contact with your technical team or host provider.
- Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.
- Establish 24/7 contact information for your ISP and alternate methods for communications.
- Finally CCIRC would like to have the server logs if possible for our future analysis.

Cyber Duty Officer | Officier de veille cybernétique

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613- s.16(2)(c)

Facsimile | Télécopieur +1 613-991-3574

PublicSafety.gc.ca | securitepublique.gc.ca

Government of Canada | Gouvernement du Canada

From:
Sent: Thursday, December 20, 2012 11:27 AM
To: Robert Lafrance; Lise Robichaud
Cc: CCIRC-CCRIC; Timothy O'Neil
Subject: RE: CE12-004178 [Anynomous #OpPartyCrasher -
Attachments: Re: CE12-004178 [Anynomous #OpPartyCrasher -

Hi Robert, I've sent an email to regarding this and it appears that he is out of the office, I've not received any feedback from on this.

s.16(2) s.16(2)(c)
s.19(1)

From: Breault, Stephen
Sent: Monday, March 04, 2013 9:23 PM
To: Beaudoin, Luc; Clow, Patrick
Cc: CYBERDO
Subject: Re: CYBER NOTIFICATION-13-002-2 – LOW IMPACT SEVERITY – MEDIA INTEREST – Ongoing Distributed Denial-of-Service Attacks Target Financial Institutions (UPDATE 2)

Just got off the phone with the GOC and nothing is in the C5 mailbox or mandrake.. They will keep an eye out for any event coming in and will notify then. I have talked to Robert and have relayed the message.

From: Beaudoin, Luc
Sent: Monday, March 04, 2013 09:19 PM
To: Clow, Patrick
Cc: CYBERDO; Breault, Stephen
Subject: Re: CYBER NOTIFICATION-13-002-2 – LOW IMPACT SEVERITY – MEDIA INTEREST – Ongoing Distributed Denial-of-Service Attacks Target Financial Institutions (UPDATE 2)

Gardez moi dans la loop.

Cell: 613 [redacted] s.19(1)

From: Clow, Patrick
Sent: Monday, March 04, 2013 09:18 PM
To: Beaudoin, Luc
Cc: CYBERDO; Breault, Stephen
Subject: RE: CYBER NOTIFICATION-13-002-2 – LOW IMPACT SEVERITY – MEDIA INTEREST – Ongoing Distributed Denial-of-Service Attacks Target Financial Institutions (UPDATE 2)

Oui...Steve attends un appel du GOC.

From: Beaudoin, Luc
Sent: Monday, March 04, 2013 9:18 PM
To: Clow, Patrick
Cc: CYBERDO; Breault, Stephen
Subject: Re: CYBER NOTIFICATION-13-002-2 – LOW IMPACT SEVERITY – MEDIA INTEREST – Ongoing Distributed Denial-of-Service Attacks Target Financial Institutions (UPDATE 2)

As tu rejoins cyberdo ?

Si oui, il faudrait aussi qu il loggout les gens du systeme de telephone car on ne peut pas rejoindre la voicemail en ce moment...

From: Clow, Patrick
Sent: Monday, March 04, 2013 09:07 PM
To: Dick, Robert
Cc: Beaudoin, Luc
Subject: FW: CYBER NOTIFICATION-13-002-2 – LOW IMPACT SEVERITY – MEDIA INTEREST – Ongoing Distributed Denial-of-Service Attacks Target Financial Institutions (UPDATE 2)

Some background information. Working on C5 access.....

From: Beaudoin, Luc
Sent: Thursday, March 07, 2013 9:53 AM
To: CYBERDO
Subject: Fw: NEWS: US Financial Institutions Face Targeted Attacks as Backlash toward Anti-Islamic Film Spreads

From: Kyle Melnychyn [mailto:Kyle.Melnychyn@rcmp-grc.gc.ca]
Sent: Thursday, March 07, 2013 09:51 AM
To: Kyle Melnychyn <Kyle.Melnychyn@rcmp-grc.gc.ca>
Subject: NEWS: US Financial Institutions Face Targeted Attacks as Backlash toward Anti-Islamic Film Spreads

FYI
Regards,

s.16(2)

From: CCIRC-CCRIC
Sent: Wednesday, March 27, 2013 5:24 PM
To: Clairmont, Lynda; Dick, Robert; Gordon, Robert; Jarmyn, Tom; Johnson, Mark; Mueller, Mike; Tony.Pickett@rcmp-grc.gc.ca; [redacted]@CSE-CST.GC.CA; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'cnoir@pco-bcp.gc.ca'; 'bdiogo@pco-bcp.gc.ca'; 'Eric.Belzile@ssc-spc.gc.ca'; Durand, Stéphanie; MacDonald, Michael; Wong, Suki
Cc: Anderson, Windy; Hatfield, Adam; Matz, Mark; Campbell, Tom; Duschner, Gabrielle; Paquet, Alain; Swift, Andrew; Bendelier, Kenneth; Clow, Patrick; Beaudoin, Luc; Klassen, Nathan; Proulx, Véronique; Pacha, Tomasz; Fortunato, Stephanie; Champoux, Martin; DeJong, Michael; Hunt, Ryan; CYBERDO; GOC-COG
Subject: CYBER NOTIFICATION-13-002-3 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST – Distributed Denial-of-Service Attack Targets Financial Institution (UPDATE 3) – Corrected Copy

CYBER NOTIFICATION – INCIDENT

Updates / changes are in **BOLD** text. Correction underlined.

Incident Number: CNT-13-002-**3** – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST

Description of Incident: [redacted] Since September 2012, CCIRC has been aware of DDoS attacks against financial institutions in the U.S. and in Canada. These DDoS attacks, which aim to disrupt the availability of computing resources from legitimate users, have primarily targeted U.S. financial institutions.

Sources of reporting: Trusted partner.

Current actions:

- The source of these cyber attacks appear to be compromised servers scattered around the world, and controlled by the attacker(s).
- CCIRC continues to observe the situation and will keep its partners informed of any significant developments.
- CCIRC and the U.S. Department of Homeland Security's US-CERT developed a joint public awareness product which was issued to CCIRC's website (IN13-001 – *Content Management Systems Security and Associated Risks*) on January 24, 2013.

Initial analysis / assessment:

- **The Canadian impact is assessed by CCIRC as minimal. Today's DDoS attack has not been reported in the media, but can reasonably be expected to garner media attention.**
- Open sources have variously linked these cyber attacks to the one year anniversary of the Occupy Movement, to the "Innocence of Muslims" video on YouTube, as well as to Iranian hackers. Since then, the Iranian Izz ad-Din al-Qassam Cyber Fighters group has claimed responsibility for these attacks, with some reports suggesting that the hacktivist group Anonymous has provided support.
- Since September 2012, affected U.S. financial institutions have included J.P. Morgan Chase, Bank of America, U.S. Bank, Wells Fargo, PNC, Citigroup, and HSBC Bank who have all acknowledged having experienced intermittent service interruptions to their websites.

CCIRC References:

- **CE13-005186**
- CYBER NOTIFICATION-12-012-2: Ongoing Distributed Denial-of-Service Attacks Target Financial Institutions (UPDATE 2)
- CCIRC Information Note (IN13-001): Content Management Systems Security and Associated Risks - http://www.publicsafety.gc.ca/prg/em/ccirc/2013/in13-001-eng.aspx
- US-CERT Alert (TA13-024A): Content Management Systems Security and Associated Risks - http://www.us-cert.gov/cas/techalerts/TA13-024A.html
- CCIRC Technical Report (TR12-001): Mitigation Guidelines for Denial-of-Service Attacks - http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Disclaimer:

This notification is only for distribution within the Government of Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Tom Pacha (613-991-3415)
Approved by: Ken Bendelier (613-993-5042)

Page 1228

is a duplicate of

est un duplicata de la

page 1230

From: Beaudoin, Luc
Sent: Sunday, April 07, 2013 8:07 AM
To: CYBERDO
Subject: Re: CE13-005294 [Anonymous - OpIsrael] RE: OpIsrael

Send to Ken + Windy for review as well. This is obviously an overkill but a good practice of this new SOP.

Incident Number: CNT-13-007 – VERY LOW IMPACT SEVERITY – MEDIA INTEREST

Current actions: CCIRC has reached out to the Israeli CERT and shared its related mitigation product.

There is no reported Canadian impact.
(Instead of very low)

----- Original Message -----
From: CYBERDO
Sent: Sunday, April 07, 2013 07:57 AM
To: Beaudoin, Luc
Subject: CE13-005294 [Anonymous - OpIsrael] RE: OpIsrael

Luc,

Please proof read/correct etc and let me know.

CYBER NOTIFICATION – INCIDENT

Incident Number: CNT-13-007 – LOW IMPACT SEVERITY – MEDIA INTEREST

Description of Incident: CCIRC is aware of media coverage on cyber attacks by the group Anonymous on Israeli web sites. No significant impact is reported. CCIRC remains vigilant and has reached out to Israeli CERT to offer assistance if needed."

Sources of reporting: Open Media Sources

Current actions: CCIRC has notified the Israeli CERT

Initial analysis / assessment:

The Current Canadian impact is assessed as very low.

Disclaimer:

This notification is only for distribution within the Government of Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Chris Briffett
Approved by: {Manager's name}

-----Original Message-----
From: Beaudoin, Luc
Sent: Sunday, April 07, 2013 7:22 AM
To: CYBERDO
Subject: OpIsrael

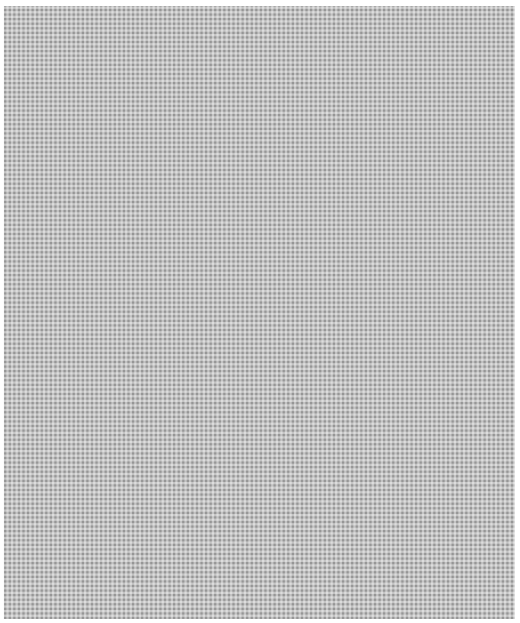
We should test the NT process this morning. Drafting a quick note on this and ensure we have an event associated with it.

Lots of media coverage.

Please also send a quick email to CERT IL with the info below, adding our Anonymous IN12-501 (or 502) and offer assistance if required. If you look for a contact, check the CIIP directory, CDO portal under contacts (first entry I think), or FIRST.org (CIIP is better).

SOP for the NT: check the wiki, and search the framework page for NT, notification product. There is an rdims template link in the SOP.

Text proposed:
"CCIRC is aware of media coverage on cyber attacks by the group Anonymous on Israel web sites. No significant impact is reported. CCIRC is monitoring and reached out to Israel CERT to offer assistance if needed."



From: Anderson, Windy
Sent: Sunday, April 07, 2013 8:51 AM
To: CCIRC-CCRIC; Bendelier, Kenneth; Beaudoin, Luc
Subject: Re: CYBER NOTIFICATION-13-007 –LOW IMPACT SEVERITY – MEDIA INTEREST - Anonymous - OpIsrael Websites

Sop worked. I did not read it [redacted] and Chris called. s.19(1)

Excellent. Good work Chris.

Chris will also send me (phone or email) some additional details so I can relay to my boss, if needed.

Windy

From: CCIRC-CCRIC
Sent: Sunday, April 07, 2013 08:12 AM
To: Bendelier, Kenneth; Anderson, Windy
Subject: CYBER NOTIFICATION-13-007 –LOW IMPACT SEVERITY – MEDIA INTEREST - Anonymous - OpIsrael Websites

Ken/Windy,

For your review, comments, edits, and whatnot.

Incident Number: CNT-13-007 – VERY LOW IMPACT SEVERITY – MEDIA INTEREST

Description of Incident: CCIRC is aware of media coverage on cyber attacks by the group Anonymous on Israeli web sites. No significant impact is reported. CCIRC remains vigilant and has reached out to Israeli CERT to offer assistance if needed."

Sources of reporting: Open Media Sources

Current actions: CCIRC has reached out to the Israeli CERT and shared its related mitigation product.

Initial analysis / assessment:

There is no reported Canadian Impact.

Disclaimer:

This notification is only for distribution within the Government of Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Chris Briffett
Approved by: Kenneth Bendelier

Cyber Duty Officer | *Officier de veille cybernétique*
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Email : [redacted] s.16(2)(c)
Telephone | Téléphone +1 613-[redacted]
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: Bendelier, Kenneth
Sent: Sunday, April 07, 2013 9:08 AM
To: Anderson, Windy; CCIRC-CCRIC; Beaudoin, Luc
Subject: Re: CYBER NOTIFICATION-13-007 –LOW IMPACT SEVERITY – MEDIA INTEREST - Anonymous - OpIsrael Websites

Well done.

From: Anderson, Windy
Sent: Sunday, April 07, 2013 09:02 AM
To: CCIRC-CCRIC; Bendelier, Kenneth; Beaudoin, Luc
Subject: Re: CYBER NOTIFICATION-13-007 –LOW IMPACT SEVERITY – MEDIA INTEREST - Anonymous - OpIsrael Websites

Thanks again Chris.

Windy

From: CCIRC-CCRIC
Sent: Sunday, April 07, 2013 08:58 AM
To: Anderson, Windy; Bendelier, Kenneth; Beaudoin, Luc
Subject: RE: CYBER NOTIFICATION-13-007 –LOW IMPACT SEVERITY – MEDIA INTEREST - Anonymous - OpIsrael Websites

FYSA,

There are a lot of media reports that sites in Israel have been attacked but no significant affect has been seen thus far. If anything further develops or the situation changes we will keep you updated.

Chris
Cyber Duty Officer | Officier de veille cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Email :
Telephone | Téléphone +1 613
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

s.16(2)(c)

From: [redacted]
Sent: Monday, April 08, 2013 3:07 AM
To: CCIRC-CCRIC; [redacted]
Subject: Re: [redacted] CCIRC CE13-005294 [Anonymous - OpIsrael]

s.13(1)(a)
s.16(2)
s.19(1)

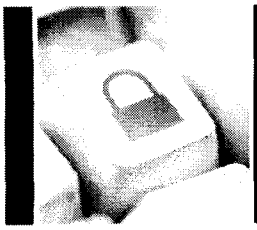
At 11:46 07/04/2013 +0000, CCIRC-CCRIC wrote:

Thanks for the headsup.

Regards,
[redacted]

>Good day,
>
> CCIRC is aware of media coverage on cyber attacks
>by the group Anonymous on Israel web sites, information attached below.
>CCIRC would like to extend our assistance to you if required. Also
>attached below is a copy of our Information Note on the group Anonymous.
>

[redacted]



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****

Date: 8 April 2013
CYBERDO: Bruce
****

[FOUO] NEW EVENTS:

1. Title: CE13-005296 [Malware Hosted on
- Summary: CCIRC has confirmed that malicious software is hosted on the following website:
  URL:
  IP:
  MD5:
  File size: 963.7 KB (986798 bytes)
  File name:
  File type: Win32 EXE
  Detection ratio: 9 / 43
  Analysis date: 2013-04-07 13:01:40 UTC
  ESET-NOD32: Win32/Injector.Autoit.BR
  Malwarebytes: Trojan.Autoit
- Action/Decision: CRR has been sent to the abuse contact.
  - Owner: Allen
  - Status: Closed

2. Title: CE13-005293 [Compromised sites that inject malicious iFrames]
- Summary: Compromised web servers potentially need to be wiped and restarted from scratch as root is often compromised via rogue SSH modules and other backdoors which may be installed. CCIRC is looking to draft a notification or CF-AL.
- Action/Decision: Research continues.
  - Owner: Allen
  - Status: Active

3. Title: CE13-005294 [Anonymous - OpIsrael]
- Summary: CCIRC is aware of media coverage on cyber attacks by the group Anonymous on Israeli web sites. No significant impact has been reported. CCIRC remains vigilant and has reached out to Israeli CERT to offer assistance if needed.
- Action/Decision: CNT-13-007 has been released.
  - Owner: Chris

- Status: Closed

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE: NIL

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS: NIL

PUBLICATIONS: NIL

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. **Anonymous hackers launch massive cyber assault on Israel Cyberspace**
   "A cyber attack campaign, dubbed *#OpIsrael* by hacking group Anonymous, targeting Israeli websites caused massive disruption to government, academic and private sites Sunday. Israeli media said small business had been targeted. Some homepage messages were replaced with anti-Israel slogans."
   Reference: http://thehackernews.com/2013/04/anonymous-hackers-launch-massive-cyber.html
2. **Hackers attack Israel, but damage 'minimal'**
   "JERUSALEM (AFP) - Hackers have launched an assault on Israeli websites, but the damage has been minimal as the Jewish state is prepared to fend off such attacks, one of the country's top cyber experts said on Sunday."
   Reference: http://au.news.yahoo.com/thewest/business/a/-/tech/16615004/
3. **New Skype trojan mines Bitcoin via your PC**
   "A new kind of Trojan is going around that converts your computer into a Bitcoin miner. Currently the outbreak of the trojan is mainly located in Eastern Europe, Spain and in parts of Central America but is progressing rapidly."
   Reference: http://vr-zone.com/articles/new-skype-trojan-mines-bitcoin-via-your-pc/19542.html

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒

SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php) ☒
XSSED (http://xssed.com/archive/special=1) ☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1) ☒

Vulnerabilities:

Secunia (http://secunia.com/advisories/historic/) ☒
TrendLabs Malware Blog (http://blog.trendmicro.com/) ☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html) ☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/) ☒
Internet Storm Center – Sans (http://isc.sans.org) ☒
Softpedia – Security (http://news.softpedia.com/cat/Security/) ☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/) ☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/) ☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/) ☒
The H Security (http://www.h-online.com/security/) ☒
Help Net Security (http://www.net-security.org/) ☒
SecuriTeam (http://www.securiteam.com/) ☒

News and Trends:

The Kaspersky Lab Security News Service (http://threatpost.com/) ☒
Sucuri Research Blog (http://blog.sucuri.net/) ☒
F-Secure (http://www.f-secure.com/weblog/) ☒
Topix News (http://www.topix.net/tech/computer-security) ☒
Krebs on Security (http://krebsonsecurity.com/) ☒
Threat Level (http://www.wired.com/threatlevel/) ☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security) ☒
Info Security News Mailing List (http://seclists.org/isn/) ☒

[FOUO] GENERAL INFORMATION: NIL

From: Alex Baron <alex.baron@rcmp-grc.gc.ca>
Sent: Friday, April 12, 2013 7:27 AM
To: CYBERDO
Cc: Eric Demers
Subject: Re: FW: Suspect: Darkleech

Hi,

We received that info from shared services via the Tech Crime Branch. The incident happen mostly on April 9th, as soon as we know, we will let you know.

Regards

Alex

>>> CYBERDO [redacted] 4/12/2013 6:52 AM >>>
Good morning Alex,

This information was passed along to the Incident Handling team, from Luc, here at CCIRC.

[redacted]

We are asking if you can provide any technical details related to this attack?

We are aware that this falls under CTEC purview, but any information you can provide would be greatly appreciated.

Thank you,

Incident Handler | Gestionnaire d'incident
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613 [redacted] Facsimile | Télécopieur +1 613-991-3574
cyber-incident@ps-sp.gc.ca
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: Alex Baron [mailto:alex.baron@rcmp-grc.gc.ca]
Sent: Thursday, April 11, 2013 04:49 PM
To: Beaudoin, Luc
Cc: Eric Demers <Eric.J.Demers@rcmp-grc.gc.ca>
Subject: Suspect: Darkleech s.16(2)

Hi Luc

[redacted] s.19(1)

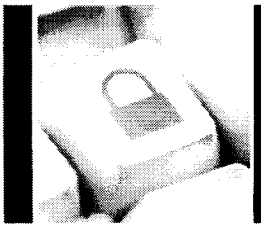
If you have any information, please let us know.

Regards

Alex

Cpl Alex Baron
Digital Forensic Investigator
Integrated Technological Crime Unit
National Division
155 McArthur ave
Ottawa, Ontario
K1A 0R4

W:(613) 949-7935
Fax: (613) 949-7952



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****

Date: 16 April 2013
CYBERDO: Vireak
****

[FOUO] NEW EVENTS:

1. Title: CE13-005374 [Anonymous OpUSA]
- Summary: CCIRC has received information regarding a possible cyber attack on the USA by the hacking group Anonymous.
  The attack has been scheduled for 07/05/2013 according to Anonymous.
- Action/Decision: CCIRC will continue to investigate.
  - Owner: Chris
  - Status: Active

2. Title: CE13-005375 [Ransomware]
- Summary: CCIRC has received a report from a company that they had been the victim of a ransomware infection.
- Action/Decision: CCIRC provided mitigation advice to the partner organization.
  - Owner: Chris
  - Status: Active

3. Title: CE13-005376 [Zegost Trojan found on .ca Site]
- Summary: CCIRC has received a report from a trusted source that a Canadian domain may be communicating with a C2 for Zegost.
- Action/Decision: Research continues.
  - Owner: Ron
  - Status: Active

4. Title: CE13-005378 [Report of .ca Sites Hosting Malware]
- Summary: CCIRC received information from a trusted source indicating that five Canadian sites may be hosting malware.
- Action/Decision: CCIRC sent notifications to the abuse contacts.
  - Owner: Ron
  - Status: Active

5. Title: CE13-005379 [Phishing Site Hosted in Canada]
- Summary: CCIRC received information regarding the following phishing site, which was being hosted in Canada:
  URL:
- Action/Decision: CCIRC sent a CRR to the hosting provider.

- Owner: Ron
- Status: Active

6. Title: CE13-005380 [Provincial Partner Observed an Increase in Scanning Activities]
- Summary: A provincial partner reported an increase of scanning/probing activities originating from a given list of IPs addresses.
- Action/Decision: Research continues.
  - Owner: Vireak
  - Status: Active

7. Title: CE13-005381 [Malware hosted on
- Summary: CCIRC confirmed that malicious code is hosted on the following website:
  URL:
  SHA1:
  MD5:
  File size: 167.8 KB (171830 bytes)
  File name:
  File type: ZIP
  Detection ratio: 27 / 46
  Analysis date: 2013-04-13 21:53:45 UTC
- Action/Decision: CCIRC notified the technical and abuse contact
  - Owner: Sharique
  - Status: Closed

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE: NIL

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS: NIL

PUBLICATIONS: NIL

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. **New security protection, fixes for 39 exploitable bugs coming to Java**
   "Oracle plans to release an update for the widely exploited Java browser plugin. The update fixes 39 critical vulnerabilities and introduces changes designed to make it harder to carry out drive-by attacks on end-user computers."
   Reference: http://arstechnica.com/security/2013/04/new-security-protection-fixes-for-39-exploitable-bugs-coming-to-java/

2. **Hackers Using Brute-Force Attacks to Harvest WordPress Sites**
   "Months of distributed denial of service attacks against major U.S. banks have evolved in magnitude and ferocity causing service disruptions for online banking customers. They've also shown the way for other attackers to adapt and evolve techniques used in those attacks."
   Reference: http://threatpost.com/en_us/blogs/hackers-using-brute-force-attacks-harvest-wordpress-sites-041513

3. **Anonymous hackers bring down North Korean websites for a second time**
   "Hackers associated with the group Anonymous earlier this month demanded that North Korean leader Kim Jong Un step down from power and adopt democracy. The demands went unanswered and the group has subsequently launched a variety of attacks aimed at North Korea's online properties. Hackers defaced social media accounts and other websites belonging to Pyongyang and mocked Kim Jong Un with images associating him with a pig. Now, for the second time in less than two weeks, Anonymous members have taken down nearly a dozen new North Korean websites."
   Reference: http://bgr.com/2013/04/15/anonymous-north-korea-cyberwar-hacking-439274/?utm_source=trending-widget&utm_medium=home

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒

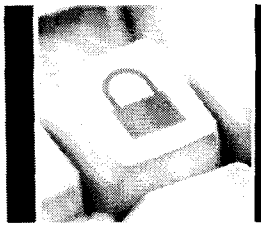
Internet Storm Center – Sans (http://isc.sans.org) ☒
Softpedia – Security (http://news.softpedia.com/cat/Security/) ☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/) ☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/) ☒
Websense Security Labs Blog
(http://community.websense.com/blogs/securitylabs/) ☒
The H Security (http://www.h-online.com/security/) ☒
Help Net Security (http://www.net-security.org/) ☒
SecuriTeam (http://www.securiteam.com/) ☒

News and Trends:

The Kaspersky Lab Security News Service (http://threatpost.com/) ☒
Sucuri Research Blog (http://blog.sucuri.net/) ☒
F-Secure (http://www.f-secure.com/weblog/) ☒
Topix News (http://www.topix.net/tech/computer-security) ☒
Krebs on Security (http://krebsonsecurity.com/) ☒
Threat Level (http://www.wired.com/threatlevel/) ☒
News Now
(http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security) ☒
Info Security News Mailing List (http://seclists.org/isn/) ☒

[FOUO] GENERAL INFORMATION: New CyberDO - Chris

Public Safety Canada / Sécurité publique Canada



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****

Date: 23 April 2013
CYBERDO: Chris
****

[FOUO] NEW EVENTS:

1. Title: CE13-005458 [Possible Leak of Municipal Police Credentials]
- Summary: CCIRC was notified that the emails and passwords of users in a municipal police force may have been publicly posted.
- Action/Decision: CCIRC notified abuse contact and were informed that the leaked credentials were falsified.
  - Owner: Tamara
  - Status: Closed

2. Title: CE13-005459 [Anonymous - OP CISPA]
- Summary: Hacking group Anonymous asked websites to black out their front pages on Monday, in protest against legislation in the U.S. that would allow online companies and government agencies to more easily share personal information.
- Action/Decision: Research continues.
  - Owner: Allen
  - Status: Active

3. Title: CE13-005460 [APT Targeting
- Summary: CCIRC has received information that there may be targeted attacked related to the upcoming
- Action/Decision: Research continues.
  - Owner: Chris
  - Status: Active

4. Title: CE13-005465 [Blacklist Canadian Domains]
- Summary: CCIRC received a report from a trusted source of blacklisted Canadian domains:

Trojan[.]JS/Kryptik[.]AJO
2013-04-19

Canada

[redacted]

Trojan[.]JS/Kryptik[.]AJA
2013-04-19

[redacted]

Trojan[.]JS/Kryptik[.]AJI
2013-04-20

[redacted]

Trojan[.]JS/Kryptik[.]AJJ
2013-04-22

[redacted]

- Action/Decision: Notifications sent to abuse or technical contacts.
  - Owner: Tamara
  - Status: Closed

5. Title: CE13-005467 [DDOS attampt on a financial sector]
- Summary: CCIRC received information that a Canadian IP was hitting the URL of a financial sector partner 474,985 times in the past two days using the user-agent

[redacted]

- Action/Decision: Notified Canadian IP abuse contact. Awaiting details of their investigation.
  - Owner: Sharique
  - Status: Active

6. Title: CE13-005468 [Blacklisted Canadian Domains]
- Summary: CCIRC received information from a trusted source of the following blacklisted canadian domains hosting malicious software.

[redacted]

Trojan[.]Java/Exploit[.]Agent[.]NDH
2013-04-22

[redacted]

Trojan[.]Java/Exploit[.]Agent[.]NDH
2013-04-22

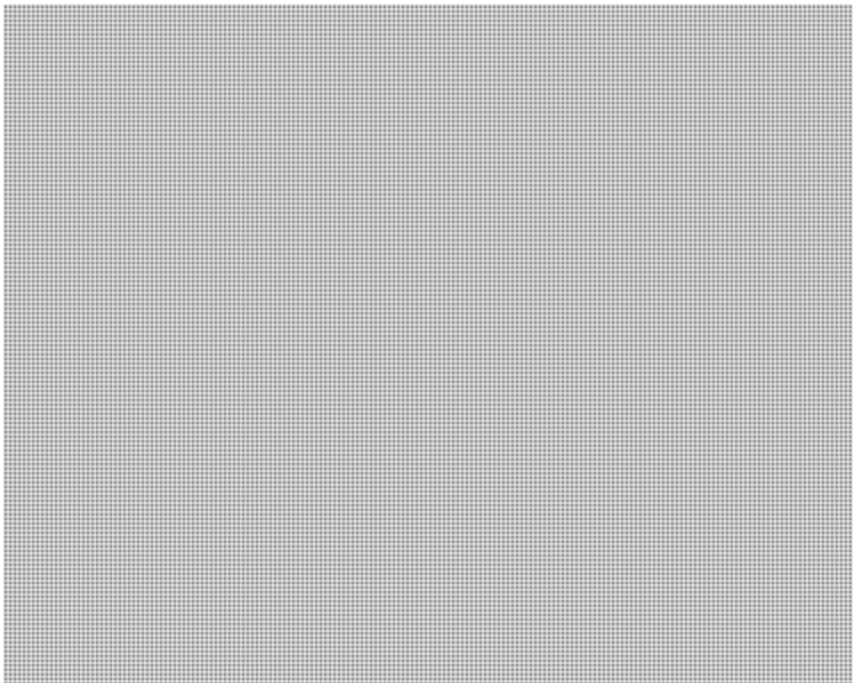
- Action/Decision: Notifications sent to abuse or technical contacts.
  - Owner: Ron
  - Status: Closed

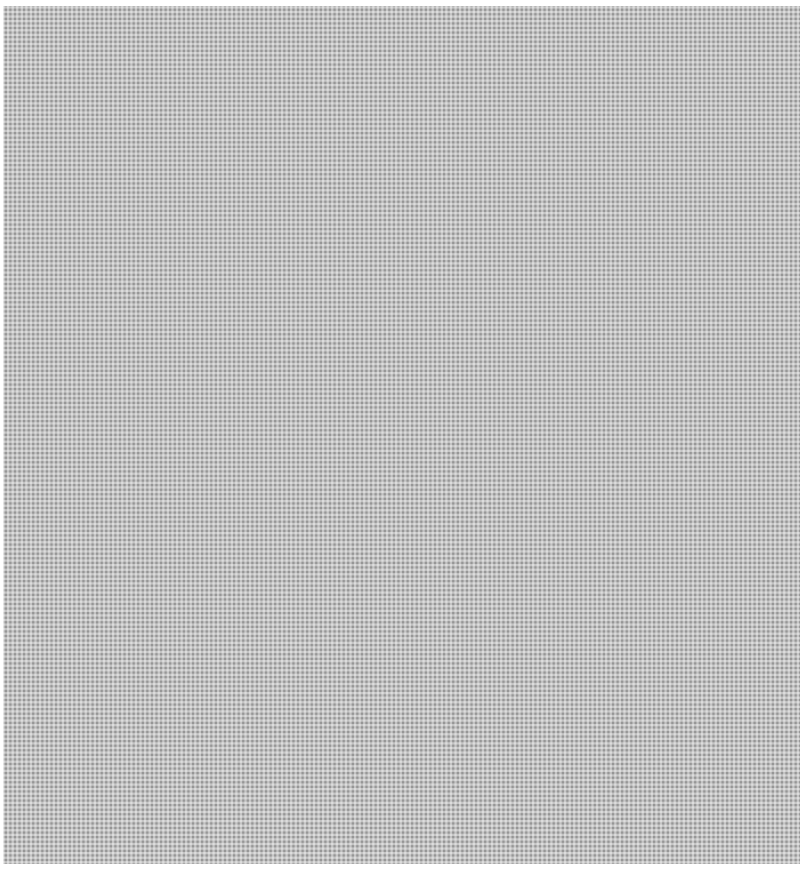
7. Title: CE13-005469 [Possible Breach of Teavana Systems]
- Summary: CCIRC has been informed of the reporting of a possible breach of Teavana systems. Reference article is below: http://krebsonsecurity.com/2013/04/sources-tea-leaves-say-breach-at-teavana/
- Action/Decision: Research continues.
  - Owner: Ron
  - Status: Active

8. Title: CE13-005470 [Zeus hosted on
- Summary: CCIRC has confirmed that malicious software is hosted on the following website:
  IP:
  Zeus Drop URL:
- Action/Decision: Notification sent to abuse or technical contacts.
  - Owner: Chris
  - Status: Closed

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. Title: CE13-005417 [Spear Phishing Report Received]
- Summary: An Intelligence Report was received from a trusted partner regarding a spear phishing operation. The following indicators have been extracted:





- Action/Decision: Notified the client.
  - Owner: Ron
  - Status: Active

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS: NIL

PUBLICATIONS: NIL

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS:

1. **VirusTotal Allows Users to Scan PCAP Files**
   "Google's malware-scanning service VirusTotal has just been improved. Starting today, besides .exe, .pdf and .apk files, information security researchers and security enthusiasts can also analyze .pcap (packet capture) files.
   PCAP files are utilized for packet sniffing and analyzing data network characteristics."
   Reference: http://news.softpedia.com/news/VirusTotal-Allows-Users-to-Scan-PCAP-Files-347409.shtml

CYBER NEWS:

1. **Expert: Anonymous Hackers Will Likely Use 4 Attack Methods for OpUSA**
   "The hacktivist collectives behind OpIsrael have announced their intentions to launch a similar operation against the US on May 7. Experts from Radware, who have been monitoring the hackers' activities, say we should expect 4 attack methods."
   Reference: http://news.softpedia.com/news/Expert-Anonymous-Hackers-Will-Likely-Use-4-Attack-Methods-for-OpUSA-347470.shtml

2. **Tea Leaves Say Breach at Teavana**
   "Multiple sources in law enforcement and the financial community are warning about a possible credit and debit card breach at Teavana, a nationwide tea products retailer. Seattle-based coffee giant Starbucks, which acquired Teavana late last year, declined to confirm a breach at Teavana, saying only that the company is currently responding to inquiries from card-issuing banks and credit card brands."
   Reference: -http://krebsonsecurity.com/2013/04/sources-tea-leaves-say-breach-at-teavana/

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☒
The H Security (http://www.h-online.com/security/)	☒
Help Net Security (http://www.net-security.org/)	☒

SecuriTeam (http://www.securiteam.com/) ☒

News and Trends:

The Kaspersky Lab Security News Service (http://threatpost.com/) ☒
Sucuri Research Blog (http://blog.sucuri.net/) ☒
F-Secure (http://www.f-secure.com/weblog/) ☒
Topix News (http://www.topix.net/tech/computer-security) ☒
Krebs on Security (http://krebsonsecurity.com/) ☒
Threat Level (http://www.wired.com/threatlevel/) ☒
News Now
(http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security) ☒
Info Security News Mailing List (http://seclists.org/isn/) ☒

[FOUO] GENERAL INFORMATION: New CyberDO - Gregg

From: Beaudoin, Luc
Sent: Thursday, April 25, 2013 9:57 AM
To: CYBERDO; [redacted] Clow, Patrick
Subject: FW: [TWG] FYI - #OpUSA

fyi

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: [redacted] [mailto:[redacted]
Sent: Thursday, April 25, 2013 9:38 AM
To: [redacted]
Cc: Beaudoin, Luc
Subject: [TWG] FYI - #OpUSA

[redacted]

Pages 1251 to / à 1252
are withheld pursuant to section
sont retenues en vertu de l'article

16(2)

of the Access to Information
de la Loi sur l'accès à l'information

[redacted]

[redacted]

Pages 1254 to / à 1272

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

From: CCIRC-CCRIC
Sent: Friday, May 03, 2013 10:08 AM
To: Clairmont, Lynda; Dick, Robert; Gordon, Robert; Jarmyn, Tom; Johnson, Mark; Mueller, Mike; Tony.Pickett@rcmp-grc.gc.ca; [redacted]@CSE-CST.GC.CA; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'cnoir@pco-bcp.gc.ca'; 'bdiogo@pco-bcp.gc.ca'; 'Eric.Belzile@ssc-spc.gc.ca'; Durand, Stéphanie; MacDonald, Michael; Wong, Suki
Cc: Anderson, Windy; Hatfield, Adam; Matz, Mark; Campbell, Tom; Duschner, Gabrielle; Paquet, Alain; Swift, Andrew; DeJong, Michael; Bendelier, Kenneth; Clow, Patrick; [redacted]Turbide, Frank; Klassen, Nathan; Proulx, Véronique; Pacha, Tomasz; Fortunato, Stephanie; Champoux, Martin; Hunt, Ryan; CYBERDO; GOC-COG
Subject: CYBER NOTIFICATION-13-010 – LOW IMPACT SEVERITY – MEDIA INTEREST – Hackers announce Operation USA

CYBER NOTIFICATION – INCIDENT

** This notification is only for distribution within the Government of Canada (see handling instructions below)*

Incident Number: CNT-13-010 – LOW IMPACT SEVERITY – MEDIA INTEREST

Description of Incident: Hackers have announced that Operation USA (OpUSA) will begin on May 7, 2013 and will reportedly target the websites of American organizations including those of financial institutions, high-profile government agencies, and commercial organizations. A number of hacker groups are expected to participate in these attacks, including the hacktivist collective Anonymous.

Sources of reporting: Open media sources and trusted partners.

Current actions:

- CCIRC has received detailed reports from a trusted partner that include information on the tools and techniques likely to be used for these attacks, the organizations likely to be targeted, as well as mitigation measures to be considered. These reports have been shared with some of CCIRC's partners.
- CCIRC will continue to assess the situation and keep its partners informed of any significant developments.

Initial analysis / assessment:

- At this time, CCIRC is not aware of any Canadian organization who may be directly targeted by these attacks. It is possible that Canadian organizations who share digital infrastructure with affiliates in the United States could be indirectly impacted.
- These attacks are expected to be similar, both in scale and in effect, to those launched against Israeli websites (OpIsreal) in April 2013, where several thousand websites are said to have been defaced.
- A trusted partner has assessed that these attacks will result in limited disruptions and will mostly consist of nuisance-level attacks against publicly accessible websites.
- Open source media has been reporting on these upcoming attacks since mid-April. It is expected that media coverage will increase when the attacks begin.

Disclaimer:

Distribution of this report remains under the control of Public Safety Canada. It is provided on condition that it is used by Government Departments and Agencies within Canada. It is not to be re-classified, copied, or resubmitted outside the

above mentioned organizations without the express permission of Public Safety Canada. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Véronique Proulx (990-7102)
Approved by: Ken Bendelier (993-5042)

From: [redacted]
Sent: Wednesday, May 08, 2013 9:58 AM
To: CCIRC-CCRIC; CSIRT
Subject: RE: OpUSA DDoS campaign

s.16(2)
s.16(2)(c)
s.19(1)
s.20(1)(c)

#OpUSA turned out to be a non-event for us yesterday- no attacks, no traffic of concern.

thanks anyhow!

[redacted]
s.19(1)

-----Original Message-----
From: CCIRC-CCRIC [mailto:[redacted]
Sent: May-08-13 9:56 AM
To: CSIRT;[redacted]
Subject: OpUSA DDoS campaign

Good morning,

I wanted to touch base with you regarding the recent OpUSA DDoS campaign led by the Anonymous group on May 7, 2013. Firstly, I wanted to make sure you were aware of the campaign. Secondly, if you notice any artifacts on your end that are suspicious or require a second opinion, please don't hesitate to send them to CCIRC. This could include logs collected at network devices, suspicious emails, malware samples, infection related packet capture and metadata.

Regards,

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-[redacted] Facsimile | Télécopieur +1 613-991-3574 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
10 Feb 2012	DirtJumper DDoS controller in Canada	2628	[redacted] s.19(1) s.20(1)(c)	Multiple	CCIRC received a request for assistance from CERT Australia in taking down Controller domain registered by a Canadian organization. [redacted] Whois comes back that EvoPlus LTD/evonames.com is the registrar. *Tech detail:* Network whois Ip: 195.3.147.30 AS41390 (Latvia, LV) Queried whois.evonames.com with "sadasdnwqjrrww.net"... Domain Name: SADASDNWQJRRWW.NET Abuse email: abuse@ru-tld.ru DOMAIN SUSPENDED DUE TO VIOLATION OF OUR TOS Registrant: [redacted] --Registrant is Ukranian CCIRC issued takedown request to EvoPlus, advised LE, CIRA and CERT Australia	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					Update: Site is now down	
7 Feb	Sendspace storing stolen data	2623			Canadian victims – 600 IP addresses Cyberflash sent 9 Feb 2012 "CCIRC has received reports of malicious activity involving the use of malware designed to collect and upload Microsoft Office documents to Sendspace.com. Sendspace is a file-hosting website that offers users the ability to send, receive, track and share large files. The attack begins by compromising the host with a malicious file named "Fedex_Invoice.exe". The file name used for this particular malware suggests that it is being used for a spam campaign, specifically one that uses messages disguised as a FedEx shipment notification. The malware attempts to access the following websites to download additional files: hxxp://south78483825.ru/hhh/index.php etc.... The malware searches the local drive of an affected system for Microsoft Word and Excel files. The documents are then archived and password-protected using a random-generated password in the user's temporary folder. After creating the archive, the malware	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					sends the archive to the Sendspace.com website. Upon successfully uploading the archive, the malware sends the generated download link and archive password to the C&C server: hxxp://south78483825.ru	
6 Feb	Fraudulent GoC website – possibly malicious	2621	Govt	N/A	Hosted in Dallas, Texas Was previously listed on MDL 2011/07/02 for trojan Renos Was previously on a malware list TrendMicro=Malicious site URL Query= malicious reputation TrustedSource=High Risk 61 domains also point to this IP address Murphy, Gregg (2/10/2012 1:11 PM): Sent request to CIRA asking for their assistance in deactivating the hrsdc-cic-gc[.]ca domain. Murphy, Gregg (2/6/2012 2:33 PM): Confirmed that site was collecting sensitive private information. Sent takedown request to abuse@softlayer.com and cc'd us-cert.	Ask Gregg what CIRA can do to deactivate the domain
8 Feb 2012	Possible APT Hop Host – Technology Institute	2624	Educational		Information received from a trusted source regarding a potential hop host in a post-secondary school [redacted]. Source recommended reviewing logs from that host for the past 2 weeks looking at port 443 traffic and any other unusual ports. No specific domains or IP addresses are	

s.16(2)(c)

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					available. It is suspected that during the early morning hours of Feb 6th, ftp activity using possibly valid credentials from unusual domains or IP addresses may have occurred. It is also suspected that changes were made to the server file store prior to Feb 6th. Suggested [redacted] review any changes to the file store or new ftp accounts that were recently created	
7 Feb 2012	Ransomware – GoC logos being used – CSIS logo	3458	Govt/Public	N/A	Reports of popups on computers saying they have been looking at child porn and their browser will be shut down unless they pay money. Logo for CSIS is being used on the messages. --Website hosted in Moldova Update: Passed to LE – RCMP investigating	
9 Feb 2012	Canadian IP listed on Zeus tracker	2626	N/A		It is part of a FastFlux botnet Hosting provider in BC, Drop URL is in Russia Email delivery to abuse contact failed. Emailed parent co. Sent takedown request to hosting provider, cc'd LE Incident now closed	
2 Feb 2012	Info compromise (Canadian Credit card info on Pastebin)	2616	General Public	Unknown	Appears to be a continuation of the Stratfor incident 6 Canadians listed in the post – they don't use GoC email addresses	
8 Feb	IRC botnet	3461	Energy		An energy partner ([redacted] reported that the Botnet in which they had participated three months ago was still active. (They provided information about an active IRC channel for the Raumoni Perl Bot controller). They were involved in a similar event 3	■

s.16(2)(c)
s.20(1)(c)

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					months ago (CE11-2508). CCIRC Ops asked Technical Team to investigate so that victims can be identified/notified. Bot channel:ircu.uk.to:81 [redacted]	
30 Jan	DNS Changer Malware	2605	Provincial govt (2), energy (1), finance (1), telecom (18), Health (1), Transport (1), universities (14), college/tech instit (2), other industries (1), other institutions (2)	43	It may be time to do some statistical analysis for who mitigated and who didn't… Luc dissuaded me last week.	Discuss with Editorial Board
1 Feb	DNS Changer Malware	2615	01B Provincial; 02A Telecoms; 02B Finance; 02C Energy; 02D Transportation; 02H Health; 05 Academia s.20(1)(c)		Notifications sent to IT security or technical contacts in the following organizations: Provincial: 2 provinces ([redacted] Telecom: 17 companies [redacted] Finance: 2 banks [redacted] Energy: 2 company [redacted] Transportation: 1 company [redacted] Health: 2 organizations [redacted] Academia: 15 universities [redacted]	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					[redacted]	
3 Feb	DNS Changer Malware	2619	01B Provincial; 02A Telecoms; 02B Finance; 02C Energy; 02D Transportation; 05 Academia		Provincial: 3 provinces [redacted] Telecom: 21 companies [redacted] Finance: 1 bank [redacted] Energy: 1 company [redacted] Transportation: 1 company [redacted] Academia: 12 universities [redacted] Thu 02/02/2012 2:47 PM **Media Report: Half of Fortune 500s, US Govt. Still Infected with DNSChanger Trojan** http://krebsonsecurity.com/2012/02/half-of-fortune-500s-us-govt-still-infected-with-dnschanger-trojan/	s.16(2)(c) s.20(1)(c)
7 Feb 2012	DNS Changer Malware	2622	Provincial, Telecom, Finance, Energy,	33	Dns-ok.ca site now up, hosted by CIRA CCIRC one of the four CERTS in the world	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
			Transportation, Education		that have this kind of site for public (NL, US, Germany)	
31 Jan	Phishing	2611	Financial	1	– registrant of malicious website is in Russia Notification sent to Bank's phishing intake, google safe browsing & APWG	
1 Feb	Phishing	2612	Financial	1	– registrar is in NL, hosted by AMEN France Network	
1 Feb	Phishing	2614	Financial	1	– hosted in Colorado Reported by RCMP (still Anti-Fraud Centre?) Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE Hosted by NTT America, Inc in Greenwood Village, Colorado.	s.20(1)(c)
2 Feb	Phishing	2617	Financial	1	 Hosted in the US Notification sent to Bank's phishing intake, google safe browsing & APWG	
30 Jan 2012	Phishing	2602 & 2603	Financial		site hosted in Colorado, USA Two Different IP addresses Reported to phishing intake, Google Phishing Filter Service & APWG	
9 Feb	Phishing	2627	Financial	1	- hosted in Vietnam Couldn't notify APWG because we don't have enough info – only got the two links hxxp://www[.]dipcare[.]com[.]vn/WBB6/https/businessbanking[.].]com/WBB/ hxxp://www[.]tradecare.com[.]vn/WBB6/https/businessbanking[.].]com/WBB/	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					Both links resolve to 203.162.71.16 AS7643 (Vietnam, VN)	
3 Feb	Phishing	2618	Financial	1	[redacted] hosted in the US Same domain we saw for [redacted] on previous day, same IP address	
6 Feb 2012	Phishing	2620	Financial	1	[redacted] - hosted in Berlin, Germany Notified [redacted] phishing intake, APWG, Google Safe Browsing	
30 Jan	Phishing	2604	Financial	1	[redacted] - site hosted in Berlin, Germany Reported to [redacted] phishing intake, Google Phishing Filter Service & APWG	
31 Jan	Phishing	2609	Financial	1	[redacted] site hosted in US Notification sent to Bank's phishing intake, google safe browsing & APWG	
31 Jan	Phishing	2068	Financial		[redacted] - site hosted in US Notification sent to Bank's phishing intake, google safe browsing & APWG	
31 Jan 2012	Website Defacement	2606	Provincial Govt (Dept Health)	1 [redacted]	Domain registered by the org listed on a well known defacement site as targeted for defacement using unspecified exploit techniques. Response from dept indicated defacement was identified by local IT staff on Sunday and default page was replaced with "under construction" until it was fixed by website support staff. No loss of personal data, no replacement of content. Website restored with correct permissions	

s.16(2)(c)
s.20(1)(c)

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
31 Jan	Website defacement	2607	Website registered by a student & community organization		Sent notification to their hosting ISP [redacted]	
31 Jan	Website defacement	2610	Education	1 (the Pipeline Security Specialist training programme)	Notification sent to operator group and their hosting provider [redacted]	
1 Feb	Website defacement	2613	Health	1	[redacted] CCIRC observed that a website operated by/for the [redacted] medical centre was recently defaced. Notification sent to the domain technical contact ([redacted]	s.20(1)(c)
8 Feb	Website defacement –	2625	Govt		CCIRC observed that a website registered by a provincial government treasury department was recently defaced.	

Upcoming events:
Cyber security workshop – Toronto, Canada – 27-29 Feb 2012
Vulnerability: (second week of Feb)

- OSCommerce v3.0.2 – persistent cross-site scripting vulnerability
  - SPAM w child porn
  - Spoofing RCMP & CSIS
  - SQL injection attacks (Bruce) – not clear what the redirect does ACTION: Talk to Bruce

Cyber News from Dailys:

- **Millions caught up in Android botnet (30 Jan 2012) – Symantec found** trojan was packaged into at least 13 free games published by three different publishers on the official app download site – *not sure about the Canadian nexus, except that Canadians do use Android phones, and increasing malware for mobile phones is a trend that was spotted for 2012 by different security companies. Researchers from Lookout Security disagreed with Symantec saying it's just adware and not*

- **Anonymous hacks French Government Website as ACTA row rumbles on (31 Jan 2012)**
- **Many pcAnywhere systems still sitting ducks – more than 140,000 computers still at risk –** ACTION: CCIRC was supposed to ask for Canadian IPs. Follow up. (Note: This software still used by small businesses, early form of PC remote control for windows, probably still used for remote computer maintenance)
- **WikiLeaks buying boat to move servers offshore?** (2 Feb 2012)
- **Hackers exposing hate movements post names of 74 Canadians (Anonymous) 2 Feb 2012**
- **Google beefs up security on Android Market**
- **FBI Friday: Anonymous Hackers Release Internal Conference Call Recording**
- **DHS website hacked by Anonymous (7 Feb 2012) –** *website was back up within minutes* http://rt.com/usa/news/homeland-security-website-anonymous-473/
- **TeamPoison Hackers hit the UN (9 Feb 2012)**
- **Google to strip Chrome of SSL revocation checking – (9 Feb 2012).** The browser will stop querying CRL (certificate revocation lists and databases that rely on the Online Certificate Status Protocol – OCSP. Instead, Google will rely on its automatic update mechanism – maintain a list of certificates that have been revoked for security reasons. Google appealed to CA's to provide a list of those. This change will happen in months. ***This is potentially a new certificate model***

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-02-12 8:49 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 2, 2012 / le 2 janvier 2012

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Un cas humain de H5N1 recensé en Chine
Un possible cas humain de grippe aviaire H5N1 a été recensé à Shenzhen dans le sud de la Chine, ont annoncé les autorités sanitaires locales. La ville borde Hong Kong où la présence du virus a été confirmée chez deux oiseaux la semaine dernière. Un chauffeur de bus de 39 ans, hospitalisé le 21 décembre avec de la fièvre, a été testé positif vendredi au virus H5N1, selon un communiqué diffusé sur les sites Internet des autorités sanitaires de la ville de Shenzhen et la province du Guangdong. Les experts de la province pensent qu'il a bien été contaminé par le virus de la grippe aviaire et ont signalé le cas au ministère chinois de la Santé pour qu'il confirme le diagnostic. L'Organisation mondiale de la santé a été prévenue par le ministère, selon le communiqué. Le Quotidien, 54

Avalanche victim identified
RCMP have identified the 45-year-old man who died in an avalanche while on a heli-skiing tour near Revelstoke, in southeast B.C. Police say the victim is Ronald Gregory Sheardown, a former Canadian from Stouffville, Ont., who had been living in Dubai. Sheardown was among a group of 11 people and a guide with Canadian Mountain Holidays when the snowslide came crashing down on some of them Friday afternoon. Three people managed to dig themselves out, but Sheardown was pulled out unresponsive after being located via the signal from his personal avalanche transceiver. Red Deer Advocate, A6; Toronto Star; Vancouver Province; Globe and Mail

CYBER SECURITY / CYBERSÉCURITÉ

Academics hack web activists
If the word "hacker" brings to mind a social outcast eating junk food in his mom's basement, you are probably underestimating the power of "hacktivism," or online activism. Academics have been studying for years the very non-academic undertakings of hacktivists - especially the group Anonymous. These include the repeated hacking of the Church of Scientology's Web site, the infamous online message board 4Chan and the philosophy of "doing it for the lulz." Their findings, while not your average classroom fare, are helping to paint a picture of a leaderless, geographically and socioeconomically diverse and powerfully disruptive group. New Brunswick Telegraph-Journal, B3

LAW ENFORCEMENT AND POLICING BRANCH / SECTEUR DE LA POLICE ET DE L'APPLICATION DE LA LOI

Murders at 25-year low - After 4 years of declines, city records 45 homicides, lowest number since 1986
Toronto has closed the book on 2011 with the lowest homicide total in a quarter century. The city recorded 45 homicides, the lowest number since 1986, when there were 37 murders. In 2010, there were 61 homicides. This is also the fourth straight year of declines since 2007, when the city recorded its deadliest year (matched in 1991) with 86 homicides. The plunge in Toronto's homicide numbers no doubt bolsters Chief Bill Blair's image. Blair's image took a hit in 2010 following the mass arrests during the meeting of G20 leaders and the controversy that followed. Regarding the homicide rate, Blair says there's still more work to do. "I think we can make this city safer," the chief told the Star. The chief attributed some of the decline in 2011 to the disruption of gang activity following sweeping raids carried out across the city and region. Toronto Star, GT1

RCMP officer sues over exploding doll - Twisted prank hurt hands, he claims

A Mountie has filed suit against two fellow officers in the bomb-squad unit, the RCMP and the province of B.C. after a mechanical doll he kept at his desk was rigged to explode, disfiguring him to the point of requiring hand surgery and hearing aids in both ears. Cpl. Tyrone Hempston suffered "severe injuries" after returning from Christmas holidays to his desk at the Explosive Disposal Unit in Delta on Jan. 4, 2010, where he noticed some-one had tampered with his Dirty Bertie mechanical doll. "He sat down and picked up the doll, held it in both hands close to his lap, then switched it on and it exploded in his hands," according to the writ filed in Vancouver Supreme Court of B.C. Vancouver Province, A4

Latest Hobbema homicide sparks call for new programs
Hobbema cops urge better anti-domestic violence programs after a slaying on the troubled reserve Saturday. "We want to get a handle on domestic violence," said RCMP Const. Perry Cardinal. "We want to bring in different programming -- like something that can (align) our domestic violence unit, the women's shelter and the victim services centre to clean all of this up." Mounties were called to a Samson Cree Nation home some time around 7:40 p.m. on New Year's Eve where they found a 34-year-old man with multiple stab wounds. Calgary Sun, 7 (Edmonton Sun); Edmonton Journal (Windsor Star); Red Deer Advocate

Cops to probe man's death
The Vancouver Police Department Major Crime Homicide Squad will investigate the death Friday of a man in custody of the Surrey RCMP. A 58-year-old male arrested Dec. 23 for breaching a court order was found lying on his cell floor Dec. 26. He was taken to hospital and died Friday. Vancouver Province, A4

Accident sends officers, driver to hospital
A pair of RCMP constables are feeling lucky to see the new year arrive after an allegedly speeding driver crashed his van into the officers' parked cruiser near Terrace, B.C., sending all three to a nearby hospital. David Schiffer, a 35-year-old Czech national working in Terrace, was driving on Highway 16 near Ferry Island late Friday night when Constable Philip Crack and Auxiliary Constable Shelley Ullery clocked his white van travelling more than 120 kilometres an hour in a 50 km/h zone. The officers say he hit the brakes but lost control, and seconds later the van careened sideways into the back of the police car they were sitting in. Both constables and Mr. Schiffer were taken by ambulance to Mills Memorial Hospital and later released, and though the extent of their wounds has not been divulged, the RCMP considers them fortunate. Globe and Mail, S1

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

How they screen the screeners - Airport guards who flunk tests for finding bombs through X-rays face suspension of screening credentials, not loss of employment
The continuing threat of aviation terrorism means guards are gauged on their ability to pick out improvised explosive devices (or IEDs) from carry-on luggage. Records show they are also tested on their ability to spot hidden guns, knives, grenades in carry-on bags - and even martial-arts weapons, such as the deadly metal throwing stars associated with Japanese ninjas. Dending a guard home for good is no easy thing in Canada. Despite failed tests, a guard could be back at work within a few weeks. His poor tests resulted in the suspension of his screening credentials, not in his being fired. Globe and Mail, A5

Border staff, police clash - No-arms rule spat rekindled
A dirty-bomb alert involving armed Montreal customs agents has re-ignited a bitter dispute over whether Canada's border services personnel should be allowed to take part in joint operations with other law enforcement agencies. Almost a year after the Canada Border Services Agency's Ottawa hierarchy halted joint operations with police forces across the country, the Ottawa Citizen has learned that Montreal agency managers twice refused to join a multi-force anti-terrorism search earlier last month after intelligence reports indicated cyanide and other dirty-bomb materials were stashed in a trailer at a Montreal storage yard. Local CBSA managers declined the request from leaders of the joint armed forces, RCMP and Quebec provincial and Montreal city police emergency force for fear of contravening their bosses' "no co-operation" edict laid down last December. Windsor Star, B1 (Ottawa Citizen, Vancouver Sun)

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Bill C-10 will target gangs not teens, minister says - Federal crime bill
Canadian jail cells are not going to be filled with teenagers and college students who share marijuana with friends, according to Justice Minister Rob Nicholson, who says his crime bill has been grossly misrepresented. In a year-end interview with Postmedia News, he said mandatory minimum sentences for marijuana production are designed to target

organized crime, gangs and grow-ops. They don't apply to youths -- and even new provisions that aim to penalize adults who are trafficking drugs around schools mean perpetrators would have to be caught with an "eight-pound joint" to be saddled with a mandatory minimum under the safe streets and communities act, he argued. The omnibus crime bill, which bundled nine different bills into one, Bill C-10, is poised to pass in early 2012. National Post, A5

Hijabs don't hinder prison guards
An editorial states "Last week, Quebec moved to allow Muslim women prison guards to wear hijabs on the job, but it only did so as part of a settlement of a human rights complaint filed four years ago. However, the decision will hopefully pave the way for other Muslim women interested in correctional careers, in Quebec and in the rest of Canada. Accommodating the hijab as part of a guard's uniform is no different than allowing Sikh RCMP officers to wear their turbans instead of the regulation hats. Turbans have never interfered with the ability of a Mountie to do his job, and it will be the same for the hijab, as long as women guards wear head scarves with Velcro fastenings that allow for quick removal in an emergency. Unlike burkas and niqabs, the hijab does not obscure the face. The line in the sand should be drawn at hijabs - they are as far as government should go in permitting religious or cultural head coverings among female guards." Calgary Herald, A8

PUBLIC SERVICE / FONCTION PUBLIQUE

PS job fears grow as cuts draw closer - 'Everything points to bleak times'
An axe hangs over federal government departments and public servants and where it falls finally should be known within weeks. The government is finalizing decisions on a sweeping operating spending review to chop billions of dollars annually from the federal budget. It has unions fearing that potentially, tens of thousands of federal employees could receive pink slips. Treasury Board President Tony Clement is leading the strategic review that is searching for $1 billion in cuts in the upcoming 2012-13 spring budget, $2 billion for 2013-14, and $4 billion annually by 2014-15 and beyond. Nearly 70 government departments and agencies have submitted scenarios for a five- and 10-per-cent cut to their budgets as part of an examination of about $80 billion in direct program spending. More than 600 proposals are being considered. The government needs the savings to help eliminate a $31-billion deficit by 2015-16, at the earliest. Ottawa Citizen, A3 (Vancouver Province, Fredericton Daily Gleaner)

INTERNATIONAL / INTERNATIONAL

Canadian role in peace relations questioned - Efforts fail to end Afghan-Pakistani border bickering
Canada's contribution to Afghan-Pakistan peace is being questioned after a recent investigation found distrust and long-standing disputes were at the root of a cross-border air-strike that killed 24 Pakistani soldiers in November. The joint U.S.-NATO study recommends several actions to prevent another such incident -- actions Canada has been trying to undertake for four years, with mixed results. The investigators made seven recommendations. Since November 2007, Canada has taken the lead in facilitating dialogue and understanding between officials on either side of the heavily travelled but unsecure border. Initially labelled the Dubai Process, the effort has since been renamed the Afghanistan Pakistan Co-operation Process. The government has boasted some successes over the years, but there have also been indications the Canadian efforts have not addressed many of the underlying issues. Numerous U.S. diplomatic cables released through WikiLeaks showed Afghan and Pakistani officials bickering as often as not. National Post, A16

Olympic health workers get shot against bio-terrorism
Five hundred health workers have been vaccinated against smallpox to deal with any biological terror attack at this year's Olympics. The move highlights the level of concern over the prospect of extremists turning to germ warfare. Britain has also stockpiled sufficient smallpox vaccines to "mount a UK-wide vaccination program" in the event of a deliberate re-lease of the disease, which was declared eradicated in 1980. A report last year warned Games venues or public trans-port would make an "appealing target" for terrorists to launch biological attacks. The deadly disease could be spread by aerosols and is highly contagious. Vancouver Sun, B4 (Ottawa Citizen)

California cracks down on global slave labour - Law forces firms to check supply chains
A new California law will force retailers and manufacturers to disclose how they guard against slavery and human trafficking throughout their supply chains, ratcheting up scrutiny of some of the largest U.S. corporations. Beginning today, about 3,200 major companies doing business or based in California, a list that includes Apple and Gap Inc., will be required to disclose steps they take, if any, to ensure their suppliers and partners do not use forced labour. Companies risk getting sued by the state attorney general if they flout that law. But experts say the real pressure will come from the court of public opinion: consumers who care about ethical working conditions and take an interest in how their favourite brands get made. Calgary Herald, B4

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From: Moore, Bruce
Sent: January-03-12 1:09 PM
To: 'Scott.Foster@rcmp-grc.gc.ca'
Cc: Bendelier, Kenneth; [redacted]
Subject: RE: CIIT Update - STRATFOR Breach [CCIRC CE11-2549]

Good Afternoon Scott & Happy New Year;

[redacted]

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

-----Original Message-----
From: Bendelier, Kenneth
Sent: January-03-12 11:05 AM
To: Moore, Bruce
Subject: Fw: CIIT Update - STRATFOR Breach

Hi Bruce,

If you're in, you might want to update Scott on what we've done.

Thanks

From: Scott Foster [mailto:Scott.Foster@rcmp-grc.gc.ca]
Sent: Tuesday, January 03, 2012 11:03 AM
To: Scott Foster <Scott.Foster@rcmp-grc.gc.ca>
Subject: CIIT Update - STRATFOR Breach

Good day,

[redacted]

Pages 1292 to / à 1293

are withheld pursuant to section

sont retenues en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-03-12 8:27 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Baker, William V.; 'Black, Dave'; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; 'Clarfield-Henry, Alexis'; Crépeault, David; 'CSIS Media Monitoring'; [redacted] De Curtis, Laura; 'Dunn, John'; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; 'Gilbert, Monica'; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; 'Patry, Line'; Patton, Michael; 'RCMP Emerging Trends'; Roberts, Shane; Robinson, N.; 'Salas, Anik'; 'Slade, Nancy'; Spendlove, Jim; Stanfield, Charles; 'Stewart, Christena'; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; 'Wadasinghe, Cheryl'; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 3, 2012/ le 3 janvier 2012

Print Media

Software scam hits Windsor area - Police get hundreds of complaints
Canada's No. 1 fraud is a computer scam that has gone viral throughout Windsor-Essex. Windsor police Staff Sgt. Gerry Corriveau, with the financial crime unit, said he received hundreds of calls in 2011 from consumers who describe someone calling them claiming they are able to help protect their personal computers from viruses. One scenario involves a caller claiming they are from Microsoft or another reputable software company. Consumers say the scammers strongly suggest purchasing an antivirus repair service by credit card over the telephone. Windsor Star

Online Media

Amazon Shipment Spam Campaign Delivers Malware - If the recipient clicks on a link in the message, they're taken to a Web site serving Windows malware
A new spam campaign claiming to come from Amazon.com states that a smartphone is being shipped to the recipient, in an attempt to spread malware. "Users who may be tempted to click on the links contained in the message are taken to a website that serves a piece of malware which relies on unpatched Windows vulnerabilities to drop its payload," writes Softpedia's Eduard Kovacs. "The malware in question is a variant of Cridex, especially designed to steal personal and financial information from the computer it lands on, reports Hoax Slayer," Kovacs writes. eSecurity Planet

Hackers hitting NGOs with backdoor attacks
Hackers may be targeting non-government organizations with a series of backdoor attacks, a computer security firm warned this week. Trend Micro said it has found evidence that Amnesty International (AI), whose UK website was attacked recently, is "not the only intended target for the attack. Based on our investigation, it seems that the initially reported affected organization is just one of the targets in this attack and that the attack itself is fashioned specifically for the targets," it said in a blog post. It cited earlier reports the attack on AI's website involved an iframe that redirected users to another compromised site in Brazil. GMA News

Indian cyberspace hit by Kim Jong-Il malware mails: IT sleuths
Indian computer security analysts have detected and alerted internet users against "malicious spam mails" in the name of the dead North Korean leader Kim Jong-Il leading to hacking and crashing of vulnerable e-mails. The Indian Computer Emergency Response Team (CERT-In), country's national agency to respond to computer security incidents, has found the malware virus streaming into the Indian cyberspace. IBN Live

Saudi hackers publish Israeli credit card numbers on the Internet

Israelis won't be in a hurry to cyber shop this week, as thousands woke up horrified Tuesday to find their credit card numbers along with their personal details published online. Overnight, Saudi hackers named Group-XP claimed they broke into a leading Israeli sports site, redirecting surfers to a page where they could download a file containing the sensitive information. The hackers claimed they published valid and current personal and credit card information belonging to nearly half a million Israelis. Credit companies pored over the lists throughout the night and cite a much lower number. According to the Bank of Israel, the number of compromised cards is approximately 15,000. Los Angeles Times

Stuxnet possède au moins quatre frères et sœurs
Stuxnet n'est pas seul. Le virus qui a détérioré des installations nucléaires en Iran, appartient en effet à une famille comptant au moins cinq cyber-armes nuisibles sorties de la même plate-forme de développement. Voilà ce qu'affirme le spécialiste russe de la sécurité Kaspersky Lab. Les experts en cyber-sécurité affirment depuis assez longtemps déjà que les Etats-Unis et Israël sont à l'origine de Stuxnet, mais ces deux pays ne veulent donner aucun commentaire en la matière. Plus tôt cette semaine, le Pentagon (le siège du ministère américain de la défense) a refusé aussi de réagir à l'enquête menée par Kasperksy. Le Vif

Operation AntiSec publishes full client list obtained in Stratfor hack
A hacker operation founded to expose and punish governmental corruption and slimy big business tactics lived up to its word last week, releasing what it claims is a full list of clients who have patronized cyber security advisement firm Stratfor. AntiSec, a global collaboration between Anonymous and upstart hacker group LulzSec, previously released a sliver of data one day after Christmas: 30,000 pieces of personal information for Stratfor customers, including credit card information. Days later, the hacktivists released the whole enchilada. MYCE.com

Japan developing ethical virus in war against cyber crime
Fujitsu is developing a 'seek and destroy' virus for the Japanese government, one that it hopes will identify and combat cyber attacks. This brings new meaning to the phrase – the best defence is a good offence. According to a report by Yomiuri Shimbun, countries such as the U.S. and China have already put similar countermeasures in place. Japan has faced a tough time in online security in the recent past, with numerous cyber attacks in 2011 that crippled everything from local government portals, to the parliament, and Japanese embassies and consulates across the world. The three-year $2.3 million project is still ongoing, and for now, the virus is still in closed environment testing stages. Relevantly, the country would have to make amendments to its laws to allow for the manufacture of the ethical virus, with all virus development still an illegal activity. Think Digit

TDS Enables Koobface Botnet to Earn Bigger Profit
The Koobface botnet, popularly known for using pay-per install and pay-per click mechanisms yearning huge amount for its masterminds has recently been upgraded with a classy traffic direction system (TDS). The TDS controls all the traffic that are related to affiliated websites, reports security researchers at security firm, Trend Micro. The TDS feature forwards the traffic into various other locations and proves to be helpful in gaining hefty amount for the crooks through access into specific sites. With Google going stricter with their creation of botnets that combats creation of fake e-mail accounts by spammers, cyber criminals are taking privilege of Yahoo mail for the accomplishment of their task. SPAMFighter News

Dvorkin, Corey

From: Dvorkin, Corey
Sent: January-03-12 8:25 AM
To: Anderson, Ian; Grigsby, Alexandre; Bradley, Kees; Mohammed, Melanie
Cc: Bonvie, Jeff
Subject: Predictions!

On Dec. 27th, 2011, Rachel King wrote for ZDNet on cybersecurity company McAfee's cyber predictions for 2012. Here are a few of McAfee's predictions:

- There will be an increase in targeted cyberattacks as opposed to general spam e-mails. In this sense, cybercriminals will migrate from broad attempts at ensnaring computer users to targeted "phising" e-mails.
- Hackers will increasingly target mobile devices.
- Cyber-criminals will increasingly target utility systems and use that information to blackmail operators.
- We'll see a proliferation in fake security certificates.
- New hacktivist groups will be created. Interestingly, McAfee feels that the hacker group Anonymous will either disband or reorganize in 2012.

There are many more predictions, and more in-depth analysis. The McAfee predicition report can be found here.

Corey Michael Dvorkin
Acting Director / Directeur par intérim
Cyber Policy / Politiques cyber
National Cyber Security Directorate / Direction générale de la cybersécurité nationale
Public Safety Canada / Sécurité Publique Canada
340 Laurier Avenue West / 340, avenue Laurier Ouest
Ottawa, Ontario, K1A OP8
Tel: (613) 990-9608
corey.dvorkin@ps-sp.gc.ca

Williston, Sandra

From: [redacted]
Sent: January-04-12 3:31 PM
To: 'Darren Sabourin'; [redacted]
Cc: [redacted]
Subject: RE: Fw: Release of Canadian Government and Corporate usernames and passwords

Darren;

Thank you for the explanation and the links.

CCIRC is responsible for receiving the information for notification purposes. We are not limited to ps-sp.gc.ca users.

Once we receive any data, we parse it and split up the "gc.ca" user and provide them to CTEC (Federal Government CERT) for notification. Public Safety is included in this list for CTEC to notify. CCIRC will not notify Public Safety users directly.

However, with the remainder of the Canadian users, CCIRC would like to parse through and locate any Critical Infrastructure we are responsible to notify.

As for who will notify the "Joe Public" user, at this point, CCIRC does not have the resources to do such a large notification. However, Stratfor should be doing this themselves, for all their clients anyway.

Again, thank you for the links. We will grab the FULL list and start CI notifications.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: Darren Sabourin [mailto:Darren.Sabourin@rcmp-grc.gc.ca]
Sent: January-04-12 2:06 PM
To: [redacted]
Cc:
Subject: Fwd: Fw: Release of Canadian Government and Corporate usernames and passwords

The size of the initial email dump has changed significantly.

There are two lists that I am now referring to.

[redacted]

Pages 1298 to / à 1299
are withheld pursuant to sections
sont retenues en vertu des articles

16(1)(a), 16(2)(c), 19(1)

of the Access to Information
de la Loi sur l'accès à l'information

[redacted]

Thank you for any info you can provided.

s.16(2)(c)

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

s.16(1)(a)

Williston, Sandra

From: Darren Sabourin <Darren.Sabourin@rcmp-grc.gc.ca>
Sent: January-04-12 2:06 PM
To: [redacted]
Cc:
Subject: Fwd: Fw: Release of Canadian Government and Corporate usernames and passwords
Attachments: [redacted]

[redacted]

Page 1302

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(a), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

From: [redacted]
Date: Wed, 4 Jan 2012 18:15:56 +0000
To: 'Darren Sabourin'
Cc: [redacted]
Subject: RE: Release of Canadian Government and Corporate usernames and passwords

Hello Darren;

The information you provided below, [redacted] has been processed.

[redacted]

Thank you for any info you can provided.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

Williston, Sandra

From: [redacted]
Sent: January-04-12 1:16 PM
To: 'Darren Sabourin'
Cc: [redacted]
Subject: RE: Release of Canadian Government and Corporate usernames and passwords

Hello Darren;

The information you provided below, [redacted] has been processed.

[redacted]

Thank you for any info you can provided.

s.15(1) - Subv
s.16(1)(a)
s.16(2)(c)
s.19(1)

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"
From: Darren Sabourin [mailto:c[redacted]
Sent: December-26-11 10:47 PM
To: [redacted]
Cc: dave.bachynski@rcmp-grc.gc.ca;[redacted] Tim O'Neil; Tiago Alves de Jesus
Subject: Re: Release of Canadian Government and Corporate usernames and passwords

[redacted]

Page 1305

is withheld pursuant to section

est retenue en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: Moore, Bruce
Sent: January-04-12 9:10 AM
To: [redacted]
Subject: FW: Stratfor Breach s.16(1)(a)
Attachments: ONeil, Timothy.vcf s.16(2)(c)

-----Original Message-----
From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: January-03-12 3:52 PM
To: tim.oneil@rcmp-grc.gc.ca
Subject: Stratfor Breach

YOU ARE BLIND COPIED

[redacted]

Page 1307

is withheld pursuant to section

est retenue en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: Clow, Patrick
Sent: January-04-12 7:42 AM
To: Turbide, Frank; Anderson, Windy
Subject: FW: UPDATE - Stratfor breach

s.16(1)(a)

Some information related to the Stratfor breach. Not sure if this is of any value to us?

From: Scott Foster [mailto:Scott.Foster@rcmp-grc.gc.ca]
Sent: January-03-12 4:13 PM
To: Scott Foster
Subject: UPDATE - Stratfor breach

Good day,

Page 1309

is withheld pursuant to section

est retenue en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: Alain.Labossiere@ic.gc.ca
Sent: January-04-12 11:38 AM
Subject: U2 - N3 - Stratfor Breach

U2 - N3 - Subject: Stratfor Breach

"...
On December 25, 2011, the Anonymous group hacked into a private intelligence agency, Strategic Forecasting Inc. or STRATFOR, based in Austin, Texas. The attack began with the release of STRATFOR's client list announced at https://twitter.com/#!/AnonymousIRC/status/150679351589998593 followed by release of accounts in batches believed to belong to STRATFOR's customers. The release announced in another Twitter post at https://twitter.com/#!/AnonymousIRC/status/150985258999885824 includes emails, passwords (hashed with MD5), home/office addresses and credit card information (full 16-digit number, expiry date and CVV number). The table below is the list of of the leaked accounts with the passwords removed.

STRATFOR has brought down their site following the attack but kept their members posted on the status of the attack via their Facebook page.

For ease of reference try: http://dazzlepod.com/stratfor/

..."

According to this website:

"...

UPDATE (January 2, 2012): We have processed all 860,000 STRATFOR's registered users and added them into the table below. These users do not have their credit card information leaked. The earlier accounts with credit card information leaked are now tagged with "cc" in the table below.

This disclosure was mentioned in PCWorld, Forbes, CNN and TheBlaze.

UPDATE (December 30, 2011): The Anonymous group has just released the remaining accounts making the total of leaked STRATFOR's accounts with credit card information to a total of approx. 75,000. The table below has been updated to include these accounts. Additionally, login information for approx. 860,000 STRATFOR's registered users have been leaked as well but they don't include credit card information; we may update the table below to include these users later.
..."

Williston, Sandra

From: [redacted]@CSE-CST.GC.CA>
Sent: January-05-12 12:10 PM
To: CYBERDO
Cc: CTEC
Subject: RE: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

s.15(1) - Def
s.16(2)(c)

Classification: UNCLASSIFIED

Thanks Sandra... I think!

[redacted]
Cyber Threat Evaluation Centre
[redacted]
ctec@cse-cst.gc.ca

From: [redacted]@ps-sp.gc.ca]
Sent: January 5, 2012 11:08 AM
To: CTEC; CYBERDO
Subject: RE: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

Good Day;

Further to our email from 27 December.

[redacted]

Pages 1312 to / à 1313
are withheld pursuant to section
sont retenues en vertu de l'article

16(2)(c)

of the Access to Information
de la Loi sur l'accès à l'information

Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

s.15(1) - Def
s.16(2)(c)

"Patience isn't a skill — it's a decision"

From: [redacted]@CSE-CST.GC.CA]
Sent: January-04-12 1:31 PM
To: CYBERDO
Cc: CTEC
Subject: RE: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

Hi,

thanks for the email. We did use the file with all email addresses when contacting departments last week, not just the cracked ones and have verified that departments were contacted with regards to all the email addresses in your spreadsheet.

cheers,
[redacted]

[redacted]
GC-CTEC Cyber Duty Officer

From: [redacted]@ps-sp.gc.ca]
Sent: January 4, 2012 1:08 PM
To: CYBERDO; CTEC
Subject: RE: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

Good Afternoon CTEC;

For clarification and possible action.

[redacted]

s.15(1) - Def

s.16(2)(c)

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: [redacted]
Sent: December-27-11 1:14 PM
To: 'CTEC <[redacted]SE-CST.GC.CA> [redacted]CSE-CST.GC.CA)'
Cc: CYBERDO
Subject: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

Greetings GTEC,

We have received a report from a partner that did a research on Stratfor hack mentioned in different news outlet (http://www.cbc.ca/news/world/story/2011/12/25/anonymous-hackers.html). Include are link to pastebin of the post and a compress file(.piz) of a different Anonymous release on Stratfor.

[redacted]

Please acknowledge.

Thanks

Vireak Phlek
Cyber Duty Officer
Public Safety Canada

Cameron, Bud

From: Cameron, Bud
Sent: January-05-12 10:00 AM
To: Hatfield, Adam
Subject: Stratfor Hack

The Anonymous collective hacked into a private intelligence company, Strategic Forecasting Inc. They have begun releasing private info of their clients' accounts with address, credit card, account passwords. The first batch released had [redacted] Being processed for notifications [redacted]
This batch is only about 5 percent of the total; another batch expected today.
Ccirc preparing a note to Robert for SA. [redacted]
Bud

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-05-12 8:44 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; [redacted] Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 5, 2012/ le 5 janvier 2012

Print Media

Government set to 'freeze' spammers
The federal government is preparing to launch a spam reporting centre (SRC) that will crack down on the illegal and annoying calls, texts and email messages that flood Canadians' cellphones, inboxes and social network accounts such as Facebook and Twitter. Private-sector bids closed this week on helping the government establish and operate a facility that observers say is desperately needed to meet international standards and eliminate Canada's reputation as a spammer haven. Industry Canada is developing a division that will be responsible for identifying and analysing trends in spam and related threats to electronic commerce. The government, which has allocated $700,000 annually to operate the facility, believes spam is an increasing threat to the Canadian economy because it can undermine consumer confidence in the online marketplace and erode productivity. Dubbed "The Freezer," the new centre will accept unsolicited electronic messages forwarded by individuals, businesses and organizations in Canada, including spam, malware (malicious software), spyware, short message services (SMS), and false and misleading representations involving the use of any means of telecommunications, says Industry Canada. Ottawa Citizen, A3 (Montreal Gazette, Windsor Star, Calgary Herald, Edmonton Journal, Vancouver Sun, National Post)

Better Business Bureau warns of top 10 scams
Even the Better Business Bureau isn't immune to its top 10 scams of 2011. The group, dedicated to keeping businesses honest, is itself the victim of "brand spoofing," on the Internet also known as "phishing," said president Lynda Pasacreta. Internet fraudsters send BBB clients emails mimicking its logo and directing them to click on a hyperlink to review a customer complaint. That allows the fraudsters access to the companies' confidential online data using spyware, she said. A similar brand-spoof scam masquerading as a Canada Revenue Agency notice of a refund landed in Dianne May-lor's email box Wednesday. It offered her an extra $410 from her revised 2011 tax return, as long as she clicked on a link. The Province, A4

Resolve to keep your computer virus-free
An opinion piece states, "Resolve to stay free of viruses and spyware - Every day, frustrated computer users call about slow systems that are bogged down with pop-up ads, re-directing them on the Internet, generating error messages or preventing booting up. The most common culprits are viruses and spyware or malware. Let me repeat my mantra: Install a free anti-virus and anti-spyware program such as Microsoft Security Essentials, and set it to automatically download and install updates. If you haven't done this yet, make a post-holiday gift of antivirus to your computer. While you're at it, resolve not to open email attachments from unknown senders - even if it most recently came from your sister. Don't click on pop-up ads (especially those professing that your computer is infected) or download programs or files from questionable sources. Trust me: The torrent site from which you're considering a download hasn't vetted the content to confirm that you'd really get a desired video or music file, free of viruses or spyware." Red Deer Advocate, B2

Online Media

Top 10 scams of 2012
The Better Business Bureau has released its list of the top 10 scams of 2012, warning scammers are capitalizing by using false pretences to con consumers. The list is developed jointly by the BBB, Consumer Protection B.C., and the B.C. Crime Prevention Association. CBC News

Cyber attack strands ETrade customers
AUSTRALIA'S second-biggest online broking business, ANZ Bank's ETrade, was forced to shut down over the Christmas-New Year period by a "malicious" cyber attack offshore. The shutdown was prompted by thousands of emails bombarding the broking site, in a denial-of-service attack. It is understood that, as risk assessments were performed on individual countries, access was restored. Access was unavailable from some countries for nearly two weeks. One frustrated customer emailed BusinessDay on December 31, saying that he was trying to prepare a tax return while in the US and Canada and still couldn't access his account. Sydney Morning Herald

Anonymous threatens Sony, spares customers
The loosely organized hacker group known as Anonymous has Sony in its sights once again. After releasing a video a few days ago wherein they threaten to destroy Sony's network, the group, which has been organizing in the IRC channel #OpSony, has clarified the meaning of their declaration. Unlike the infamous PlayStation Network hack of 2011, the target of this attack is not Sony's customers or even the Playstation Network itself, but Sony's executives. As a direct response to Sony's alignment with recent SOPA legislation, Anonymous intends to "dox" (find and expose personal information) about the company's executives. The group has already begun to publicize some private information (including credit card numbers) and plans to continue releasing more and more information in as public a way as possible in the near future. IT World Canada

Japan Fights Virus With Virus
The Japanese government is developing a computer virus to track down the source of a cyber-attack and neutralize it, underscoring the seriousness of the threat. According to a report from The Times of India, software company Fujitsu is reportedly developing the "electronic weapon," a process that has taken three years and $2.3 million, to combat Internet-based threats. The virus works by monitoring for attacks, identifying the source, and closing it down to prevent further programs. Forbes; Branchez-Vous; ZDNet; Huffington Post

Banking Trojans Cover Their Tracks
Virtually all modern viruses, Trojans, and other malware threats exist to make money for their creators. Botnet herders rent out their private armies of infected computers to spew spam. Android Trojans secretly send texts to premium numbers. Possibly the most lucrative, though, are banking Trojans. A banking Trojan like Zeus or SpyEye insinuates itself into the victim's browser and takes control of the online banking experience using what's called a "man in the browser" attack. Security giant Trusteer reports that in 2011 several banking Trojans developed a new type of attack specifically designed to postpone discovery as long as possible. After the actual theft, the Trojan manipulates the victim's view of online transactions, hiding the fraudulent activity. Those who haven't gone paperless will eventually receive evidence in the form of a mailed statement, but by hiding online evidence the criminals have bought extra time in which to complete transactions or siphon off additional funds. PC Magazine; InfoWorld

Sites knocked offline by OpenDNS freeze on Google
Innocent websites were blocked and labelled phishers on Wednesday following an apparent conflict between OpenDNS and Google's Content Delivery Network (CDN). OpenDNS - a popular domain name lookup service* - sparked the outage by blocking access to googleapis.com, Google's treasure trove of useful scripts and apps for web developers. According to reports, a flood of errors hit pages that used Google-hosted jQuery and hundreds of thousands of sites fell over. Visitors to websites were confronted with a message saying: "Phishing site blocked. Phishing is a fraudulent attempt to get you to provide personal information under false pretenses." Other visitors were greeted with a 404 error, aka the dreaded 'file not found' message. The Register

Spam Attacks on Twitter Massive during November 2011: Kaspersky
According to its most recent November 2011 monthly report, Kaspersky Labs states that spammers massively attacked Twitter.com the micro-blogging social networking site during November 2011. Thus, members of Twitter appeared to have hugely spammed invitations asking people to enroll themselves within the social network. Furthermore, Twitter.com was as well used for registering false notifications during November 2011 although in smaller amounts compared to 2010 summer that had an explosion of the said kind of notifications across the Net. Nevertheless, spammers find them popular even now: whenever the web-link is clicked, users get diverted onto a site serving one Viagra ad as well as malware. SPAM Fighter

APWG Reports Data Theft Program Propagation Surge of January-June 2011
The Anti-Phishing Working Group (APWG) recently issued its Phishing Activity Trends Report for H1-2011 i.e. first ½-year of 2011 according to which, certain crimeware's propagation rose during January-June 2011, with malicious programs, designed to steal data climbing to a new infection level as well as remaining stable thereof, so published Marketwatch.com in news on December 25, 2011. Specifically, during H1-2011, there was an over 45% rise in data-stealing programs as well as general PC Trojans from total malware spotted between January 2011 and April 2011. Thereafter, the increase leveled at much more than 40% during H2-2011 i.e. July-December 2011. Previously, the maximum increase in these malware programs was 44% during just one month i.e. August 2010. SPAM Fighter

Smart Grid Security Inadequate, Threats Abound
Near chaos. That's the current state of security for smart grids, according to Pike Research. A recent report by the research firm finds that a lack of security standards, a hodgepodge of products and increasingly aggressive malicious hackers will make 2012 a challenging year for securing smart grids. CIO

Government engineers actively plan for cyberwar
A decade ago, most viruses and worms were unleashed by curious students, pranksters and punks wanting to see what kind of damage they could inflict. That quickly evolved into criminals and thieves writing most of the malware once they realized money could be made. Now, governments have arrived for the party. State-sponsored cyberwar is an increasing concern as more and more nations arm themselves with cyber-weapons. CSO Online

Pentagon Solutions: NDU iCollege team talks Stuxnet, cyber threats
A team from the National Defense University's iCollege, which was recently honored by the the Defense Department's chief information officer for a special cybersecurity workshop, joined Pentagon Solutions. The event hosted more than 200 people from the Pentagon, international defense organizations, industry and academia. The workshop focused on identifying cyber threats, such as the Stuxnet worm, and responding to them. It also highlighted risks to the power grid and other critical infrastructure. Federal News Radio

Will We See More Relatives of Stuxnet in the Near Future?
When the Duqu Trojan made its appearance, many people in the security industry believed it was related to the Stuxnet Trojan. Now, after confirmation from Kaspersky Lab that the same team did, indeed, create both pieces of malware, the question is this: Will we see more Stuxnet relatives in the coming months? The answer is most likely yes. IT Business Edge

Smartphone hacking will rise in 2012, experts warn
Security experts predict 2012 will be a breakthrough year for cyber-attacks on smartphones. There are now enough of these mobile computers in use to make them an inviting target. "Shopping and mobile banking are things that are going to leave a trail and contain lots of goodies that criminals can go after," says Rachel Ratcliff Womack with the digital security firm Stroz Friedberg. MSNBC

Overlapping criminal and state threats pose growing cyber security threat to global Internet commerce, says Open Group speaker
This special BriefingsDirect thought leadership interview comes in conjunction with The Open Group Conference this January in San Francisco. The conference will focus on how IT and enterprise architecture support enterprise transformation. Speakers in conference events will also explore the latest in service oriented architecture (SOA), cloud computing, and security. We're here now with one of the main speakers, Joseph Menn, Cyber Security Correspondent for the Financial Times and author of Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet. ZDNet

A look ahead at healthcare law, privacy and security
Industry experts representing healthcare law, privacy, security, regulatory and data breach were asked to forecast healthcare data trends for 2012. The overall forecast? Protecting patients' protected health information (PHI) should be viewed as a patient safety issue. If the right actions are not taken, experts predict healthcare data breach will reach epidemic proportions this year. Help Net Security

Williston, Sandra

From: [redacted]
Sent: January-05-12 2:01 PM
To: Beaudoin, Luc
Subject: Cyber Events

s.16(2)(c)
s.20(1)(b)

CCIRC Internal Portal - CDO Watch and Operations

Cyber Events - Daily Summary

Modify my alert settings View Cyber Events

Title	Modified	Modified by	
[redacted] **Drone Notifications...**	1/4/2012 2:21 PM	Moore, Bruce	Edited

CE-Number CE12-2559

Status Closed

Summary [redacted] Canada Drone Report: 2012-01-03 notifications to multiple organizations. Hosts within these organizations were communicating with a [redacted] sinkhole server. Infection types included (DNS Changer, Mebroot, or Torpig).

Updates Wed 04/01/2012 12:27 PM
Notifications sent to IT security or technical contacts in the following organizations:
Federal: [redacted]
Provincial: [redacted]
Financial: [redacted]

CI Sector Federal; Provincial; CI - Bank / Finance

Date Closed 1/4/2012 1:55 PM

REF_COL_LOOKUP [redacted] CE12-2559 [redacted] Drone Notifications - Multiple Organizations]

Possible compromised .ca TLDs	1/5/2012 8:09 AM	Pitcher Robert	Edited

Status Closed

Updates [redacted]
CCIRC processing these notifications through our regular channels.

Closing event.

Possible compromised website ser... 1/5/2012 9:15 AM Moore, Bruce **New!**

CE-Number	CE12-nnnn
Status	Active
Title	Possible compromised website serving malware [redacted]
CCIRC Handler	Moore, Bruce
Take-down	Yes
Notification	No
Reporting Organization	SpyEye Tracker
Summary	
Updates	
Incident Type	Cat 3 - MALICIOUS CODE / COMPROMISE
CI Sector	Other industries
Severity	Normal
Impact	Degradation / disruption
Primary Contact	
Related Incidents	
_NOT_USED_Secondary Contact	
_NOT_USED_IATFF Category	Event
_NOT_USED_Primary Event	No
_NOT_USED_Assigned To	
_NOT_USED_Priority	(2) Normal
_NOT_USED_Category	(2) Category2
_NOT_USED_Due Date	1/5/2012 10:00 AM
REF_COL_LOOKUP	CE12-nnnn [Possible compromised website serving malware [redacted]

s.16(2)(c)

Stratfor Hack affected Canadians 1/5/2012 10:42 AM Williston, Sandra Edited

Updates

[redacted]

Pages 1322 to / à 1324
are withheld pursuant to section
sont retenues en vertu de l'article

16(2)(c)

of the Access to Information
de la Loi sur l'accès à l'information

January 5

UNCLASSIFIED

DATE:

File No.: 384942
RDIMS No.: 541243

MEMORANDUM FOR THE DIRECTOR GENERAL

CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

(Information only)

ISSUE

Thirty four Federal Government workers and an unknown number of Provincial, Municipal, and Critical Infrastructure users have been affected by the hacking of a private international intelligence agency.

BACKGROUND

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

CONSIDERATIONS

There are financial, workplace security, and privacy considerations regarding this incident.

First, there is a financial risk to all impacted individuals as the credit card information posted online contained the full 16 digit number, expiry date, and Card Verification Value number (i.e. everything needed to make purchases).

Second, compromised individuals could be victims of specific and targeted attacks, such as malicious emails, social engineering, and attempts to compromise workplace security.

Third, impacted individuals privacy could be compromised as work/ home telephone numbers and work/home addresses were released. Given the fact that 860,000 login credentials have been compromised, there is also a strong likelihood that additional downstream privacy risks exist for impacted individuals as a significant percentage of the population uses the same password for many internet sites and work.

NEXT STEPS

There are three main actions CCIRC is taking to address this situation.

First, CCIRC is working with RCMP to identify Federal Government users registered with STRATFOR. Identified users will be notified through CTEC.

Second, CCIRC is performing further analysis in order to identify and notify any Provincial, Municipal and Critical Infrastructure users who have been affected.

Third, CCIRC plans to recommend that affected users change all internet account passwords that use elements from their compromised password; monitor their credit card transactions and; contact their bank regarding the credit card breach.

We will inform you of any significant developments. Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, CCIRC
National Cyber Security

Prepared by: Nate Klassen
Sandra Williston

Page 1327

is a duplicate

est un duplicata

Page 1328

is a duplicate

est un duplicata

Page 1329

is a duplicate

est un duplicata

Page 1330

is a duplicate

est un duplicata

Page 1331

is a duplicate

est un duplicata

Page 1332

is a duplicate

est un duplicata

Key Ethical and Legal Trends in the Next Decade and Implications for Cyber Security Policy

Draft - Not for Distribution

David Fewer

5 January, 2012

Table of Contents

Executive Summary

Analysis

Issue #! - The Decline of Privacy

Issue #2 - Hacktivism

Issue #3 - The Surveilled State

Issue #4 - The Hacktivist State

Conclusions and Recommendations

Introduction

The dispersal of technological innovation throughout the publicly available communications infrastructure is changing the way individuals interact.

As communications tools move onto the internet, they are becoming social, meaning they are interactive. Participants do not simply receive information, but dynamically volunteer information themselves. These tools are networked, dynamic and evolutionary. Social interactions on them may be publicly available or protected from public view in some way, and may involve a single voice in the dark or a virtual mob. Social networks such as Facebook and Twitter are obvious examples of social communications media, but even older information communications formats, such as newspapers, as they move onto the internet offer new means of interacting with readers. These range from permitting readers to post comments to news stories to promoting the live interaction of "readers" with online journalists or interview subjects.

Communications tools are becoming increasingly mobile, as well. Divisions between communications categories are crumbling: telephony and broadcast no longer make good definitions for categories of communications; internet and proprietary networks are overlapping. All of the tools available over the internet are being made available over networks that have historically borne much greater control than the internet. The regulability of these private networks has implications for security policy.

Communications media are also fractured today like never before. Consider telephony: in the past, a single network ensured regulability from a public safety perspective. The introduction of mobile networks complicated that picture, but the inherent regulability of these networks was not compromised. Today, the internet has introduced new tools and formats for voice communications, and the potential for participants to use encryption further complicates the regulability of communications. Expand the range of communications to include text exchanges and one gets a sense of the challenge facing public safety officials.

Finally, these innovations in communications technologies has permitted a greater range of instant, real-time communications. Text now enjoys the same immediacy as voice communications. However, many of these technologies also introduce persistence to what may be considered a real-time exchange. Text messages, for example, may replace a vocal conversation but stay on the network for later review.

These disruptive innovations pose challenges to the abilities of those charged with ensuring public safety to do their jobs. The potential responses to these challenges raise, in turn, challenges to both ethical and legal rules governing the conduct of public safety officers. This report explores key ethical and legal trends over the next decade and considers the implications of these trends for cyber security policy.

This Report considers both ethical and legal trends in relation to cyber security policy. This mandate merits some discussion. First, the context limits the Report's exploration of trends. Although one might fully expect the adoption of alternative energy sources to be a dominant ethical and legal trend over the next decade, it is one which is unlikely to have implications for cyber security policy and so receives no consideration in this Report. The Report examines

cyber security, and so focuses on ethical and legal trends in *cyber* space - communications media and tools.

Second, "ethical trends" refer to the evolution of those norms governing the conduct of those charged with ensuring the safety of the Canadian public. "Norms" in this sense embraces the collective understanding of acceptable behaviour that act to both guide and restrain behaviour. Laws may reflect norms; theft, for example, is a violation of both the *Criminal Code* and our common understanding of acceptable behaviour. But not all norms find an equivalent in our laws. Plagiarism, for example, violates many rules of social interaction but finds no equivalent in the laws of Canada.

Third, "legal trends" refer to the evolution of the rule of law and its enforcement. The "rule of law" refers to the principle that governance occurs through adherence to known principles. Law enforcement agents act pursuant to lawful authority: what they enforce are laws, not policies or arbitrary decisions. Their exercise of authority is also derived from law: their powers of action are again derived from law, and not arbitrary. Institutions of democratic governance provide authority for both the law enforced and the powers of action permitting its enforcement.

Cyber security policy is ordinarily conceived of as the realm of public officers, but in practice the execution of those policies requires significant co-operation amongst public and private entities. For this reason, this Report's examination of ethical and legal developments will consider developments for both public and private actors. What happens in the marketplace may have a significant impact on individual action. In this sense, private actors - businesses - may act as a regulator of individual behaviour. This may accordingly have implications for cyber security policy.

Any exercise in prognostication is necessarily an exercise in guesswork. However, that guesswork can be guided by making reasoned assumptions.

First, this Report proceeds on the assumption that developments in technology and the safeguarding of the public over the next decade will have their roots in present developments. This Introductory section began with a discussion of the recent evolution of communications technologies, and offered the thesis that modern communications media and tools are becoming increasingly social, mobile, fractured and instant. The Report assumes this trend will continue.

Second, this Report assumes that the public response to the the tragedy of 9/11 will be generational, and not simply political. In other words, the Report proceeds with the view that the response of governance institutions to 9/11 has fundamentally changed the way those institutions approach security and the trade-offs involved. This approach has profound implications for privacy and other civil liberties, and potentially challenges principles that lie at the root of democratic states.

Finally, the Report assumes that no catastrophic, unforeseeable event disrupts global society over the next decade. A report drafted in the year 2000 prognosticating on the future of security

policy in the first decade of the twenty-first century would have been reduced by 9/11 a year later to the status of a historical curiosity. Similarly, scandal, gross abuse of power, or public outrage over a glaring usurpation of democratic institutions could result in the scaling back of powers enjoyed by law enforcement agents. These sorts of events are always possible, but by nature not amenable to prediction.

In Part I, the Report describes the methodology employed in its development. In Part II, the Report turns to considering likely key ethical and legal trends over the next decade and their implications for cyber security policy. The Report focuses on the following four key trends:

> (1) **The Decline of Privacy** - The next decade will see a steady erosion in both the degree of privacy enjoyed by individuals in the marketplace and the willingness of regulators to take firm action to limit the ability of market participants to intrude on the privacy of individuals.
> (2) **Hacktivism** - Individuals are willing to act collectively to use use online communications tools and privacy enhancing technologies to engage in "extra-legal" activism - policy-directed action that may violate the law. Hailed as online civil disobedience or damned as terrorism, the phenomena will continue.
> (3) **The Surveilled State** - Law enforcement agents will enjoy unprecedented powers to surveill ordinary citizens and subjects both within and without their borders.
> (4) **The Hacktivist State** - Mirroring Hactivism, state agents will enjoy aggressive new powers to investigate and disrupt threats to cyber security.

For each of these key trends, the Report offers a description of the trend, identifies the drivers behind the trend, and considers its Implications for cyber security policy. Part III concludes this Report with recommendations for government action in light of these trends.

Part I - Methodology

Crafting this paper involved undertaking significant research. Our research will embraced three streams:

- Academic Literature Survey: We conducted a traditional survey of academic periodicals and other secondary literature, making use of both legal and social science databases and search tools.
- Public Source Survey: In the area of computer and online security, much of the most innovative writing and thinking occurs in non-traditional venues, such as blogs; websites of civil society organizations; publications of security researchers, research firms and consulting firms; online publications not otherwise indexed by academic periodical indexes; and, of course, government publications. We conducted a thorough online search of these sources.
- Primary Source Research – Interviews: We interviewed a half dozen or so individuals known to us to be involved in thinking about technological security, threat detection and harm prevention, including:
    - David McMahon, Bell Canada, National Security and Complex Programs;

- Bill St. Arnaud – former Chief Research Officer for CANARIE Inc., Canada's Advanced Internet Development Organization;
- Professor Ron Diebert, Director of the Citizen Lab, Monk School of Busness, University of Toronto;
- members of the Software Security Research Group, a collaborative project between SITE (the School of Information Technology and Engineering) at the University of Ottawa and IBM;
- Google Engineering – individuals at Google provided their time and thoughts on some of the
- Security firm contacts – We will reach out to contacts at businesses involved in selling security solutions to consider their perspectives. Targeted firms include Sophos (Vancouver) Blue Coat (Ottawa) and Symantec (Cupertino).

Our initial research centred around technological phenomena reshaping the ways we communicate today. These include:

- "Cloud Computing";
- The mobile network;
- "Social Media" and security;
- the industrialization of malware production (the economic basis for online
- crime); and
- "Hacktivism".

Finally, we posed questions to individuals at Public Safety to gain an understanding of their perspectives, and their expectations with respect to this Report.

Part II - Analysis

The second decade of the twenty-first century has seen the emergence of a number of online phenomena, and the continuation of many phenomena originating in the previous decade. These are, to a significant extent, driven by the disruptive technological innovations canvassed in the Introduction of this Report: social media, fractured communications streams, mobile networks, and real-time exchanges. They are also global phenomena: the innovative use of communications technologies that facilitated the Arab spring has also helped differentiate the Occupy movement from previous protest movements in North America.

This Report has focused on the following four key emerging or continuing ethical and legal trends:

(1) **The Decline of Privacy** - The next decade will see a continuing diminishment of the privacy enjoyed by individuals.
(2) **Hacktivism** - Online activism will continue to explore the grey areas at the borders of lawful activity, and the forbidden areas beyond the law.
(3) **The Surveilled State** - States will move closer to the model of citizen oversight exercised by China than that espoused in the past by Western states.
(4) **The Hacktivist State** - States will begin enacting laws legitimizing the State's authorization of the kinds of tactics employed by Hacktivists against them.

The first two of these trends focus largely on developments in the private sphere, rather than the public sphere, but which have obvious implications for cyber security. The final two trends more directly involve the exercise of public power but, interestingly, potentially implicate private actors acting as state agents. An overarching theme, common to all of these trends, is the increasing interdependence of public and private agents in securing public safety online.

Some might characterize this list as overly pessimistic, and taking a dim view of civil liberties' prospects in the coming decade. Certainly, that is one facet of these trends. However, with accountability, realistic safeguards against abuse, enshrined instiutional balances, and when derived from lawful authority, expanded state powers may be consistent with liberty and democratic values. Moreover, expanded state powers can do a world of good when directed against real threats to liberty, democracy, and economic values.

Issue #1: The Decline of Privacy

(a) Description

The first decade of the twenty-first decade has seen the sphere of privacy enjoyed by individuals shrink. This has predominantly occurred online through the development of an infrastructure of commercial surveillance. Social networking services such as Facebook have developed sophisticated infrastructures to mine the personal data of site users. Regulators have blessed these activities provided the service is transparent about its practices. The transparency requirement is met so long as the service discloses its practices, even ex post, somewhere on its service. In this way, "transparency" is replacing consent as the mechanism for evading liability for invasion of privacy, and contractual standards of exchange are replacing knowledge as the standard for consent. The end result is that individuals currently enjoy a sphere of personal privacy greatly diminished from that enjoyed a decade ago.

The next decade will see continued erosion of both the sphere of privacy enjoyed by individuals in the marketplace and a willingness of regulators to limit the ability of commercial actors to intrude on the privacy of individuals. The legal model describe above for obtaining the right to collect, use and exchange the personal information of individuals is expanding out from social networks to mobile networks and even use of internet-based devices such as the iPad. The coming decade will see continued expansion of the reach of the information network into an ever-expanding range of devices: from smart-phones and smart-metres today to smart energy devices tomorrow to even networked automobiles tomorrow. Each of these devices will collect, use and exchange the personal information of users and individuals interacting with those users. The proprietors of those devices will similarly employ contracts and notices to evade restrictions on the manner in which it may deal with that personal information.

(b) Drivers

The decline of privacy may be laid at the feet of three predominant drivers: technology, the marketplace, and the regulatory regime overlying privacy laws.

From a technological perspective, the emergence of tools and services that permit effective surveillance of users has permitted this system to evolve. However, these tools have been around for some time. What is different today is the emergence of a marketplace willing to use these tools. Finally, the development of a legal framework amenable to this market structure has enabled the phenomenon. This legal framework has its origins in two camps: one American, the other Canadian. First the absence in the United States of dedicated privacy protection laws means that privacy interests may be dealt with in that jurisdiction on a liability rules basis: under the US framework, fraud, misrepresentation, and unfair trade practices trigger liability, not an absence of consent. Second, Canada's comprehensive private sector personal information protection legislation, PIPEDA, has been interpreted to adhere effectively to the American standard of privacy protection. Globally, other privacy regulators have not departed markedly from the lead set by Canadian privacy regulators.

(c) Implications

Privacy is not dead, contrary to some assertions. It is, however, a greatly reduced impediment to the collection, use and disclosure of personal information by private actors. This replacement of consent with transparency as the tool for evading liability for dealing with personal information has significant benefits for public agents such as law enforcement and public security agencies.

First, individual privacy rights may pose a potential barrier to private actors in securing the viability of their own infrastructure. For example, objectives of public safety include securing critical infrastructure such as communications facilities and public internet infrastructure. Most agreements among service providers and their customers will include sweeping consents to ensuring infrastructure integrity and responding to security threats.

Second, law enforcement and security agencies routinely engage in public-private partnerships in furtherance of general public safety. Simply, public agencies lack the expertise oversee the operation of private networks and services. Similarly, private actors lack the expertise (and lawful mandate) to address security concerns arising from use of their services and facilities. Co-operation between public and private actors has grown common. While it is possible for laws to address the liability concerns of both participants to these partnerships, it can be simpler to deal with individual privacy claims contractually. Consent can address a number of risks law enforcement may encounter in collecting and using evidence in court: why bother with a warrant when the user has already clicked "OK" to disclosures to law enforcement requests?

Issue #2: Hacktivism

(a) Description

Individuals are willing to act collectively to use use online communications tools and privacy enhancing technologies to engage in "extra-legal" activism - policy-directed action that may violate the law. Hailed as online civil disobedience or damned as terrorism, the phenomena will continue over the coming year.

Hacktivism was not born with the Wikileaks-cablegate controversy of 2010, nor did it first achieve political signficance with the Arab Spring of 2011. However, Hacktivism did occupy the global spotlight with the consecutive development of these events. Today, we may describe "Hacktivism" as politically motivated digital disruption of specific targets. While some Hacktivist

groups operate under a brand (such as "Anonymous" and "LulzSec"), in practice Hacktivism is a leaderless, geographically dispersed and socio-economically diverse phenomenon.

We must distinguish politically motivated attacks from hackers and "script kiddies" motivated by entertainment or the "challenge" of overcoming the defenses of a formidable online presence. Hacktivism, in contrast, is motivated by political objectives and generally involves a collective of like-minded participants. This implies no formal organization but simply an agreement to work on a common objective.

We should also recognize that Hacktivism does not exclusively employ illegal tactics such as breaching security and engaging in denial of service attacks. Hacktivism also employs legal tools of protest. Civil protest is inevitably moving online.

(b) Drivers

The emergence of Hacktivism has been driven by technology and, this Report argues, by a normative response to public-private security and law enforcement partnerships.

From a technological perspective, the primary tools of Hacktivism remain data breach and denial of service attacks. These have proven effective tools: once selected, a target is inevitably compromised. Organizational tools involve commonplace online communications vehicles such as image boards, Internet Relay Chat and private servers. Hacktivists also make ample use of privacy-enhancing technologies, using encryption and onion routing to cover traces of their activities. These are not new techologies. Indeed, hacking collectives are not themselves new phenomena. What is new is the politically motivated co-ordintated deployment of these web service disruption tools against select targets.

The cause of this is arguably normative: commercial actors have been perceived to be in alliance with law enforcement and in so doing have arguably broken a norm of neutrality: commercial actors do not co-operate with law enforcement against the interests of customers who are not alleged to have broken any laws. The cardinal example of this remains the reaction of Anonymous to the cessation of payments by financial intermediaries to Wikileaks in response to the publication by Wikileaks of American diplomatic cables in 2010. In disrupting the websites of these intermediaries, Anonymous sent a message that these actors were violating norms of acceptable behaviour.

(c) Implications

The continuing exploits of Hacktivist groups will have significant ongoing implications for cyber security policy.

First, Hacktivism opposes the private half of public-private partnerships directed towards politically ambigous or controversial investigations or operations. Private actors acting as state agents invite attack. This may in turn compromise law enforcement or public safety strategies.

Second, public institutions may find themselves targets of Hacktivist attacks. While this it is common for government agencies to find theselves targets of security breach attempts, Hacktivist attacks are different in kind. They do not seek to remain quiet or undiscovered; quite

the reverse, Hacktivism seeks publicity. The point is not to go undetected, but to make news. To the extent that such attacks target public infrastructure, they raise additional public safety concerns.

Finally, individuals are now vulnerable to politically-motivated attacks. Such attacks need not violate any laws: scraping publicly available data off websites such as Facebook may violate no laws but still achieve the objectives of the Hactivist: to influence the future action of the target, and to influence public opinion on the target.

Issue #3: The Surveilled State

(a) Description

The coming decade will see Canadian law enforcement agents obtain unprecedented powers to surveill ordinary citizens and subjects both within and without their borders. This has been a devlopment long in coming: ever since Canada signed the Cybercrime Convenion, Canadian law enforcement agencies have sought expanded powers to investigate, gather evidence, and intercept digital communications. A number of previous attempts to modify Canadian laws governing law enforcement access to private information have failed to pass into law, due both to the controversial nature of those laws and the vagaries of Canadian electoral politics. With the current majority government's commitment to a "law and order" ideology, those barriers appear certain to be overcome in the near future.

Nor will that expanded surveillance agenda be satisfied with the passage of the current lawful access proposals. A second wave of expanded law enforcement powers will come with the obligations attached to further international instruments, most notably those implicated in current discussions involving the Perimeter Agreement with the United States. Finally, as discussed in the previous section, informal public-private partnerships are serving to greatly expand the state's reach into the personal information of Canadians in a manner completely outside the scope of legislation governing public surveillance powers.

Canada one decade from now will be a comprehensively serveilled state. Privacy will arise as a by-product of staying offline - increasingly difficult to do in a world in which even common household items are online - or by taking extra-ordinary steps to utilize privacy enhancing technologies to maintain privacy.

(b) Drivers

The drivers behind the emergence of the surveillance state are largely technological and normative, and enabled by the emergence of a marketplace able to navigate away from liability for privacy invasion.

From a technological perspective, the tools of widespread public surveillance are only recently evolved. It has simply been a question of storage, processing power, and network architecture. From a normative perspective, the tragedy of 9/11 has provided security agencies with motivation to push an unprecedented security agenda. It is clear, as American Secretary of State Hilary Clinton asserts, that security trumps the economy in a hierarchy of public policy

priorities; however, it is even clearer that security trumps privacy in any contest between the two. This agenda has been abetted by marketplace developments placing private actors - such as online service providers and network access merchants - as custodians of access to personal information of their customers. Those developments have placed these private actors in the perfect position to act as agents of the state in surveillance operations.

(c) Implications

The emergence of the surveillance state will have profound effects on civil liberties, dramatically weakening the rights individual citizens enjoy. This will potentially provide a series of crises.

First, expanded state powers of investigation will foreseably raise the potential for abuse of those powers. Civil libertarian challenges to the expansion of law enforcement powers call for checks, balances, and oversight in the use of these powers. The challenge for proponents of expanded state powers is to see the imposition of these checks and balances as necessary safeguards rather than meddlesome irritants to the use of those powers. This sets aside, of course, fundamental questions about the need for expanded state powers to begin with, or the question of whether these powers should aim for the outer limits of constitutional authority or more conservatively for standards already settled by law as well within constitutional limits.

Second, and more fundamentally, ubiquitous state surveillance may amount to a rechacterization of what it means to live in a liberal democracy. Traditionally, we have defined the difference between authoritarian states and Canada as comprising both liberty and democracy. We have long regarded privacy as inherent to liberty. Ubiquitous state surveillance challenges that regard. Is liberty no more than the freedom to shop under the watchful eye of the state? If so, is the only real difference between authoritarian regimes and Canada that Canadians elect their government? And if so, ubiquitous state surveillance promises a crisis of democracy itself.

Or is this concern simply alarmist? After all, Canadians only enjoy constitutional protection against unreasonable search and seizure by the Canadian government. We enjoy much more limited protections against the surveillance activities of foreign governments, including the United States. Online communications take no heed of borders. Indeed, emails from one part of Canada to another are liable, even likely, to be routed through borders to the United States and beyond.

Issue #4: The Hacktivist State

(a) Description

Mirroring Hactivism, state agents will enjoy aggressive new powers to investigate and disrupt threats to cyber security. States will begin enacting laws legitimizing the State's authorization of the kinds of tactics employed by Hacktivists against them, and going beyond, to disrupt the manner in which the internet itself facilitates communications with target sites. In its simplest form this may include state authorization of security firms to destroy botnets distributed on the personal computers of individuals. More complex remedies interfere with the functioning of the internet itself.

The internet has long been regarded by civil libertarians as inviolate: disrupt the bedstone principles upon which the internet was built and you will threaten the media's potential as a generator of innovation and economic growth. The next decade will see the creation of new law enforcement powers that challenge this assumption. States will start to enact laws that violate principles that the internet was built upon, such as the end-to-end principle, and disrupting the rules that govern internet addressing: why build a case against a target when the root can be re-written to elimate the target from the net entirely?

We can already see the earliest forms of these powers in, of all things, the advocacy of the American government in the service of the entertainment industry. First, the U.S. Immigration and Customs Enforcement agency ("ICE"), an agency of the United States Department of Homeland Security, has taken exceptional steps to address allegations of copyright infringement. On the basis of unproven allegations of infringement supported by untested evidence, ICE has seized domain names registered to third parties, replacing the internet sites with a notice of seizure.

This remedy is being touted as the centrepiece of legislation currently before Congress, the House bill, *Stop Online Piracy Act*, H.R. 3261, and its Senate counterpart, the *PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property) of 2011*, U.S. Senate Bill S.968. The remarkable nature of these remedies should be clear: they propose treatment of speech akin to that afforded in Canada to unambigous cases of online child pornography imagery. Globally, it is a remedy akin to the kind of consorship practiced in authoritarian regimes. If accepted in the context of intellectual property rights enforcement, we can expect the remedy to spread both to other areas of private rights - defamation, trade-mark infringement, etc. - and to areas of public concern, including security and law enforcement.

(b) Drivers

The phenomena of aggressive remedial action to security threats - and, apparently, to the merely commercial interests of intellectual property owners in the United States - is not based on the recent emergence of technology. The ability to seize domain names has long existed by not used. Rather, these seem based on market interests and the normative position of regulators supporting those commercial interests.

(c) Implications

The emergence of robust remedies for addressing security concerns - of both the informational integrity and economic variety - are significant.

First, state-sponsored Hacktivism runs the risk of provoking indeterminate liability. State actors - whether law enforcement or private actors acting as state agents - must be secure in the knowledge that their intervention is based on accurate information, targeted solely at bad actors, and will not harm innocent parties. Failure of any of these conditions may result in liability. Accordingly, there will be pressure brought for legislative "cover" for these kinds of activities. Advocates will demand that such laws ought to provide authorization of the remedy (extending

to any private parties acting as state agents), and that the laws provide immunity from prosecution or lawsuits within "safe harbours" of activity (a "responsible intervention" defense).

Second, more aggressive remedies involving domain name seizures will provoke a stronger reaction amongst civil libertarians and, potentially, others. At its root, domain seizures challenge the globe's trust and confidence in the United States as custodian of the internet. American authorities control "the root" - the domain name system that underlies all communications over the internet. Locally, national domains are potentially subject to the same sorts of remedies: the Canadian government could conceivably pass laws compelling CIRA, the Canadian Internet Registry Authority, to pull the plug on targeted domain names. To address these fears, states may take measures to protect national firms against the threat of irresponsible domain stewardship. This raises the spectre of a balkanized internet.

From an economic perspective, suspicion of governmental power over the internet may undermine trust and confidence in the internet as a vehicle of communications and commerce. This is turn may undermine innovation on the 'net. To the extent that cyber security policy promotes the economic potential of the internet for securing Canada's well-being, these dramatic new remedies pose as many potential problems as solutions.

Part III - Conclusions and Recommendations

Bibliography

Klassen, Nathan

From: Williston, Sandra
Sent: January-05-12 9:42 AM
To: Klassen, Nathan
Subject: RE: Briefing note for RD -- can you prepare a routing slip and file number

Hackers attack US security think tank Stratfor, promise more targets for Christmas
Associated Press (APR)
Cassandra Vinograd
Dec 25 08:04

LONDON _ Hackers on Sunday claimed to have stolen 200 GB of emails and credit card data from United States security think-tank Stratfor, promising a weeklong Christmas-inspired assault on a long list of targets.
Members of the loose hacking movement known as ``Anonymous'' posted a link on Twitter to what it said was Stratfor's secret client list _ including the U.S. Army, the U.S. Air Force, Goldman Sachs and MF Global.
``Not so private and secret anymore?,'' the group taunted in a message on the microblogging site.
Anonymous said it was able to get credit details, in part, because Stratfor didn't bother encrypting them _ an easy-to-avoid blunder which _ if true _ would be a major embarrassment for any security company.
Stratfor said in an email to members that it had suspended its servers and email after learning that its website had been hacked.
``We have reason to believe that the names of our corporate subscribers have been posted on other websites,'' said the email, passed on to The Associated Press. ``We are diligently investigating the extent to which subscriber information may have been obtained.''
The email, signed by Stratfor Chief Executive George Friedman, said the company is ``working closely with law enforcement to identify who is behind the breach.''
``Stratfor's relationship with its members and, in particular, the confidentiality of their subscriber information, are very important to Stratfor and me,'' Friedman wrote.
Stratfor's website was down midday Sunday, with a banner saying ``site is currently undergoing maintenance.''
Wishing everyone a ``Merry LulzXMas'' _ a reference to spinoff and fellow troublemakers Lulz Security _ Anonymous also posted a link on Twitter to a site containing the email, phone number and credit number of a U.S. Homeland Security employee.
The employee, Cody Sultenfuss, said he had no warning before his details were posted.
``They took money I did not have,'' he told The Associated Press in an email. ``I think why me? I am not rich.''
Anonymous warned it has ``enough targets lined up to extend the fun fun fun of LulzXmas through the entire next week.''
The group has previously claimed responsibility for attacks on companies such as Visa, MasterCard and PayPal, as well as others in the music industry and the Church of Scientology.

On December 25, 2011, the Anonymous group hacked into a private intelligence agency, Strategic Forecasting Inc. or STRATFOR, based in Austin, Texas.

The attack began with the release of STRATFOR's client list announced at https://twitter.com/#!/AnonymousIRC/status/150679351589998593 followed by release of accounts in batches believed to belong to STRATFOR's customers.

The release announced in another Twitter post at https://twitter.com/#!/AnonymousIRC/status/150985258999885824 includes emails, passwords (hashed with MD5), home/office addresses and credit card information (full 16-digit number, expiry date and CVV number).

STRATFOR has brought down their site following the attack but kept their members posted on the status of the attack via their Facebook page.

UPDATE (December 30, 2011): The Anonymous group has just released the remaining accounts making the total of leaked STRATFOR's accounts with credit card information to a total of approx. 75,000.

Additionally, login information for approx. 860,000 STRATFOR's registered users have been leaked as well but they don't include credit card information.

CCIRC is working with LE to identify Federal Government users who registered with the site. To date, 34 gc.ca users were identified and notified through CTEC (Federal Government CERT). Further analysis is being performed to identify and notify any Provincial, Municipal and Critical Infrastructure users who have been affected.

CCIRC's recommendation users should be advised to change the password of all other accounts, (business or personal on the Internet), that use elements from the compromised password.

Also, to contact their bank regarding the possible breach of their credit card and to monitor for any unusual transactions on the card.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: Klassen, Nathan
Sent: January-05-12 9:32 AM
To: St-Louis, Danielle
Cc: Williston, Sandra
Subject: Briefing note for RD -- can you prepare a routing slip and file number

Hi Danielle,

Can you prepare a routing slip and file number WRT a brief Sandra and I are preparing for RD? Please ensure AH also gets a copy.

Title = **CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY**

RDIMS =541243

Cheers,

Nate

P.S. Since Bud is no longer here the routing slip will probably go from us to Windy.

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

Williston, Sandra

From: Timothy O'Neil <tim.oneil@rcmp-grc.gc.ca>
Sent: January-06-12 11:57 AM
To: CYBERDO
Cc: Anderson, Windy; Angus Smith; Anna Gray-Henschel; Darren Sabourin; David Hubley; Debora at Work; Dominic Lafleur; [redacted] Victor Munro
Subject: RE: FW: Stratfor Breach
Attachments: ONeil, Timothy.vcf

Will do and thanks for the follow up.

s.13(1)(a)
s.16(2)(c)
s.19(1)

For my RCMP colleagues please note CCIRC response to the Stratfor breach.

Kindly ensure this message is shared with your RCMP colleagues.

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
[redacted]

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> [redacted] 2012-01-06 11:52 >>>

[redacted]

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

s.16(1)(a)
s.16(2)(c)

From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: January-06-12 11:31 AM
To: [redacted]
Cc: Anderson, Windy; Darren Sabourin; [redacted] Victor Munro
Subject: Re: FW: Stratfor Breach

s.16(1)(a)
s.16(2)(c)
s.19(1)

Thanks Sandra

Just so you are aware, my email account was identified on the Stratfor breach and I have not heard anything from anyone on this. So who should I, and for that matter, my RCMP colleagues have heard from within the GoC on this issue?
Thanks.....Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
[redacted]

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> [redacted] 2012-01-06 11:24 >>>
Good Day;

[redacted]

Hope this helps.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

From: Anderson, Windy
Sent: January-06-12 9:17 AM
To: [redacted]

Subject: FW: Stratfor Breach

Can someone get back to Tim about what we are doing on this?
Have a great day,

s.16(2)(c)
s.19(1)

Windy
Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada
From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: January-06-12 9:04 AM
To: Angus Smith; Bruce Rae; Darren Sabourin; [redacted]
Cc: Anderson, Windy; John (CI) SUTHERLAND; tiago.dejesus@rcmp-grc.gc.ca; Victor Munro
Subject: Re: Stratfor Breach

Thank you [redacted] and Angus for sharing.

This type of messaging will probably occur more frequently.

By means of this message I am providing to [redacted] for his assessment.

Darren - do you have the means to check out the noted websites, and provide an assessment for this obviously bogus message.

I am aiming to provide an updated assessment to our stakeholders so they should be aware as to how to handle these types of messages.

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
[redacted]

>>> [redacted] 2012-01-06 08:40 >>>

[redacted]

s.16(1)(a)
s.19(1)

s.16(2)(c)
s.19(1)

Williston, Sandra

From: [redacted]
Sent: January-06-12 11:52 AM
To: 'Timothy O'Neil'; [redacted]
Cc: Anderson, Windy; Darren Sabourin; [redacted] Victor Munro
Subject: RE: FW: Stratfor Breach

[redacted]

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: January-06-12 11:31 AM
To: [redacted]
Cc: Anderson, Windy; Darren Sabourin; [redacted] Victor Munro
Subject: Re: FW: Stratfor Breach

Thanks Sandra

Just so you are aware, my email account was identified on the Stratfor breach and I have not heard anything from anyone on this. So who should I, and for that matter, my RCMP colleagues have heard from within the GoC on this issue?
Thanks.....Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
[redacted]

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> [redacted] 2012-01-06 11:24 >>>
Good Day;

[redacted]

Hope this helps.

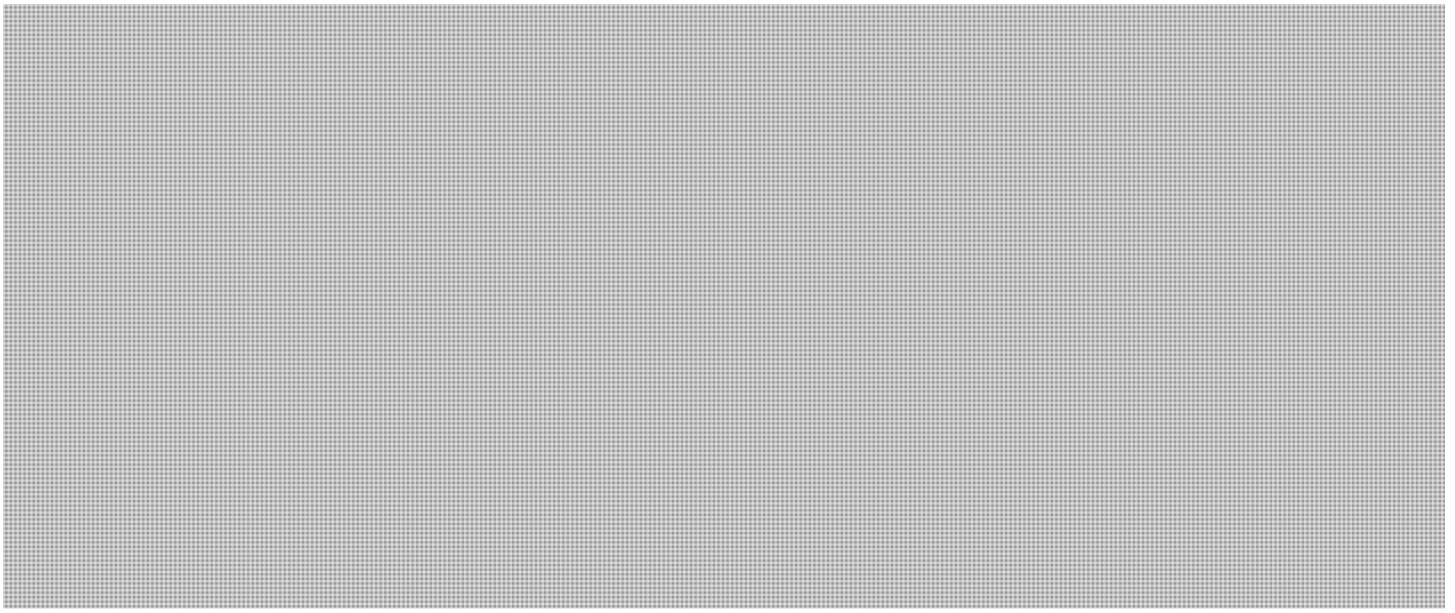
Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

From: Anderson, Windy
Sent: January-06-12 9:17 AM
To: [redacted]
Subject: FW: Stratfor Breach

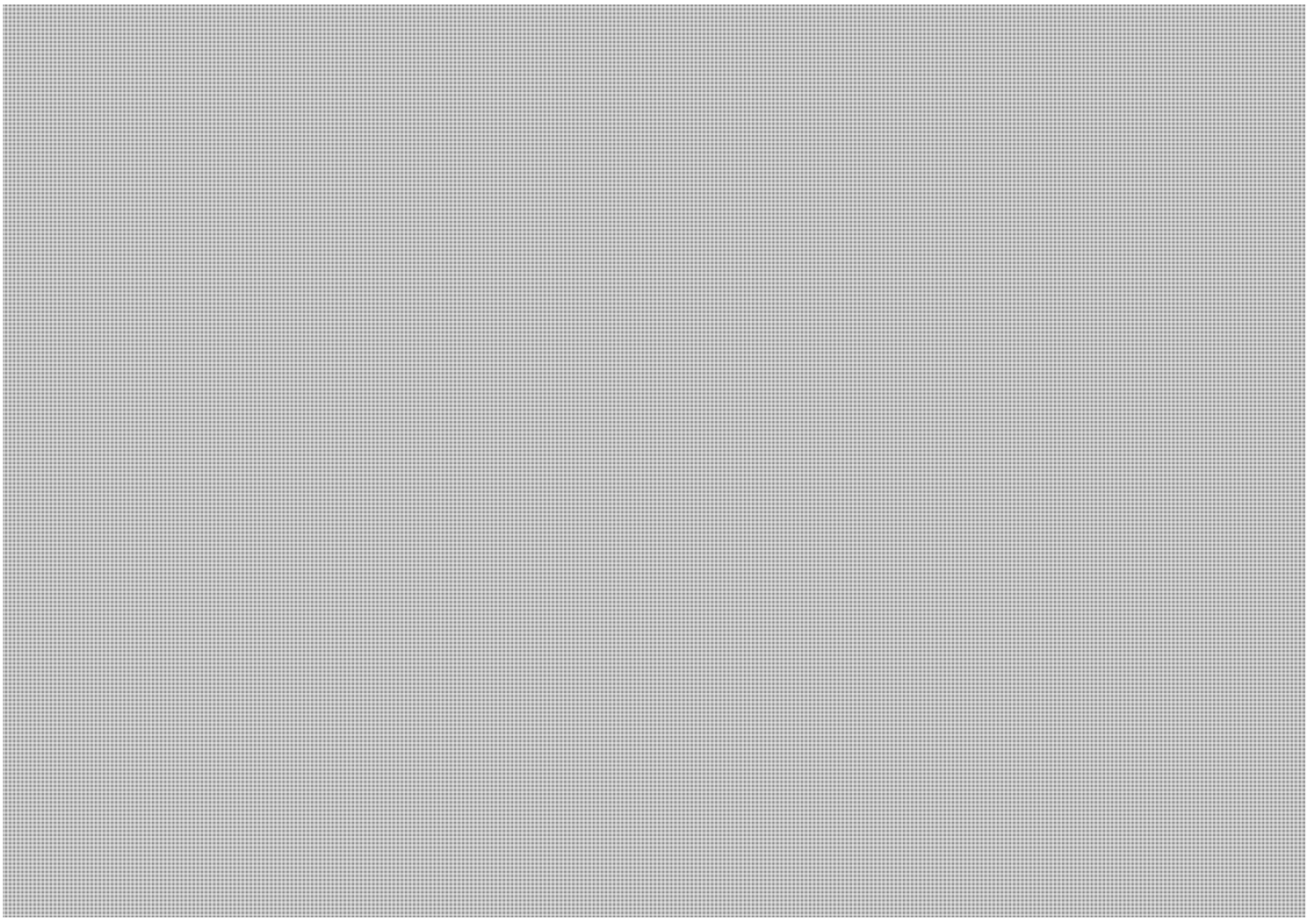
Can someone get back to [redacted] about what we are doing on this?
Have a great day,

Windy
Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada
From: [redacted]
Sent: January-06-12 9:04 AM
To: [redacted]
Cc: Anderson, Windy; [redacted] tiago.dejesus@rcmp-grc.gc.ca; Victor Munro
Subject: Re: Stratfor Breach

Thank you [redacted] and Angus for sharing.



"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> Dominic Lafleur 2012-01-06 08:40 >>>
Good morning



Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265

s.19(1)

Williston, Sandra

From: [redacted]
Sent: January-06-12 11:41 AM
To: 'tim.oneil@rcmp-grc.gc.ca'; [redacted] s.16(2)(c)
Cc: Anderson, Windy; CYBERDO
Subject: RE: Stratfor Breach

Good Day Tim;

Thank you for the information below.

We were not aware of this twitter posting, but it sounds like they are preparing for another "wave".

We will stay diligent and keep you informed if we see anything. Thanks!

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada.
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: Anderson, Windy
Sent: January-06-12 10:54 AM
To: [redacted]
Subject: FW: Stratfor Breach

fyi

Have a great day,

Windy

Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca

s.15(1) - Subv
s.16(2)(c)
s.19(1)

From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: January-06-12 10:07 AM
To: bev.richardson@cbsa-asfc.gc.ca; Anderson, Windy; Darren Sabourin; Ken Mcphee;
Cc: Robert Lafrance; tiago.dejesus@rcmp-grc.gc.ca
Subject: Stratfor Breach

Good Day Darren and Windy

Are either of you two able to provide more information/assessment relating to this?

Specifically: "The Anonymous syndicate behind the recent hacking of Stratfor has published "another exciting zine release, and this is a big one."

I believe that we will be getting many more similar requests for assistance regarding this issue.

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265

>>> 2012-01-06 07:36 >>>

I found this on twitter via this email not sure what it means or what the implications are.....F.Y.I.

Results for

- **Tweets ·**
- Top
  - **Top**
  - **All**
  - **With links**
- Refine results »

»

AnonymousIRC
Countdown to Lulz started. Fasten your seatbelts.

13 hours ago
Retweeted 100+ times
»

The Anonymous syndicate behind the recent hacking of Stratfor has published "another exciting zine release, and this is a big one."

CRIIU

From:
Sent: January-05-12 11:45 AM
To: bev.richardson@cbsa-asfc.gc.ca; Ken Mcphee; Terry Pomeroy
Subject: Fwd: Stratfor Breach
For information purposes and dissemination as you see fit to other partners and agencies.;

Pages 1362 to / à 1365

are withheld pursuant to section

sont retenues en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: [redacted]
Sent: January-06-12 11:25 AM
To: Timothy O'Neil (tim.oneil@rcmp-grc.gc.ca)
Cc: [redacted] Anderson, Windy
Subject: FW: Stratfor Breach

Good Day;

[redacted]

I have requested our Technical Analysis Team to perform analysis on the three links in the email received by Dominic Lafleur. We will let you know the results when they are back.

[redacted]

Hope this helps.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

From: Anderson, Windy
Sent: January-06-12 9:17 AM
To: [redacted]
Subject: FW: Stratfor Breach

Can someone get back to Tim about what we are doing on this?
Have a great day,

Windy
Director Canadian Cyber Incident Response Centre Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097 windy.anderson@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada
From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]

Pages 1367 to / à 1368
are withheld pursuant to section
sont retenues en vertu de l'article

16(1)(a)

of the Access to Information
de la Loi sur l'accès à l'information

Williston, Sandra

From: Williston, Sandra
Sent: January-06-12 9:56 AM
To: Anderson, Windy
Cc: Klassen, Nathan; [redacted]
Subject: CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

CCIRC CE11-2549
File No.: 384942
RDIMS No.: 541243

Hello Windy;

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

Stratfor Global Intelligence has already notified all affected users through email, facebook and twitter. The mitigation advise to their customers was to contact their financial institution and inform them of this incident and to watch for any unauthorized activity on their accounts. In addition, they have advised that they will provide paid subscribers with identity protection coverage with a leading provider of global identity protection company at their expense for 12 months.

[redacted]

CCIRC has closed this incident and will continue to monitor.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

Klassen, Nathan

From: Klassen, Nathan
Sent: January-06-12 10:04 AM
To: Williston, Sandra
Subject: RE: CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

Looks great!

From: Williston, Sandra
Sent: January-06-12 9:56 AM
To: Anderson, Windy
Cc: Klassen, Nathan; [redacted]
Subject: CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

CCIRC CE11-2549
File No.: 384942
RDIMS No.: 541243

Hello Windy;

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

Stratfor Global Intelligence has already notified all affected users through email, facebook and twitter. The mitigation advise to their customers was to contact their financial institution and inform them of this incident and to watch for any unauthorized activity on their accounts. In addition, they have advised that they will provide paid subscribers with identity protection coverage with a leading provider of global identity protection company at their expense for 12 months.

CCIRC has completed notifications to Federal and Provincial STRATFOR clients through their respective IT Security departments. The final count of affected users is [redacted] users in 9 Provinces. CCIRC provided further mitigation advise to affected Government employees to be on the outlook for targeted email attacks and social engineering which may result from this compromise.

CCIRC has closed this incident and will continue to monitor.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

Klassen, Nathan

From: Williston, Sandra
Sent: January-06-12 9:56 AM
To: Anderson, Windy
Cc: Klassen, Nathan; [redacted]
Subject: CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

s.16(2)(c)

CCIRC CE11-2549
File No.: 384942
RDIMS No.: 541243

Hello Windy;

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

Stratfor Global Intelligence has already notified all affected users through email, facebook and twitter. The mitigation advise to their customers was to contact their financial institution and inform them of this incident and to watch for any unauthorized activity on their accounts. In addition, they have advised that they will provide paid subscribers with identity protection coverage with a leading provider of global identity protection company at their expense for 12 months.

CCIRC has completed notifications to Federal and Provincial STRATFOR clients through their respective IT Security departments. The final count of affected users is [redacted] users in 9 Provinces. CCIRC provided further mitigation advise to affected Government employees to be on the outlook for targeted email attacks and social engineering which may result from this compromise.

CCIRC has closed this incident and will continue to monitor.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

Williston, Sandra

From: [redacted]
Sent: January-06-12 10:32 AM
To: [redacted]
Subject: FW: Internet facing device. [PGP]
Attachments: PGPexch.htm.pgp; Message2.pgp

s.13(1)(a)
s.16(2)(c)

[redacted]

*** END PGP DECRYPTED/VERIFIED MESSAGE ***

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

Page 1373

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(a), 16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

-----END PGP MESSAGE-----

Anderson, Windy

From: [redacted]
Sent: January-06-12 1:29 AM
To: dominic.lafleur@rcmp-grc.gc.ca
Subject: Rate Stratfor's Incident Response

For the video announcement, please see [redacted]
Read full press release: [redacted] Rate Stratfor's incident response:
[redacted]

Hello loyal Stratfor clients,

We are still working to get our website secure and back up and running again as soon as possible.

To show our appreciation for your continued support, we will be making available all of our premium content *as a free service* from now on.

We would like to hear from our loyal client base as to our handling of the recent intrusion by those deranged, sexually deviant criminal hacker terrorist masterminds. Please fill out the following form and return it to me

[redacted]

s.16(2)(c)
s.19(1)

Williston, Sandra

From: Darke, Peter
Sent: January-06-12 9:41 AM
To: Mack, Laurie; Clow, Patrick; Bergeron, Dominic
Subject: FW: Symantec Confirms Source Code Leak in Two Enterprise Security Products

fyi

Peter Darke
Senior Advisor | Conseiller
Network & Security | Réseau et Sécurité
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West, Ottawa Ontario K1A 0P8 | 269, avenue Laurier Ouest Ottawa (Ontario) K1A 0P8
Tel | Tél: (613) 991-7750
Fax | Téléc: (613) 996-1085
Email | Courriel: peter.darke@ps-sp.gc.ca
Web: www.publicsafety.gc.ca | www.securitepublique.gc.ca

From: CSO News Watch [mailto:cso_newsletters@cxolyris.cxomedia.com]
Sent: January 6, 2012 9:40 AM
To: Darke, Peter
Subject: Symantec Confirms Source Code Leak in Two Enterprise Security Products

GCHQ Awards Bonuses to Stop IT Security Experts Leaving | WhatsApp to Roll Out Stronger Fixes for Messaging Vulnerability

CSO News Watch

Forward this to a Friend >>>

Symantec Confirms Source Code Leak in Two Enterprise Security Products

Symantec late Thursday confirmed that source code used in two of its older enterprise security products was publicly exposed by hackers this week. **Read More**

In this Issue

- Lawmakers Seem Intent on Approving SOPA, PIPA
- Microsoft Plans Big January Patch Tuesday
- Blind spots: How cyber defense is like stopping Tim Tebow
- Two New Security Books Ponder: Just How Vulnerable Are We?
- SpyEye Malware Borrows Zeus Trick to Mask Fraud
- Smart Grid Security Inadequate, Threats Abound
- Murder Retrial Ordered After Court Records Destroyed By Virus
- Japan Testing 'virus' Cyberdefence Weapon, Reports Say
- Anonymous Threatens Sony, Spares PSN Customers
- Windows 8 Can Scrub Data From Disk, but Not Up to Tough Security Specifications
- Microsoft Researcher: Passwords Aren't Dead but They Need Fixing
- Facebook Brings Back the Hack
- Anonymous Targets Neo-Nazis Sites: Anti-Hate Groups Condemn Action

GCHQ Awards Bonuses to Stop IT Security Experts Leaving

Can they compete with IT giants though? **Read More**

WhatsApp to Roll Out Stronger Fixes for Messaging Vulnerability

The problem lets someone change the status message of another person merely by knowing their phone number **Read More**

E-Voting Machine Freezes, Misreads Votes, U.S. Agency Says

DS200 optical scanner from ES&S doesn't meet federal standards, but remains certified, Election Assistance Commission says **Read More**

Government engineers actively plan for cyberwar

Governments are arming themselves to their cyber-teeth with offensive and counter-defense cyber weapons, and there's little enterprises can do to avoid the fray. **Read More**

U.S. State Department Investigating Huawei on Iran Concerns

Six U.S. lawmakers have previously called for the investigation of Huawei's activities in Iran **Read More**

Murdoch Wife Fake Twitter Account Highlights Online Identity Risk

Fake Wendi Deng Murdoch account was initially verified by Twitter as genuine **Read More**

Privacy 2012: I know what you did at 3:30 a.m.

For a peek into what experts expect this year and beyond when it comes to privacy, we turn to the Rebecca Herold (aka the Privacy Professor) for answers. **Read More**

Ramnit Worm Goes After Facebook Credentials

The worm appears to have collected 45,000 logins and passwords already, according to Seculert Read More

Facebook Timeline Scams Prey on Wishful Thinking
Read More

Anatomy of an ATM Skimmer Scam
Skimmers could steal your financial information at the ATM—or even at your local supermarket. Here's how to protect yourself. Read More

Lawmakers Seem Intent on Approving SOPA, PIPA
So far, strong opposition to the copyright bills hasn't changed many minds Read More

Microsoft Plans Big January Patch Tuesday
Mystery of the month, say experts, is what Microsoft means by 'security feature bypass' update Read More

Blind spots: How cyber defense is like stopping Tim Tebow
Michigan's CTO on the extremes of marketing hype and defeatist mentality in security Read More

Two New Security Books Ponder: Just How Vulnerable Are We?
Read More

WEBCAST: CA Technologies

A Step-by-Step Guide to Building Virtualization Maturity
This webinar will explain the key phases of virtualization maturity, outline the critical maturity challenges, and provide you with a step-by-step guide to building your virtualization maturity and maximizing your virtualization outcomes. View Now

---

SpyEye Malware Borrows Zeus Trick to Mask Fraud
One of the most powerful banking trojans has an additional tricky feature, according to Trusteer Read More

Smart Grid Security Inadequate, Threats Abound
Read More

Murder Retrial Ordered After Court Records Destroyed By Virus
Stenographer blamed after backup records nixed Read More

Japan Testing 'virus' Cyberdefence Weapon, Reports Say
Capable of tracing and disabling attackers Read More

Anonymous Threatens Sony, Spares PSN Customers
The hacker collective threatens to expose private information of Sony executives, promising to spare customers and the PlayStation Network Read More

Windows 8 Can Scrub Data From Disk, but Not Up to Tough Security Specifications
Read More

Microsoft Researcher: Passwords Aren't Dead but They Need Fixing
Read More

Facebook Brings Back the Hack
In its third annual Hacker Cup, Facebook is inviting programmers to rapidly solve programming challenges Read More

Anonymous Targets Neo-Nazis Sites: Anti-Hate Groups Condemn Action
Anonymous hacktivists name names at Nazi-leaks.net in latest round of attacks against controversial targets Read More

Editor's Picks: All-time classics, part 3

1. What is a Chief Security Officer?
2. A few good information security metrics
3. 10 tough security interview questions and how to answer them
4. Red gold rush: The copper theft epidemic
5. 19 ways to build physical security into a data center

Get more CSO peer perspective online
LinkedIn | Facebook | Twitter

Page 1380

is a duplicate

est un duplicata

Page 1381

is a duplicate

est un duplicata

Page 1382

is a duplicate

est un duplicata

Page 1383

is a duplicate

est un duplicata

Page 1384

is a duplicate

est un duplicata

Page 1385

is a duplicate

est un duplicata

Page 1386

is a duplicate

est un duplicata

Page 1387

is a duplicate

est un duplicata

Page 1388

is a duplicate

est un duplicata

s.20(1)(c)

DATE	SECTOR	INCIDENT/ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
3 Jan 2012	Financial	CE11-2552 [redacted] Phishing] CE11-2553 [redacted] Trust Phishing]	Phishing		- 2552 appears to originate from Paris - 2553 is routed through Paris but directed to US server	
4 Jan 2012	Government (Fed, Prov/Dept Education) Transportation Universities	CE11-2554 [Sinkhole Notification – Multiple Organizations]	Hosts within these organizations were infected with DNS Changer malware.			
					Federal: Reported to Federal Gov't CERT Provincial: Reported to Provincial Department of Education Transportation: Reported to City's Airport Authority Academia: Reported to 4 Universities.	
5 Jan 2012	Telecom	CE12-2555 [Defacement hosting provider website] - Summary: CCIRC observed that a website operated by an Internet hosting service				

		provider located in Manitoba was recently defaced.				
	Financial	CE12-2556 [redacted] Phishing] -	- Summary: hxxp://charltonhats[.]com/admin[.]html - 63.247.80.138(Global Net Access – Atlanta Georgia). This site redirected to the final phishing page located at:			
		: CE12-1257 [redacted] Phishing] -	- (Axarnet Communications – Malaga Spain)			
		CE12-2558 [redacted] Phishing]	- 62.193.220.178 (AMEN Networks, Paris France)			
	Government (Fed, Prov); Financial (banks)	CE12-2559 [Drone Notifications - Multiple Organizations]	- Infection types included (DNS Changer, Mebroot, or Torpig). : Federal: 2 departments (via CTEC) Provincial: 3 provincial governments Financial: 2 banks -			
	Fed Govt plus	CE11-2549 [Stratfor Hack affected Canadians]	- Summary: On December 25, 2011, the Anonymous group hacked into a private intelligence agency,			

			Strategic Forecasting Inc. or STRATFOR, based in Austin, Texas. The attack began with the release of STRATFOR's client list, followed by release of accounts in batches believed to belong to STRATFOR's customers. The release includes emails, passwords (hashed with MD5), home/office addresses and credit card information (full 16-digit number, expiry date and CVV number). CCIRC received a report from a LE regarding Stratfor account compromises. - Action/Decision: Update - A. Item: CCIRC received the first set of data, 40,235 compromised accounts. Results: 34 gc.ca accounts – sent to Federal Government CERT for notification. 1803 Canadians – analysing for CI notification. -			

International: IWWN Spring Meeting – Need to sign up – who's going from GoC?

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: JAN 09 2012

File No.: 384961
RDIMS No.: 541955

Seen by the DM
Vu par le SM

JAN 10 2012

MEMORANDUM FOR THE DEPUTY MINISTER

CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

(Information only)

ISSUE

Eight hundred and eighty federal government workers and 109 provincial government users in nine provinces have been affected by the hacking of a private international intelligence agency.

BACKGROUND

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter, they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

CONSIDERATIONS

There are financial, workplace security, and privacy considerations regarding this incident.

First, there is a financial risk to all impacted individuals as the credit card information posted online contained the full 16 digit number, expiry date, and Card Verification Value number (i.e. everything needed to make purchases).

Second, compromised individuals could be victims of specific and targeted attacks, such as malicious emails, social engineering, and attempts to compromise workplace security.

Third, impacted individuals' privacy could be compromised as home/office telephone numbers and home/office addresses were released. Given the fact that 860,000 login credentials have been compromised, there is also a strong likelihood that additional downstream privacy risks exist for impacted individuals as a significant percentage of the population uses the same password for many Internet sites and work.

NEXT STEPS

There are three main actions that the Canadian Cyber Incident Response Centre (CCIRC) is taking to address this situation.

First, CCIRC is working with RCMP to identify federal government users registered with STRATFOR. Identified users will be notified through the Cyber Threat Evaluation Centre (CTEC).

Second, CCIRC has completed its analysis and identified provincial government users who have been affected. CCIRC has notified each provincial government's lead cyber security department.

Third, CCIRC has recommended that affected government employees change all Internet account passwords that use elements from their compromised password; monitor their credit card transactions and; contact their bank regarding the credit card breach.

CCIRC has closed this incident and will continue to monitor for any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Sandra Williston

Deputy
This is useful background material for your meeting later this week with CCIRC.

s.15(1) - Subv

s.16(2)(c)

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-10-12 8:37 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 10, 2012/ le 10 janvier 2012

Print Media

Canning the spam
The federal government can't move soon enough on its spam reporting centre, dubbed the "Freezer," which is designed to crack down on the millions of unwanted messages clogging Canadians' cellphones, inboxes and social network accounts. Times Colonist, A10

Online Media

Obama defence plan details heightened global cyber danger
US president Barack Obama has spoken of the drastically heightened cyber threat facing nations around the world, as he announced major changes to the American defence strategy. As he appeared at the Pentagon last week to unveil the new defence strategy, Obama promised to focus closely on improving the technological capabilities of the US armed forces. "We will ensure that our military is agile, flexible and ready for the full range of contingencies," he said. PC Advisor UK

Cyber tension follows hacker attack on Israeli credit card users
Last week, a hacker published credit card information belonging to about 20,000 Israelis on the Internet, along with the personal details of hundreds of thousands more. Israeli credit card companies swiftly canceled the cards and pledged to reimburse customers for damages caused by fraudulent use. Los Angeles Times

Venezuela's Chavez Backs Diplomat Who Was Expelled by US
Venezuelan President Hugo Chavez Monday night backed the South American country's consul general in Miami, who was expelled by U.S. authorities over the weekend and was linked to an alleged plot to launch a cyber attack against the U.S. government. Wall Street Journal

Israeli Official Threatens Retaliation After Cyber Attack
A top Israeli official said over the weekend that cyberattacks are akin to terrorism and threatened aggressive action against those who recently posted online personal information belonging to Israelis. PC Magazine; CNN; SC Magazine

US authorities probe Indian govt spy unit for email hacking
US authorities are investigating allegations that an Indian government spy unit hacked into emails of an official US commission that monitors economic and security relations between the United States and China, including cyber-security issues. Reuters; Forbes

SEC Push May Yield New Disclosures of Cyber Attacks on Companies

China-based hackers rifled the computers of DuPont Co. (DD) at least twice in 2009 and 2010, hunting the technological secrets that made the company one of the world's most successful chemical makers. It's not something investors would have learned from DuPont's regulatory filings, or from those of other companies victimized by hackers. Bloomberg

'Anonymous' hacktivists expose the intelligence gap
Over Christmas a busy, secretive group were at work, with their own views on who had been naughty and nice. However it was not Santa's elves, but the amorphous "Anonymous" collective making the decisions. This group of hackers released a vast trove of email addresses, passwords and credit card information belonging to subscribers of the US intelligence company Stratfor – and the hangover has carried on into the new year, with the release of MoD and Nato officials' details. The Guardian

Top UK security officials exposed in hack attack
Hundreds of sensitive email addresses for UK security officials were among details stolen in a major hacking attack, it has emerged. The hackers scooped the email addresses and other information during a Christmas attack on security consultancy Stratfor, but the type of UK officials breached has only just come to light. PC Pro

Google patches Chrome, beefs up malicious file blocking tech
Google last week patched Chrome 16 and improved the download warnings in the impending Chrome 17. Last Thursday, Google updated Chrome 16 with a security update that quashed three bugs, all rated "high," the company's second-most-dire threat rating. PC Advisor

Zeus returns: FBI warns of 'Gameover' ID-theft malware
A new variant of the notorious Zeus identity-theft Trojan is making the rounds and the Federal Bureau of Investigations (FBI) says it is capable of defeating common methods of user authentication employed by financial institutions. ZDNet

Anti-spam plan lacks teeth: Prof
If you still find your e-mail in-box inundated daily with unwanted messages from faraway royalty offering you free money or companies claiming they'll send you pharmaceuticals at a fraction of their price, you were likely pleased with the federal government's announcement of anti-spam legislation. Canoe

Do you know your cyberthreats?
The watchdogs at the Government Accountability Office this week issued a report that takes a look at what information, or guidance as they call it, is available to help government agencies and public sector companies bulk up their cybersecurity efforts. PC Advisor

s.16(2)(c)

Grigsby, Alexandre

From: Grigsby, Alexandre
Sent: January-10-12 2:48 PM
To: 'Vivasvat.Dadwal@international.gc.ca'
Cc: Heather.Dryden@ic.gc.ca; 'Dvorkin, Corey'
Subject: RE: Tech gets its day in Congress as SOPA fight continues

That's why you avoid picking fights with the Internets

From: Vivasvat.Dadwal@international.gc.ca [mailto:Vivasvat.Dadwal@international.gc.ca]
Sent: January-10-12 12:39 PM
To: Loris.Mirella@international.gc.ca
Cc: Sean.Clark@international.gc.ca; Grigsby, Alexandre; Heather.Dryden@ic.gc.ca; Jonathan.Solomon@international.gc.ca; Lynn.McDonald@international.gc.ca; Nicholas.Gordon@international.gc.ca
Subject: RE: Tech gets its day in Congress as SOPA fight continues

And to add to that, check the link out:
Stay On Top of the Fight Against SOPA/PIPA with These Tools: [redacted]

They have developed tools to monitor the situation!

From: Dadwal, Vivasvat -TMI
Sent: January 10, 2012 12:33 PM
To: Mirella, Loris -TMI; [redacted]
Cc: Clark, Sean -WSHDC -TD
Subject: RE: Tech gets its day in Congress as SOPA fight continues

This was in TIME magazine a couple of days ago...don't think it would ever happen, but interesting to think about it anyhow.

SOPA: What if Google, Facebook and Twitter Went Offline in Protest?

By Graeme McMillan

Can you imagine a world without Google or Facebook? If plans to protest the potential passing of the Stop Online Piracy Act (SOPA) come to fruition, you won't need to; those sites, along with many other well-known online destinations, will go temporarily offline as a taste of what we could expect from a post-SOPA Internet.

Companies including Google, Facebook, Twitter, PayPal, Yahoo! and Wikipedia are said to be discussing a coordinated blackout of services to demonstrate the potential effect SOPA would have on the Internet, something already being called a "nuclear option" of protesting. The rumors surrounding the potential blackout were only strengthened by Markham Erickson, executive director of trade association NetCoalition, who told FoxNews that "a number of companies have had discussions about [blacking out services]" last week.

According to Erickson, the companies are well aware of how serious an act such a blackout would be:

> This type of thing doesn't happen because companies typically don't want to put their users in that position. The difference is that these bills so fundamentally change the way the Internet works. People need to understand the effect this special-interest legislation will have on those who use the Internet.

The idea of an Internet blackout should seem familiar to anyone who's been paying attention to the debate so far. In addition to a blackout already carried out by Mozilla, hacking group Anonymous proposed the same thing a couple of weeks ago, suggesting that sites replace their front pages with a statement protesting SOPA. That suggestion itself came a week after Jimmy Wales had asked Wikipedia users about the possibility of blacking out that site in protest of the bill.

(**MORE:** 'Anonymous' Blacks Out the Internet in Response to SOPA Debate)

As a way of drawing attention to the topic, it's something that will definitely work. Just Google alone going dark would cause havoc online, but the idea of it happening at the same time as Facebook, Twitter et al. follow suit seems almost unimaginable.

The question then becomes how to translate the inevitable confusion and outrage from those who don't know what SOPA is into activism. The key, I assume, lies in the execution of the blackout: Will the sites that voluntarily go down be entirely unavailable or will they follow the Anonymous-proposed model of replacing the front page with a statement explaining what is going on, why and how users can best become involved in the discussion? If the sites do go *entirely* dark, is the hope that the resulting outrage will be enough to fuel news stories about the reason behind the decision? And that users will not transfer their frustration to the sites themselves, as opposed to the bill they're protesting?

The fact that Facebook and Twitter are both said to be considering taking part in the blackout is simultaneously heartening and worrying. The former because, well, they're standing up for what they collectively believe in — and that's a good thing. But the latter because the lack of availability for social media on the proposed blackout day feels like it's giving up the best chance to harness the frustration and energy people will feel about the temporary loss of the Internet as they know it, and a great possibility to focus and direct that energy into productive activism against SOPA. Then again, it may take losing Facebook and Twitter to really drive home how dramatically SOPA could affect the Internet.

All of this may come to nothing, of course. The companies may decide not to black out their sites and find other ways to protest SOPA. That could be for the best; collectively closing down the most trafficked sites on the Internet to prove a point will certainly garner a lot of attention, but the effects it'll have beyond that (and the reactions it'll cause as a result) are difficult to predict and could easily end up causing a backlash against the sites responsible at a time when they least want it. But still ... just try to imagine an Internet without Google, Facebook or Yahoo. Even for a day. Almost makes you want it to happen, just to make people realize how reliant we are on the Internet as we know it now, doesn't it?

MORE: Sorry, Folks: Game Publishers Didn't 'Drop' SOPA Support

Graeme McMillan is a reporter at TIME. *Find him on Twitter at @Graememm or on Facebook at Facebook/Graeme.McMillan. You can also continue the discussion on* TIME's *Facebook page and on Twitter at @TIME.*

Related Topics: *Anonymous, mozilla, paypal, SOPA, Stop Online Piracy Act, wikipedia, Yahoo, Companies, Facebook, Google, Reviews & Features, Social Unrest, Twitter*

Read more: http://techland.time.com/2012/01/05/sopa-what-if-google-facebook-and-twitter-went-offline-in-protest/#ixzz1j4sNzEBa

---

From: Mirella, Loris -TMI s.16(2)(c)
Sent: January 10, 2012 12:28 PM
To: [redacted]
Cc: Clark, Sean -WSHDC -TD
Subject: Tech gets its day in Congress as SOPA fight continues

Tech gets its day in Congress as SOPA fight continues

By Stacey Higginbotham Jan. 9, 2012, 1:10pm PT 2 Comments
http://gigaom.com/2012/01/09/tech-gets-its-day-in-congress-as-sopa-fight-continues/

Representative Darrell Issa (R-Calif.) has called a hearing that will bring more voices from the technology industry to Washington, D.C. to discuss how legislation such as the Stop Online Piracy Act (SOPA) would affect the Internet. On Jan. 18, industry representatives that include Brad Burnham from Union Square Ventures; Lanham Napier, the CEO of Rackspace Hosting; and Alexis Ohanian, co-founder of Reddit.com, will testify before Congress.

At the previous SOPA hearing, the tech industry was represented by a single Google executive, while the five other participants testifying were from the content industry. Issa's upcoming hearing, however, is not about SOPA directly. Issa – who is pushing his own version of an IP protection bill dubbed the Online Protection and Enforcement of Digital Trade, or OPEN, Act – is holding his hearing on how Congress can help protect IP without breaking the Internet. Perhaps it can also lead to legislation that actually solves the problem of piracy a bit better as well. From his release:

> House Committee on Oversight and Government Reform Chairman Darrell Issa (R-CA) today announced that the Full Committee will hold a hearing on January 18 to examine the potential impact of Domain Name Service (DNS) and search engine blocking on American cyber-security, jobs and the Internet community. In light of policy proposals affecting the way taxpayers access the Internet, the hearing will also explore federal government strategies to protect American intellectual property without adversely affecting economic growth. The Committee will hear testimony from top cyber-security experts and technology job creators.

This news comes amid some wins and losses around SOPA overall. Despite wrongly fingering Rep. Paul Ryan (R-Wis.) as a co-sponsor of the SOPA bill, Reddit users appear to have forced the Wisconsin Congressman to take a stand against the legislation, while a look at the TV operations of news organizations whose parent companies are in support of SOPA show that those organizations are not covering the issue in depth for their viewers (but they are doing so online). As we wait for the next official SOPA markup hearing later this month (the last attempt to push the legislation out of committee was delayed over the Congressional recess), Issa's hearing will be a chance for the tech community to make its points. Hopefully, someone in the House Judiciary Committee committee that's holding the SOPA markups will be listening.

Loris Mirella
Intellectual Property Trade Policy Division (TMI) | Direction de la politique commerciale sur la propriété intellectuelle (TMI)
111 promenade Sussex Drive loris.mirella@international.gc.ca
Tel. | Tél. 613-996-8312
Facsimile | Télécopieur 613-944-0066
Foreign Affairs and International Trade Canada | Affaires étrangères et Commerce international Canada

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-10-12 1:44 PM
To: [redacted]
Subject: RE: Stratfor Breach

s.19(1)
s.20(1)(c)

[redacted]

Pages 1401 to / à 1402
are withheld pursuant to sections
sont retenues en vertu des articles

19(1), 20(1)(c)

of the Access to Information
de la Loi sur l'accès à l'information

Page 1403

is withheld pursuant to section

est retenue en vertu de l'article

20(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-11-12 8:38 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted]; Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 11, 2012/ le 11 janvier 2012

Print Media

Privacy watchdog to probe UVic in security breach
An investigation by B.C.'s Office of the Information and Privacy Commissioner will determine whether the University of Victoria contravened accepted standards by keeping sensitive, unencrypted information about more than 11,700 employees on a mobile device. A weekend break-in at the administration services building saw the theft of laptops, handheld electronics, storage devices, cheques and a small amount of cash. The data stolen included names, payroll information and social insurance numbers of UVic employees dating back to Jan. 1, 2010. Times Colonist, A1

Computer virus scam goes viral
It's a consumer scam that reached epidemic proportions in Canada last year. You get a call from someone who says your computer is at risk of crashing because of a virus or malicious software. The caller may suggest he or she works for Microsoft and is aware of issues with your Windows operating system. Toronto Star, B1

Online Media

Energy Department to analyze power grid cyber threats
U.S. Energy Secretary Steven Chu has unveiled an initiative that seeks to further protect the power grid from cyber attacks. The Electric Sector Cybersecurity Risk Management Maturity project, a federal program to find and contain gaps in the cyber security defenses protecting the nation's electric grid, will be headed by the Department of Energy (DOE), with assistance from the Department of Homeland Security (DHS) and the private sector. SC Magazine

U.S. ousts Venezuelan consul for plotting cyberattack on U.S. nukes
Diplomats accredited to foreign governments can't be arrested, prosecuted and imprisoned by the country that hosts the embassy in which they work. It sounds like an idiotic rule when you look at the number of traffic and parking tickets UN diplomatic cars pick up in New York, but it's the only way governments can keep non-suicidal negotiators on staff who can be sent to talk to a potentially hostile governments with a reasonable chance of coming back with all their body parts attached in the traditional way. IT World

Anonymous hackers attack anti-piracy groups
Cyber-activists attacked the websites of Finnish anti-piracy groups after a local internet service provider was forced to block access to a popular file-sharing website, officials said. Antti Kotilainen, a spokesman for the Copyright Information and Anti-Piracy Centre (CIAPC), told AFP that websites run by his organisation and the International Federation of the Phonographic Industry (IFPI) had been "down since Monday". New Zealand Herald

Cyber Attacks May Be Revealed to Investors as SEC Rules Push Disclosures

China-based hackers rifled the computers of DuPont Co. at least twice in 2009 and 2010, hunting the technological secrets that made the company one of the world's most successful chemical makers. It's not something investors would have learned from DuPont's regulatory filings, or from those of other companies victimized by hackers. MSN

Obama defence plan details heightened global cyber danger
US president Barack Obama has spoken of the drastically heightened cyber threat facing nations around the world, as he announced major changes to the American defence strategy. As he appeared at the Pentagon last week to unveil the new defence strategy, Obama promised to focus closely on improving the technological capabilities of the US armed forces. Computerworld

Adobe plugs 6 critical holes in Reader
Adobe on Tuesday patched six vulnerabilities in the newest version of its popular Reader PDF viewer, making good on a late-2011 promise when it shipped an emergency update for an older edition. Computerworld

US probing hacking allegation against Indian spies
American law enforcement agencies are probing an allegation that Indian military intelligence (MI) spied on a US-China Economic and Security Review Commission member's email. The move comes after hackers posted letters and documents allegedly stolen from Indian servers in November last year. India Today

DHS asks America to run more computer virus scans
"Cyber fit" is a watchword of the President Obama's counterterrorism bureacurats, as the Department of Homeland Security (DHS) suggested this morning that Americans adopt greater online security as a New Year's Resolution. Washington Examiner

Who are the go-to cybersecurity help groups?
There are a ton of groups out there that offer cybersecurity help and guidance, the trick, it seems is finding the right one for your organization. The Government Accountability Office this week issued a report on just that notion saying: "Given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Network World

Microsoft issues seven security patches, BEAST fix included
Microsoft on Tuesday released seven security fixes, including one cited as "critical," to correct eight vulnerabilities. None of the patches addressed major, ongoing attacks, but several were notable because Microsoft identified them as fixes that address issues that are easy to implement and capable of executing malware remotely. SC Magazine

Google patches Chrome, beefs up malicious file blocking tech
Google last week patched Chrome 16 and improved the download warnings in the impending Chrome 17. Last Thursday, Google updated Chrome 16 with a security update that quashed three bugs, all rated "high," the company's second-most-dire threat rating. PC Advisor UK

Dincoy, Rana

From: Dincoy, Rana
Sent: January-11-12 11:46 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce
Subject: Confirming the incident write-ups for the Weekly Summary

Hi Luc,

Can you please confirm the below? I've spoken with Bruce to obtain clarification where I needed it (Bruce please let me know if something isn't right).

I want to make sure particularly that I am not overstating things in my "Comments" section. I'd appreciate your feedback by tomorrow morning... Thanks! Rana

For the Week of 31 Dec 2011 – 6 Jan 2012

Issued: 12 Jan 2012

HIGHLIGHTS:

Notable Incidents:

- Client information for a private US intelligence agency posted on the Internet by Anonymous – clients include Canadians
- Malicious e-mails from threat actors impersonating Canadian banks, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems of provincial government, financial, transportation, and education sector organizations
- A website hosting service provider's website vandalized by hackers

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

NOTABLE INCIDENTS– 31 DECEMBER 2011 THROUGH 6 JANUARY 2012:

Canadian Critical Infrastructure:

Provincial Government, Transportation and Education: Computers of two provinces' departments of education, an airport authority and four universities may have been compromised by certain common malicious software. There were also reports of compromised computers as a result of the worldwide internet fraud "Ghostclick", which the FBI exposed in late 2011.

CCIRC notified contacts in those organizations of these potential compromises and offered mitigation advice. Impact of the compromises is unknown but could potentially include data theft or remote use of these computers to commit malicious acts on the Internet. In the "Ghostclick" fraud, computer users were unknowingly re-directed to certain webpages, which financially benefited the fraudsters.

Comment: Open source computer infection reports indicate which organizations appear to be infected with certain commonly found malicious software. However, only the affected organization can confirm whether their computers have been truly been infected and the impact. **While there hasn't been any such confirmation in this situation, CCIRC believes it likely that there were compromises.**

CCIRC continues to notify stakeholder organizations that were impacted by the worldwide Ghostclick fraud and is in contact with US CERT.

Financial Sector. Threat actors impersonating prominent Canadian banks tried to compromise computer users' machines by persuading them to click on malicious links in an e-mail. CCIRC notified these institutions, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be identified as such, warning future unsuspecting users. The malicious links led to websites hosted in United States, France and Spain.

Telecommunication Sector. CCIRC observed that a website operated by an internet hosting service provider was vandalized by hackers. The impact is unknown.

Comment: Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website that can be vandalized by hackers is also vulnerable to being used to compromise the computers of that website's visitors.

International:

Anonymous, the famed hacker group, released personal and credit card information of a private US intelligence company's clients, on the Internet. These include Canadian clients. CCIRC notified the Canadian stakeholders and offered mitigation advice. CCIRC continues to analyze the situation.

Comment: The personal information released includes names and e-mail addresses, which can be used for a variety of malicious purposes by any threat actor. This can include sending malicious e-mails to those clients to compromise their computers or using the credit card information for financial gain. The release of physical addresses could be of concern to certain clients for privacy and security reasons.

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

WEEKLY CYBERSECURITY REPORT FOR CIOs

CCIRC CYBER AWARNESS PRODUCT: 12-S-001
WEEK OF JANUARY 3, 2012

s.16(2)(c)

Purpose

To inform security and information technology executives in government and critical infrastructure sectors about cyber events and notable news seen by the Canadian Cyber Incident Response Centre.

Overview

There was no new nation-wide cyber security incident this week. The major event of the week was the hacking of STRATFOR, a private US intelligence company, where clients' online credentials and credit card information was leaked. [redacted] were affected. CCIRC continued to receive reports on common computer infections that benefit cyber criminals and fraud attempts to access Canadians' bank accounts or credit. There are also continued reports of Ghostclick fraud victims in Canada.

Highlights

New Events reported to CCIRC:

- Client information for STRATFOR, a private US intelligence company, posted on the Internet by a hacker group – clients include Canadian federal and provincial employees
- Infection reports in computer systems of provincial government, financial, transportation, and education sector organizations
- Fraudsters impersonating Canadian banks, enticing Internet users to reveal personal information and financial credentials
- An Internet and webhosting service provider's website vandalized by hackers

Updates:

- Ghostclick fraud notifications continue – 19,000 hosts in Canada remain infected

CCIRC Products Released this week: None

Noteworthy News:

- Hackers impersonating U.S. Computer Emergency Response Team (US-CERT) targeting U.S. federal, state, and local governments, as well as many US private sector organizations
- Symantec's Norton AntiVirus source code exposed by hackers

NEW EVENTS REPORTED IN CANADIAN CRITICAL INFRASTRUCTURE

Federal Government Sector

(content to be supplied by CTEC)

Non-Federal Government Sector

STRATFOR hacking. CCIRC learned from law enforcement that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s report clients were posted on the Internet by a hacker group. STRATFOR is a US intelligence company. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have since been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident and will reach out to its stakeholders if they have been affected.

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure employee password and credit card information is secure. Employees whose names and corporate e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information or credentials. The release of physical addresses could also be of concern to certain clients for privacy and security reasons. STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information.*

Credential stealing malicious software infections. CCIRC received reports indicating computers of two provinces' departments of education and two banks were infected with common malicious software (Torpig/Mebroot). This malicious software is typically used by cyber criminals to discover financial/banking credentials of computer users and is quite common. **CCIRC** reached out to contacts in those organizations and offered mitigation advice.

Comment: *The organizations in question were unaware they were infected until they were notified by CCIRC. It is critical the affected organizations remedy the situation as soon possible because the presence of these infections likely means the organization's anti-virus protection has been compromised and software patching may be disabled. This may have exposed the organization to other types of undetected malicious software. Organizations whose networks are open to the public or who regularly interact with the public online may be more susceptible to these types of common infections. It is recognized that on-going checking of infection reports and clean-up of these infections can be resource intensive.*

Fraud attempts in Financial Sector. CCIRC received reports from law enforcement that fraudsters impersonating prominent Canadian banks and a credit card company tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown how many computer users provided their credential to these fraudsters. The links in these e-mails led to websites hosted in United States, France and Spain.

CCIRC notified the financial institutions of these fraud attempts. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website vandalized. CCIRC observed that a website operated by an Internet and webhosting service provider in Manitoba was vandalized by hackers. CCIRC notified the service provider, who then applied a software patch and remedied the situation.

Comment: *Organizations should monitor their websites and be vigilant against website defacements. Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to vandalism may also be used to compromise the computers of that website's visitors.*

UPDATES:

Ghostclick Fraud. There were new reports of infected computers in a provincial government, an airport authority and four Canadian universities attributed to Operation Ghostclick. This worldwide fraud campaign, exposed in late 2011 by the FBI, hijacked Internet web searches and diverted users from legitimate websites to websites that generated advertising and sales revenue for a criminal cyber ring. Computers across multiple sectors, in organizations large and small, and those belonging to the general public have been affected.

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to monitor the situation. As new reports come in, CCIRC will continue to reach out to affected partner organizations.

Comment: *According to reports received, CCIRC estimates there are still about 19,000 hosts in Canada where mitigation measures haven't been taken. These computers could lose their connection to the Internet on March 8, 2012, if their owners/operators do not take mitigation measures. Organizations should ensure they have taken the mitigation measures outlined in CCIRC's Information Note. It should be noted many of the reported infections are on computers of ordinary Canadians that connect to the Internet via Service Providers. These Internet Service Providers receive information from CCIRC.*

NOTEWORTHY NEWS IN THE MEDIA:

Fraudsters posing as U.S. Cybersecurity organization. A number of U.S. officials as well as certain private sector organizations are receiving e-mails from fraudsters impersonating the U.S. Computer Emergency Readiness Team (US CERT). The true US CERT has issued a public alert about this phishing campaign. The impact of this event is unknown.

Comment: *Organizations should be vigilant with all incoming e-mails, even from supposedly trusted sources. Fraudulent e-mails like this are often used by fraudsters to install viruses when opened, or they entice users to enter their personal information for a seemingly legitimate purpose. This type of incident not only damages the US CERT's credibility with its stakeholders but also could suggest someone is targeting a sizable IT security community's information. Technical*

analysis of these e-mails by US CERT continues and pertinent information will likely be shared with international partners like CCIRC.

Symantec's Norton Antivirus source code exposed by hackers. A hacker group called "the Lords of Dharmaraja" claimed to have stolen Symantec source code and documentation from the servers of Indian intelligence agencies. Symantec publicly confirmed that a segment of its source code was accessed from a third party. Symantec stated "there are no indications that customer information was impacted or exposed at this time".

Comment: *Symantec's Norton Antivirus code is commonly used around the world to protect computer systems. The stolen source code is said to be for an older version of the Antivirus software, so organizations are advised to ensure their antivirus protections are up to date.*

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

NOTES

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Dvorkin, Corey

From: [redacted]
Sent: January-12-12 10:08 AM
To: DAVID.LEHMAN@forces.gc.ca; DONALD.NEILL@forces.gc.ca; serge.stang@forces.gc.ca; Dvorkin, Corey; [redacted]
Subject: Fwd: HOMELAND SECURITY UPDATE DEC 28 2011 - JAN 8, 2012
Attachments: 010912 CQ - House Cybersecurity Bill.docx; 010912 CQ - The Year of the Lone Wolf.docx; 010912 CQ - Where to Cut and Where to Spend.docx

Of note:

"DEC 29 - According to recent studies by university researchers and security companies, cars and trucks have become increasingly vulnerable to cyberattacks. One found that a car's computer controls could be remotely accessed through its Bluetooth, Wi-Fi or OnStar connections, potentially allowing terrorists to control the brakes of numerous cars simultaneously, corporate spies to eavesdrop on a motoring executive's phone calls, or thieves to electronically locate, break into and start cars they've targeted to steal."

By not having a car, I'm doing my part to defeat the terrorist. And Skynet.

>>> <Katie.Tolan@international.gc.ca> 1/9/2012 4:01 pm >>>

SUMMARY OF KEY ITEMS OF INTEREST:

I. PEOPLE: (1) Department of Homeland Security (DHS) Secretary Janet Napolitano held a change of command ceremony for US Customs and Border Patrol (CBP) DEC 30 , announcing that CBP Commissioner **Alan Bersin will be now hold the position of Assistant Secretary for International Affairs in the Office of Policy at DHS. Deputy CBP Commissioner David Aguilar stepped up to become acting CBP Commissioner** and **Thomas Winkowski**, Assistant Commissioner of Field Operations, **became acting Deputy Commissioner**. Mr. Bersin had served as International Affairs Assistant Secretary for almost a year, when in March 2010 he accepted a recess appointment valid through DEC 31, 2011 from President Barack Obama to become Commissioner of CBP (note - the title at that time was Assistant Secretary for International Affairs and Special Representative for Border Affairs). During the change of command ceremony, **Secretary Napolitano signalled that in holding the Assistant Secretary position Mr. Bersin will oversee the department's international engagement, leading the strategic development and execution of DHS international plans and policies and forging new partnerships with foreign governments and international organizations.** The Secretary noted that this is the Department's "chief diplomatic officer" (See DHS for related links).

(2) The Assistant Attorney General for the Office of Justice Programs (OJP), **Laurie Robinson,** announced JAN 3 that she would be leaving her position at the end of February. Assistant Attorney General Robinson was confirmed by the Senate in November, 2009. **Principal Deputy Assistant Attorney General Mary Lou Leary will serve as acting assistant attorney general** following Robinson's departure. (See DOJ for related link)

II. BUREAU OF COUNTERTERRORISM: The **Department of State (DOS) announced the establishment of the Bureau of Counterterrorism JAN 4,** fulfilling one of the key recommendations of the Quadrennial Diplomacy and Development Review concluded in December 2010. The Bureau of Counterterrorism will lead the Department's engagement in support of U.S. government efforts to counter terrorism abroad and to secure the United States against foreign terrorist threats. The new Bureau will assume

the responsibilities of the Office of the Coordinator for Counterterrorism. The Fact Sheet released noted that the United States faces a continuing terrorist threat from al-Qaida and other groups and individuals who subscribe to violent extremism. While good progress has been made in combating terrorism since the 9/11 attacks, challenges remain. Together with defense, intelligence, law enforcement, and homeland security, diplomacy and development are critical to keeping America safe. To secure the future, there is a need to continue to strengthen the international coalition against terrorism, build foreign partner capacity to mitigate terrorist threats, reinforce resilience against attacks, and counter the ideologies and ideas that fuel violent extremism around the world. **The Bureau of Counterterrorism will implement its mission by:**

• **Developing and implementing counterterrorism strategies, policies, and operations:** The U.S. government has no greater responsibility than to protect the American people. The Bureau of Counterterrorism will play an integral role in meeting this obligation by leading the Department's engagement to develop and implement counterterrorism strategies, policies, and operations to disrupt and defeat the networks that support terrorism. The Bureau will work to safeguard American security interests while promoting U.S. values, including support for human rights, democracy, and the rule of law.

• **Strengthening counterterrorism diplomacy:** Strengthening existing partnerships and building new relationships is a cornerstone of U.S. counterterrorism policy. The Bureau of Counterterrorism will engage with bilateral partners, regional organizations, and the United Nations to broaden and deepen counterterrorism cooperation. **In one of many initiatives, the Bureau will lead U.S. government efforts on behalf of the State Department to support the Global Counterterrorism Forum,** a new multilateral initiative focused on setting the international counterterrorism agenda for the 21st century.

• **Strengthening homeland security:** Securing the homeland from external terrorist threats is central to U.S. foreign policy. The Bureau of Counterterrorism will be the principal State Department link with the Department of Homeland Security on counterterrorism strategy and operations. The Bureau will work in partnership with DHS, as well as other agencies and bureaus, to strengthen international cooperation on a wide range of homeland security issues including transportation security, the interdiction of terrorist travel, and critical infrastructure protection.

• **Countering violent extremism:** To defeat terrorists, there is a need to undermine their ability to recruit. The Bureau of Counterterrorism will focus the State Department in U.S. government efforts to counter violent extremism, thereby reducing radicalization and mobilization abroad. The Bureau will work to delegitimize the violent extremist narrative, to develop positive alternatives for populations vulnerable to recruitment, and to build partner government and civil society capacity to counter violent extremism themselves.

• **Building the capacity of foreign partners:** The security of the United States depends on the strength of its partners and allies abroad. With capable partners who are able to manage the threats within their borders and regions, the likelihood of U.S. forces being called into action is greatly reduced. The Bureau of Counterterrorism will work with other bureau and agency partners in supporting U.S. government work to build international partner counterterrorism capacity in the civilian sector and will contribute to efforts in the military and defense sectors. (See DOS Section for related link)

THIS WEEK IN WSHDC:

JAN 9: An American man is reported to have been sentenced to death in Iran after a court there convicted him of working for the CIA and going to the Persian nation to spy. The family of Amir Mirzaei Hekmati, a 28-year-old former U.S. Marine, says he was in Iran to visit his grandmothers. According to Iran's state-run Press TV, "the verdict was issued by Tehran's Revolution Court on JAN 9 after the defendant was found guilty of collaboration with the US government and its intelligence agency, the CIA, against the Islamic Republic of Iran." The Associated Press reports that Hekmati was born in Arizona, graduated from high school in

Michigan and was an Arabic translator while in the Marines. The wire service adds that "his family is of Iranian origin. His father, a professor at a community college in Flint, Mich., has said his son is not a CIA spy and was visiting his grandmothers in Iran when he was arrested." Iran Sentences American To Death In Spy Case

JAN 4 - A New Mexico sheriff said a retired Sandia Labs scientist was apparently building bombs at his home before he died. Torrance County Sheriff Heath White tells KOB-TV it appears 81-year-old David O'Keefe spent his retirement on the outskirts of Estancia continuing his work up until he died a few months ago. White says O'Keefe was trying to make a new type of explosive and was experimenting with different chemicals and different compounds to make that explosive, which put neighbors within a half mile in great danger. Deputies discovered the explosives Saturday when the property owner went to check on the home and found the chemicals. White says cleanup will take some time. Article

JAN 4 - Police departments across the country are looking into a startling statistic. For the last two years the number of officers killed in the line of duty has jumped. Local officers say the threat of violence is present at every call they respond to and they say it's not easy knowing 177 fellow officers were killed this past year. Article

JAN 4 - Health researchers and wildlife biologists say the number of infectious diseases that have jumped the boundary from animals to humans and between animal species is on the rise. Scientists believe the increase may be a result of more frequent contact between humans and wild animals, as well as the growing trade in wild animals, both legal and illegal. Article

JAN 3 - China-based hackers for months have been targeting federal agencies and contractors through infected emails apparently to spy on the Pentagon's drone strategy and other intelligence matters, according to Internet security researchers. The reported espionage employed a tactic known as spear-phishing where infiltrators, operating under the guise of a legitimate sender, email specific victims a virus-laden file or link. In this case, the hackers used email addresses from military and other government organizations, Jaime Blasco, manager of AlienVault Labs, said JAN 3 Article

JAN 1 - International hacker group Anonymous claims responsibility for hacking and releasing information about members of the California State-wide Law Enforcement Association union. Anonymous released the names, addresses and phone numbers of members; plus, credit card information taken from the association's online gift store was posted. The information dump was called "pr0j3ct m4hy3m". Article

DEC 29 - According to recent studies by university researchers and security companies, cars and trucks have become increasingly vulnerable to cyberattacks. One found that a car's computer controls could be remotely accessed through its Bluetooth, Wi-Fi or OnStar connections, potentially allowing terrorists to control the brakes of numerous cars simultaneously, corporate spies to eavesdrop on a motoring executive's phone calls, or thieves to electronically locate, break into and start cars they've targeted to steal. Article

DEC 28 - It's a case of drug dealing, international money laundering and funneling money to a known terrorist group, Hezbollah. And there's a Georgia connection. 11Alive's Center for Investigative Action spent the day digging for clues as to how a local family has been caught up in it. The family ran a used car dealership out of Fairburn and is alleged to have made more than $1 million in profit by selling used cars that ended up being part of an elaborate money laundering scheme to fund Hezbollah in Lebanon. The family is not accused of anything illegal and is not charged with a crime, but the dealership is one of 30 that federal agents have moved in on over the last couple of weeks to recover money. It's all in a **75 page complaint filed by the US attorney** in Manhattan. Thirty used car dealers in the U.S. are caught up in it, including Fairburn's Baaklini North America, Inc., which is alleged to have made $1.4 million, possibly selling cars to help fund Hezbollah. Here's

how it's supposed to have gone down: Since 2007 about $300 million in Lebanese drug money was reportedly funneled through financial institutions in North America. The money went to buy used cars in the U.S., which were then shipped to West Africa and sold. The laundered money was alleged to have been smuggled back to Lebanon. Article

WHITE HOUSE:

JAN 7: President Obama shares his New Year's resolution: doing whatever it takes to move the economy forward and ensure that middle class families regain the security they've lost in the last decade. http://www.whitehouse.gov/blog

JAN 5 - President Obama traveled to the Pentagon to discuss a major shift in the nation's strategic military objectives -- with a goal of moving away from the expansive wars in Iraq and Afghanistan and toward a different posture that emphasizes a new focus for the future. Blog

JAN 4 - President Obama announced today his intent to recess appoint four individuals to fill key administration posts that have been left vacant: Richard Cordray, Director, Consumer Financial Protection Bureau; Sharon Block, Member, National Labor Relations Board; Terence F. Flynn, Member, National Labor Relations Board; and Richard Griffin, Member, National Labor Relations Board. Press Release

DEC 31 – President Obama signed into law H.R. 1540, the "National Defense Authorization Act for Fiscal Year 2012" which authorizes funding for the defense of the United States and its interests abroad, crucial services for service members and their families, and vital national security programs that must be renewed. Press Release

DHS:

JAN 6 : Underscoring the Obama Administration's commitment to family unity and administrative efficiency, this morning U.S. Citizenship and Immigration Services posted a Notice of Intent in the Federal Register to begin a regulatory change that would reduce the amount of time that U.S. citizens are separated from their families while their family members go through the process of becoming legal residents of the United States. USCIS Proposes Regulatory Change to Decrease the Time U.S. Citizens are Separated from Family Members who are Legally Immigrating to the U.S.

DEC 30 - DHS Secretary Janet Napolitano held a change of command ceremony for US CBP, announcing that CBP Commissioner Alan Bersin has returned to the position of assistant secretary for international affairs in the policy shop at the DHS. Deputy CBP Commissioner David Aguilar stepped up to become acting CBP commissioner and Thomas Winkowski, assistant commissioner of Field Operations, became acting deputy commissioner. Bersin served as international affairs assistant secretary for almost a year, when in April 2010 he accepted a recess appointment good through Dec. 31 from President Barack Obama to become CBP chief. Remarks http://www.dhs.gov/xabout/structure/bio_1269973987071.shtm http://www.dhs.gov/ynews/releases/pr_1239820176123.shtm

DEC 29 – DHS announced a new partnership between DHS' "If You See Something, Say Something™" public awareness campaign and the National Hockey League (NHL) - highlighting the Department's continued partnership with the sports industry to ensure the safety and security of employees, players and fans. Press Release

DEC 28 - DHS officials were among the first to discover that the Public Advocate's Office website was hacked over Christmas weekend. The federal Multi-State Information Sharing and Analysis Center notified the city's tech department about the cyberattack in which data about thousands of users was stolen. Article

DEC 28 - Many prisons and jails use SCADA (Supervisory Control And Data Acquisition) systems with Programmable Logic Controllers (PLCs) to open and close doors. Researchers discovered significant vulnerabilities in PLCs used in correctional facilities and were able to remotely flip the switches to "open" or "locked closed" on cell doors and gates. Article

DEC 28 – FEMA mailed out 83,000 debt notices this years seeking to recover more than $385 million it says was improperly paid to victims of hurricanes Katrina, Rita and Wilma. The debts, which average about $4,622 per recipient, represent slightly less than 5 percent of the roughly $8 billion that FEMA distributed after the storms. At least some of the overpayments were due to FEMA employees' own mistakes, ranging from clerical errors to failing to interview applicants, according to congressional testimony. Article

CBP:

JAN 4 - The U.S. Customs and Border Protection agency is disputing the assertion that a Canadian man gained entry into the U.S. by only using a scanned photo of his passport on his iPad. Agency spokeswoman Jenny Burke said scanned documents are not accepted. She says if an individual does not have a passport, an enhanced driver's license or an expedited travel pass the border officer must determine identity and citizenship using a variety of other means, or deny entry. Burke says Reisch had both a driver's license and birth certificate. Article

DEC 29 - Federal law enforcement authorities are rapidly expanding a military-style unmanned aerial reconnaissance operation along the US-Mexico border. Eight Predators fly for the Customs and Border Protection agency — five, and soon to be six, along the southwestern border. Drones now patrol most of the southern boundary, from Yuma, Arizona, to Brownsville, Texas. Planning documents for the CBP envision as many as 24 Predators and their maritime variants in the air by 2016, giving the agency the ability to deploy a drone anywhere over the continental United States within three hours. Article

ICE:

JAN 5 – DOJ's most recent Summary of Major U.S. Export Enforcement Prosecutions cited that more than 74 percent of the government's most significant counter-proliferation investigation prosecutions were either led by ICE or had a significant contribution from ICE HSI agents. Press Release

DEC 29 - ICE announced new measures to ensure that individuals being held by state or local law enforcement on immigration detainers are properly notified about their potential removal from the country and are made aware of their rights. The new measures include a new detainer form and the launch of a toll-free hotline. Press Release

TSA:

JAN 5 – The TSA has found 1,200 guns, snakes, C4 explosives and inert landmines in the past year at airport checkpoints around the country. TSA has compiled a list of their top 10 good catches of 2011. Press Release

DEC 29 - Although overall appropriations for the DHS are down slightly this year from Fiscal Year (FY) 2011, the TSA received about $7.85 billion, up $153 million from 2011. Article

DOS:

JAN 4 - The U.S. State Department announced JAN 4, the elevation of its counterterrorism office to a full-scale bureau. The mission of the new bureau will be to lead the Department in the U.S. Government's effort to counter terrorism abroad and to secure the United States against foreign terrorist threats. The bureau will have a number of concrete responsibilities. In coordination with Department leadership, the National Security Staff, and U.S. Government agencies, other U.S. Government agencies, it will develop and implement counterterrorism strategies, policies, operations, and programs to disrupt and defeat the networks that support terrorism. The bureau will lead in supporting U.S. counterterrorism diplomacy and seek to strengthen homeland security, countering violent extremism, and build the capacity of partner nations to deal effectively with terrorism. Briefing; State Department Fact Sheet: New Bureau of Counterterrorism

DOJ

JAN 3 - The Assistant Attorney General for the Office of Justice Programs (OJP), Laurie Robinson, announced y that she would be leaving her position at the end of February. Assistant Attorney General Robinson was confirmed by the Senate in November, 2009. Principal Deputy Assistant Attorney General Mary Lou Leary will serve as acting assistant attorney general following Robinson's departure. Press Release

FBI:

JAN 4 - U.S. Attorney William J. Hochul, Jr. announced today that Minnetta Walker, 44, of Buffalo, N.Y., who was convicted of conspiracy to defraud the United States, was sentenced to 24 months in prison, to be followed by one year supervised released. Ms. Walker while on official duty with the TSA, assisted certain individuals in bypassing the normal security procedures, measures, and requirements at the Buffalo Airport. Press Release

JAN 4 - Trey Scott Atwater, of Hope Mills, N.C., was arrested DEC 24 while trying to go through security at an airport in Texas where he was planning to fly back home. Authorities say the 30-year-old had a carry-on bag containing C4, a powerful explosive used in Iraq and Afghanistan to blow the hinges off doors or destroy unexploded ordinance. Atwater was detained at the Fayetteville, N.C., airport on Dec. 24 when security agents found a military smoke grenade in his carry-on bag. Article

JAN 3 - Three people reported falling ill JAN 3 after exposure to a suspicious powder in the mail room of the state attorney's office in West Palm Beach, Florida, a city spokesman said. Article

JAN 2 - The FBI Seattle Division joined the National Park Service (NPS) in announcing the end to the multi-agency manhunt for the subject suspected of killing Ranger Margaret Anderson on January 1, 2012 in Mount Rainier National Park. FBI, NPS, and PCSD officials confirmed that the suspect, Benjamin Barnes, was found dead. Press Release

ODNI:

JAN 4 - Statement by Director of National Intelligence James R. Clapper on the signing of the Intelligence Authorization Act for fiscal year 2012. Statement

AFGHANISTAN/PAKISTAN WAR:

JAN 6 - Husain Haqqani, Pakistan's embattled former ambassador to Washington, fears he will be murdered if he leaves his sanctuary in the official residence of the country's Prime Minister Yusuf Raza Gilani. Article

JAN 5 - The Afghan government said JAN 5 that it was shutting down the operations of one of the largest foreign security companies operating in the country after detaining two of its contractors on suspicion of gun smuggling. After months of growing tension between the government and foreign security contractors, the decision marks a sharp escalation into public action by the Afghan authorities. President Hamid Karzai is in the midst of replacing foreign security contractors with Afghan guards. The Interior Ministry said it was immediately withdrawing the company's license, although the company, GardaWorld, a private Canadian security outfit, said it was in discussions with the government and hoped to be able to continue to operate. The Interior Ministry said that the contractors, two Britons, who were detained on JAN 3 after being found with an arsenal of unlicensed AK-47 assault rifles in their sport utility vehicle, were among the 341 Afghan guards and 35 foreign contractors employed by GardaWorld in Afghanistan. Article

JAN 5 - Afghanistan President Hamid Karzai is demanding that the U.S. detention center at Bagram Air Base be handed over to Afghan control within a month. Article

JAN 3 - The Afghan Taliban said JAN3 they have reached a preliminary agreement to set up a political office in the Gulf nation of Qatar, and asked for the release of prisoners held at the U.S. military prison in Guantanamo Bay. Article

JAN 3 - The United States will support Afghan-led efforts to reach a negotiated end to the war with the Taliban, including a possible Taliban political office in the Gulf state of Qatar if that is agreed by all sides, the U.S. State Department said on JAN 3. Article

JAN 2 - Pakistani Taliban factions and their allies have set up a council of elders in hopes of coordinating efforts against NATO troops in Afghanistan, a spokesman said. Article

JAN 2 - Afghanistan's national power company says it will cut the electricity supply to the main prison unless it pays its overdue bills in the next few weeks. It says it is contemplating similar action against several government departments which have also failed to pay bills. It estimates it is owed approximately $40m. Article

JAN 2 - In what could be the biggest change in a decade in a relationship that has been a mainstay of U.S. military and counterterrorism policy since the 9/11 terror attacks, the United States and Pakistan are lowering expectations for what the two nations will do together and planning for a period of more limited contact. Article

GAO:

JAN 6 – GAO released its report concerning the US Coast Guard finding that continued improvements were needed to address potential barriers to equal employment opportunity. Report

CONGRESS:

Note: Congress is currently in recess. The 2nd Session of the 112th Congress will convene on January 17, 2012. Announcement

JAN 3 – For a business community looking for any sign that the federal government is taking action on cybersecurity, a recent information-sharing bill from the House Intelligence Committee looks like a promising start, according to officials from the computer security firm McAfee. The measure (HR 3523), which the panel approved in early December, has attracted support from groups such as the U.S. Chamber of Commerce and the National Cable and Telecommunications Association. McAfee also has endorsed the measure. While some in the private sector have concerns about the legislation, it has received mostly positive reviews among industry leaders said Tom Gann, McAfee's vice president of government relations, and Phyllis Schneck, vice president and chief technology officer for the firm's global public sector. The officials told CQ that the bill represents a critical first step in establishing information-sharing relationships that will allow companies to better protect themselves and their customers. (See attached for CQ Article)

DEC 30 - The Disaster Relief Fund (DRF) administered by the Federal Emergency Management Agency (FEMA) received appropriations at the full level requested by FEMA for Fiscal Year (FY) 2012 through two spending bills signed by President Barack Obama last week -- the Consolidated Appropriations Act (Public Law 112-074) and the Disaster Relief Appropriations Act (PL 112-077). President Obama signed the bills into law on Dec. 23, funding the DRF with $700 million in the consolidated spending act and another $6.4 billion in the disaster relief legislation. Article

UPCOMING HEARINGS:

Nothing to report. Both house are in recess although the Senate has been meeting sporadically. The 2nd Session of the 112th Congress will convene on January 17, 2012.

THINK TANKS:

JAN 6: Successful Exercise Demonstrates Implementation of Nuclear Detection Architecture
http://blog.dhs.gov/

JAN 6 – Centre for Strategic and International Studies hosted a discussion of "The Al Qaeda Factor: Plots Against the West", a new book from Mitchell D. Silber, Director of Intelligence Analysis, Analytic and Cyber Units, New York City Police Department. The Al Qaeda Factor: Plots Against the West

JAN 5 – The Council on Foreign Relations published an interview with Michael Elleman, Senior Fellow for Regional Security Cooperation, International Institute for Strategic Studies on "How Serious are Iran's Threats?" Interview

JAN 5 – The Center for American Progress published an article by Ken Sofer and Jennifer Addison

"The Unaddressed Threat of Female Suicide Bombers - Women Terrorists an Increasingly a Problem" discussing why we need to acknowledge the growing number of female attacks in our counterterrorism strategy. Article

UPCOMING EVENTS:

JAN 10: The Centre for Strategic and International Studies will host: "The Future of the Internet – Who Decides?" 15:30-17:000 1800 K Street, N.W.

ARTICLES/ REPORTS OF INTEREST:

JAN 4: A Whole Community Approach to Emergency Management - **Posted by: David Kaufman, Director, Office of Policy and Program Analysis - FEMA Blog**

JAN 3 – Homeland Security Experts Weigh In: Where to Cut and Where to Spend. See attached for CQ Article)

JAN 2 - President Obama Signed The National Defense Authorization Act - Now What? Forbes. Article

JAN 2 - Homeland Security Experts Weigh In: The Year of the 'Lone Wolf'. (See attached for CQ Article)

DEC 29 - Terrorists Struggle To Gain Recruits On The Web. NPR. Article

Kathleen Tolan
Counsellor
Public Safety and Border Security
Public Safety Canada
501 Pennsylvania Avenue, N.W.
Washington, D.C. 20001-2114
Tel: (202) 448-6338 Cell: 202 497-5898
Fax: (202) 682-7792
Email: katie.tolan@international.gc.ca

Williston, Sandra

From: Dincoy, Rana
Sent: January-12-12 10:30 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce; Anderson, Windy
Subject: RE: Confirming the incident write-ups for the Weekly Summary

Hi Luc, thanks for your comments and suggestions. You have a valid point about using the reports CCIRC receives to pull out some numbers to sketch out a picture of the cyber ecosystem. We in the strategic unit have talked about this previously and decided it would be appropriate to put them in a monthly product that would talk more about trends. We also have some work to do in terms of evaluating how meaningful these numbers would be for situational awareness and putting the right context around them for non-technical senior managers. We will also need some technical help with the analysis of that data. For example, in the next update of the Notification tool, an automatic counter and categorization by CI sector would be helpful.

As for the DNS Changer: I was under the impression you were in contact with US authorities on this matter and thought it was the CERT. If that's not true I'll remove it.

As requested, I will no longer copy the cyberdo in my e-mails for the Weekly Summary.

Thanks again for your comments and getting back to me so quickly... One of my challenges in writing this product is striking the balance between technical accuracy and clarity for non-technical readers... It's like the holy grail!

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

From: Beaudoin, Luc S
Sent: January-11-12 7:41 PM
To: Dincoy, Rana
Cc: Moore, Bruce; Anderson, Windy
Subject: Re: Confirming the incident write-ups for the Weekly Summary

Rana, I would appreciate if you addressed your questions to me, as stated before. Bruce and the other IH are busy doing their tactical job and should not be disrupted unless a new operational matter comes to your attention and I am not around. Strategic reports review is not their role.

There are fundamentals in these reports which are in my opinion inaccurate. These subtilties are important.

1) Item 1 is stratfort. It is public, so just say their name. They are not an "agency", they are a company. Go on wikipedia for more info.

2) Malicious email and threat actor refer usually to malware and state sponsored. Use Phishing or scam email and cyber criminals instead.

3) Don t state "potential compromise of povincial computer systems". Rather state "limited number of computer systems in Canadian Critical Infrastucture organisations potentially affected by known botnets malicious codes.

4) A website provider...replace by: a canadian internet and webhosting service provider website defaced by cyber vandals.

5) First note: typo (repeated "been" twice. Remove yellow section. State CCIRC data sources have consistently proven to be of high accuracy.

6) Not sure what US CERT has to do with DNSChanger. Remove.

7) CI finance: bank phishing does not lead to compromise. It entice users to enter PII by luring them to fake bank site (copies)

8) Comment on ISP vandalized: BEAUTIFUL !!!!

9) Stratfor: name it. [redacted] Otherwise, phishing emails have been reported so far focussed at embarassing the stratfort organisation. No malware was reported in phishing cases at this time. Stratfort posted public information and a video about the breach as well as contacted all its clients offering them 1 year privacy protection services from a 3rd party.

10) Why are we still not stating metrics like: total and average number of canadian infected hosts per day [redacted] number of canadian host still infected by ghostclick [redacted] who will loose connection to internet on the 8 Mar, number of canadian malicious sites in sandbox reports and [redacted], Arbor networks canadian ranking, trends in these values, number of reported canadian banking phishing sites reported... Why ? These are more meaningfull SA for canada.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: Dincoy, Rana
Sent: Wednesday, January 11, 2012 11:45 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce
Subject: Confirming the incident write-ups for the Weekly Summary

Hi Luc,

Can you please confirm the below? I've spoken with Bruce to obtain clarification where I needed it (Bruce please let me know if something isn't right).

I want to make sure particularly that I am not overstating things in my "Comments" section. I'd appreciate your feedback by tomorrow morning... Thanks! Rana

For the Week of 31 Dec 2011 – 6 Jan 2012

Issued: 12 Jan 2012

HIGHLIGHTS:

Notable Incidents:

- Client information for a private US intelligence agency posted on the Internet by Anonymous – clients include Canadians
- Malicious e-mails from threat actors impersonating Canadian banks, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems of provincial government, financial, transportation, and education sector organizations
- A website hosting service provider's website vandalized by hackers

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

NOTABLE INCIDENTS– 31 DECEMBER 2011 THROUGH 6 JANUARY 2012:

Canadian Critical Infrastructure:

Provincial Government, Transportation and Education: Computers of two provinces' departments of education, an airport authority and four universities may have been compromised by certain common malicious software. There were also reports of compromised computers as a result of the worldwide internet fraud "Ghostclick", which the FBI exposed in late 2011.

CCIRC notified contacts in those organizations of these potential compromises and offered mitigation advice. Impact of the compromises is unknown but could potentially include data theft or remote use of these computers to commit malicious acts on the Internet. In the "Ghostclick" fraud, computer users were unknowingly re-directed to certain webpages, which financially benefited the fraudsters.

Comment: Open source computer infection reports indicate which organizations appear to be infected with certain commonly found malicious software. However, only the affected organization can confirm whether their computers have been truly been infected and the impact. While there hasn't been any such confirmation in this situation, CCIRC believes it likely that there were compromises.

CCIRC continues to notify stakeholder organizations that were impacted by the worldwide Ghostclick fraud and is in contact with US CERT.

Financial Sector. Threat actors impersonating prominent Canadian banks tried to compromise computer users' machines by persuading them to click on malicious links in an e-mail. CCIRC notified these institutions, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be identified as such, warning future unsuspecting users. The malicious links led to websites hosted in United States, France and Spain.

Telecommunication Sector. CCIRC observed that a website operated by an internet hosting service provider was vandalized by hackers. The impact is unknown.

Comment: Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website that can be vandalized by hackers is also vulnerable to being used to compromise the computers of that website's visitors.

International:

Anonymous, the famed hacker group, released personal and credit card information of a private US intelligence company's clients, on the Internet. These include Canadian clients. CCIRC notified the Canadian stakeholders and offered mitigation advice. CCIRC continues to analyze the situation.

Comment: The personal information released includes names and e-mail addresses, which can be used for a variety of malicious purposes by any threat actor. This can include sending malicious e-mails to those clients to compromise their computers or using the credit card information for financial gain. The release of physical addresses could be of concern to certain clients for privacy and security reasons.

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

Klassen, Nathan

From: Klassen, Nathan
Sent: January-12-12 1:14 PM
To: Cameron, Bud
Subject: RE: Confirming the incident write-ups for the Weekly Summary

Txs Bud – [redacted] Cheers,

Nate
Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

From: Cameron, Bud
Sent: January-12-12 10:07 AM
To: Klassen, Nathan
Subject: FW: Confirming the incident write-ups for the Weekly Summary

Note the suggestions for stats at the end.
Bud

From: Dincoy, Rana
Sent: January-12-12 10:03 AM
To: Bendelier, Kenneth
Cc: Cameron, Bud
Subject: FW: Confirming the incident write-ups for the Weekly Summary

FYI – I intend to respond to this e-mail. Some good suggestions (though harshly delivered in some cases!), some others that may be technically more accurate but completely obscure the meaning for senior managers....

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

From: Beaudoin, Luc S
Sent: January-11-12 7:41 PM
To: Dincoy, Rana
Cc: Moore, Bruce; Anderson, Windy
Subject: Re: Confirming the incident write-ups for the Weekly Summary

Rana, I would appreciate if you addressed your questions to me, as stated before. Bruce and the other IH are busy doing their tactical job and should not be disrupted unless a new operational matter comes to your attention and I am not around. Strategic reports review is not their role.

There are fundamentals in these reports which are in my opinion inaccurate. These subtilties are important.

1) Item 1 is stratfort. It is public, so just say their name. They are not an "agency", they are a company. Go on wikipedia

for more info.

2) Malicious email and threat actor refer usually to malware and state sponsored. Use Phishing or scam email and cyber criminals instead.

3) Don t state "potential compromise of povincial computer systems". Rather state "limited number of computer systems in Canadian Critical Infrastucture organisations potentially affected by known botnets malicious codes.

4) A website provider...replace by: a canadian internet and webhosting service provider website defaced by cyber vandals.

5) First note: typo (repeated "been" twice. Remove yellow section. State CCIRC data sources have consistently proven to be of high accuracy.

6) Not sure what US CERT has to do with DNSChanger. Remove.

7) CI finance: bank phishing does not lead to compromise. It entice users to enter PII by luring them to fake bank site (copies)

8) Comment on ISP vandalized: BEAUTIFUL !!!!

9) Stratfor: name it. Mention the concern remains that these be used in targeted attacks by (yes) threat actors. Otherwise, phishing emails have been reported so far focussed at embarassing the stratfort organisation. No malware was reported in phishing cases at this time. Stratfort posted public information and a video about the breach as well as contacted all its clients offering them 1 year privacy protection services from a 3rd party.

10) Why are we still not stating metrics like: total and average number of canadian infected hosts per day , number of canadian host still infected by ghostclick who will loose connection to internet on the 8 Mar, number of canadian malicious sites in sandbox reports and , Arbor networks canadian ranking, trends in these values, number of reported canadian banking phishing sites reported... Why ? These are more meaningfull SA for canada.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: Dincoy, Rana
Sent: Wednesday, January 11, 2012 11:45 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce
Subject: Confirming the incident write-ups for the Weekly Summary

Hi Luc,

Can you please confirm the below? I've spoken with Bruce to obtain clarification where I needed it (Bruce please let me know if something isn't right).

I want to make sure particularly that I am not overstating things in my "Comments" section. I'd appreciate your feedback by tomorrow morning... Thanks! Rana

For the Week of 31 Dec 2011 – 6 Jan 2012

Issued: 12 Jan 2012

HIGHLIGHTS:

Notable Incidents:

- Client information for a private US intelligence agency posted on the Internet by Anonymous – clients include Canadians
- Malicious e-mails from threat actors impersonating Canadian banks, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems of provincial government, financial, transportation, and education sector organizations
- A website hosting service provider's website vandalized by hackers

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

NOTABLE INCIDENTS– 31 DECEMBER 2011 THROUGH 6 JANUARY 2012:

Canadian Critical Infrastructure:

Provincial Government, Transportation and Education: Computers of two provinces' departments of education, an airport authority and four universities may have been compromised by certain common malicious software. There were also reports of compromised computers as a result of the worldwide internet fraud "Ghostclick", which the FBI exposed in late 2011.

CCIRC notified contacts in those organizations of these potential compromises and offered mitigation advice. Impact of the compromises is unknown but could potentially include data theft or remote use of these computers to commit malicious acts on the Internet. In the "Ghostclick" fraud, computer users were unknowingly re-directed to certain webpages, which financially benefited the fraudsters.

Comment: Open source computer infection reports indicate which organizations appear to be infected with certain commonly found malicious software. However, only the affected organization can confirm whether their computers have been truly been infected and the impact. While there hasn't been any such confirmation in this situation, CCIRC believes it likely that there were compromises.

CCIRC continues to notify stakeholder organizations that were impacted by the worldwide Ghostclick fraud and is in contact with US CERT.

Financial Sector. Threat actors impersonating prominent Canadian banks tried to compromise computer users' machines by persuading them to click on malicious links in an e-mail. CCIRC notified these institutions, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be identified as such, warning future unsuspecting users. The malicious links led to websites hosted in United States, France and Spain.

Telecommunication Sector. CCIRC observed that a website operated by an internet hosting service provider was vandalized by hackers. The impact is unknown.

Comment: Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website that can be vandalized by hackers is also vulnerable to being used to compromise the computers of that website's visitors.

International:

Anonymous, the famed hacker group, released personal and credit card information of a private US intelligence company's clients, on the Internet. These include Canadian clients. CCIRC notified the Canadian stakeholders and offered mitigation advice. CCIRC continues to analyze the situation.

Comment: The personal information released includes names and e-mail addresses, which can be used for a variety of malicious purposes by any threat actor. This can include sending malicious e-mails to those clients to compromise their computers or using the credit card information for financial gain. The release of physical addresses could be of concern to certain clients for privacy and security reasons.

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

Dincoy, Rana

From: Dincoy, Rana
Sent: January-12-12 10:38 AM
To: Bendelier, Kenneth
Cc: Cameron, Bud
Subject: FW: Confirming the incident write-ups for the Weekly Summary

Sent this out before getting your message. You can certainly expand on it with the measures question...

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

From: Dincoy, Rana
Sent: January-12-12 10:30 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce; Anderson, Windy
Subject: RE: Confirming the incident write-ups for the Weekly Summary

Hi Luc, thanks for your comments and suggestions. You have a valid point about using the reports CCIRC receives to pull out some numbers to sketch out a picture of the cyber ecosystem. We in the strategic unit have talked about this previously and decided it would be appropriate to put them in a monthly product that would talk more about trends. We also have some work to do in terms of evaluating how meaningful these numbers would be for situational awareness and putting the right context around them for non-technical senior managers. We will also need some technical help with the analysis of that data. For example, in the next update of the Notification tool, an automatic counter and categorization by CI sector would be helpful.

As for the DNS Changer: I was under the impression you were in contact with US authorities on this matter and thought it was the CERT. If that's not true I'll remove it.

As requested, I will no longer copy the cyberdo in my e-mails for the Weekly Summary.

Thanks again for your comments and getting back to me so quickly... One of my challenges in writing this product is striking the balance between technical accuracy and clarity for non-technical readers... It's like the holy grail!

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

From: Beaudoin, Luc S
Sent: January-11-12 7:41 PM
To: Dincoy, Rana
Cc: Moore, Bruce; Anderson, Windy
Subject: Re: Confirming the incident write-ups for the Weekly Summary

Rana, I would appreciate if you addressed your questions to me, as stated before. Bruce and the other IH are busy doing their tactical job and should not be disrupted unless a new operational matter comes to your attention and I am not around. Strategic reports review is not their role.

There are fundamentals in these reports which are in my opinion inaccurate. These subtilties are important.

1) Item 1 is stratfort. It is public, so just say their name. They are not an "agency", they are a company. Go on wikipedia for more info.

2) Malicious email and threat actor refer usually to malware and state sponsored. Use Phishing or scam email and cyber criminals instead.

3) Don t state "potential compromise of povincial computer systems". Rather state "limited number of computer systems in Canadian Critical Infrastucture organisations potentially affected by known botnets malicious codes.

4) A website provider...replace by: a canadian internet and webhosting service provider website defaced by cyber vandals.

5) First note: typo (repeated "been" twice. Remove yellow section. State CCIRC data sources have consistently proven to be of high accuracy.

6) Not sure what US CERT has to do with DNSChanger. Remove.

7) CI finance: bank phishing does not lead to compromise. It entice users to enter PII by luring them to fake bank site (copies)

8) Comment on ISP vandalized: BEAUTIFUL !!!!

9) Stratfor: name it. . Mention the concern remains that these be used in targeted attacks by (yes) threat actors. Otherwise, phishing emails have been reported so far focussed at embarassing the stratfort organisation. No malware was reported in phishing cases at this time. Stratfort posted public information and a video about the breach as well as contacted all its clients offering them 1 year privacy protection services from a 3rd party.

10) Why are we still not stating metrics like: total and average number of canadian infected hosts per day number of canadian host still infected by ghostclick who will loose connection to internet on the 8 Mar, number of canadian malicious sites in sandbox reports and , Arbor networks canadian ranking, trends in these values, number of reported canadian banking phishing sites reported... Why ? These are more meaningfull SA for canada.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: Dincoy, Rana
Sent: Wednesday, January 11, 2012 11:45 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce
Subject: Confirming the incident write-ups for the Weekly Summary

Hi Luc,

Can you please confirm the below? I've spoken with Bruce to obtain clarification where I needed it (Bruce please let me know if something isn't right).

I want to make sure particularly that I am not overstating things in my "Comments" section. I'd appreciate your feedback by tomorrow morning... Thanks! Rana

For the Week of 31 Dec 2011 – 6 Jan 2012

Issued: 12 Jan 2012

HIGHLIGHTS:

Notable Incidents:

- Client information for a private US intelligence agency posted on the Internet by Anonymous – clients include Canadians
- Malicious e-mails from threat actors impersonating Canadian banks, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems of provincial government, financial, transportation, and education sector organizations
- A website hosting service provider's website vandalized by hackers

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

NOTABLE INCIDENTS– 31 DECEMBER 2011 THROUGH 6 JANUARY 2012:

Canadian Critical Infrastructure:

Provincial Government, Transportation and Education: Computers of two provinces' departments of education, an airport authority and four universities may have been compromised by certain common malicious software. There were also reports of compromised computers as a result of the worldwide internet fraud "Ghostclick", which the FBI exposed in late 2011.

CCIRC notified contacts in those organizations of these potential compromises and offered mitigation advice. Impact of the compromises is unknown but could potentially include data theft or remote use of these computers to commit malicious acts on the Internet. In the "Ghostclick" fraud, computer users were unknowingly re-directed to certain webpages, which financially benefited the fraudsters.

Comment: Open source computer infection reports indicate which organizations appear to be infected with certain commonly found malicious software. However, only the affected organization can confirm whether their computers have been truly been infected and the impact. While there hasn't been any such confirmation in this situation, CCIRC believes it likely that there were compromises.

CCIRC continues to notify stakeholder organizations that were impacted by the worldwide Ghostclick fraud and is in contact with US CERT.

Financial Sector. Threat actors impersonating prominent Canadian banks tried to compromise computer users' machines by persuading them to click on malicious links in an e-mail. CCIRC notified these institutions, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be identified as such, warning future unsuspecting users. The malicious links led to websites hosted in United States, France and Spain.

Telecommunication Sector. CCIRC observed that a website operated by an internet hosting service provider was vandalized by hackers. The impact is unknown.

Comment: Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website that can be vandalized by hackers is also vulnerable to being used to compromise the computers of that website's visitors.

International:

Anonymous, the famed hacker group, released personal and credit card information of a private US intelligence company's clients, on the Internet. These include Canadian clients. CCIRC notified the Canadian stakeholders and offered mitigation advice. CCIRC continues to analyze the situation.

Comment: The personal information released includes names and e-mail addresses, which can be used for a variety of malicious purposes by any threat actor. This can include sending malicious e-mails to those clients to compromise their computers or using the credit card information for financial gain. The release of physical addresses could be of concern to certain clients for privacy and security reasons.

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

Anderson, Windy

From: Labelle, Sébastien
Sent: January-12-12 11:18 AM
To: Hatfield, Adam; Anderson, Windy
Subject: FW: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

As discussed yesterday. Sorry for the delay.

Sébastien Labelle
Director of National Cyber Security Engagement and Partnerships /
Directeur national de la Mobilisation et des partenariats pour la cyber sécurité
National Cyber Security Directorate / Direction générale de la Cyber sécurité nationale
Public Safety Canada / Sécurité publique Canada
Room / pièce 11C079, 340 Laurier, Ottawa, ON,
tel 613-990-2655 ; fax 613-990-3287; mob 613-614-5263
sebastien.labelle@ps-sp.gc.ca

From: Dick, Robert
Sent: January-10-12 8:46 AM
To: Matz, Mark
Cc: Gordon, Robert; Hatfield, Adam; Labelle, Sébastien
Subject: Fw: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Note article on Israeli official's categorization of cyber identiy theft as an act of terrorism. In the Israeli context, situating something in that realm rather than crime could have especially interesting ramifications, if it's true.

From: PSMediaCentre/CentredesmediasdeSP
Sent: Tuesday, January 10, 2012 08:36 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Baker, William V.; Black, Dave <dave.black@rcmp-grc.gc.ca>; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, [redacted]; Crépeault, David; CSIS Media Monitoring [redacted] CYBERDO; De Curtis, Laura; Dunn, John <JDunn@justice.gc.ca>; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica <Monica.Gilbert@ic.gc.ca>; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line <Line.Patry@ic.gc.ca>; Patton, Michael; RCMP Emerging Trends <emerging.trends@rcmp-grc.gc.ca>; Roberts, Shane; Robinson, N.; Salas, Anik <ASalas@justice.gc.ca>; Slade, Nancy <Nancy.Slade@ic.gc.ca>; Spendlove, Jim; Stanfield, Charles; Stewart, Christena <Christena.Stewart@ps-sp.gc.ca>; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl <Cheryl.Wadasinghe@ps-sp.gc.ca>; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 10, 2012/ le 10 janvier 2012

Print Media

Canning the spam
The federal government can't move soon enough on its spam reporting centre, dubbed the "Freezer," which is designed to crack down on the millions of unwanted messages clogging Canadians' cellphones, inboxes and social network accounts. Times Colonist, A10

Online Media

Obama defence plan details heightened global cyber danger
US president Barack Obama has spoken of the drastically heightened cyber threat facing nations around the world, as he announced major changes to the American defence strategy. As he appeared at the Pentagon last week to unveil the new defence strategy, Obama promised to focus closely on improving the technological capabilities of the US armed forces. "We will ensure that our military is agile, flexible and ready for the full range of contingencies," he said. PC Advisor UK

Cyber tension follows hacker attack on Israeli credit card users
Last week, a hacker published credit card information belonging to about 20,000 Israelis on the Internet, along with the personal details of hundreds of thousands more. Israeli credit card companies swiftly canceled the cards and pledged to reimburse customers for damages caused by fraudulent use. Los Angeles Times

Venezuela's Chavez Backs Diplomat Who Was Expelled by US
Venezuelan President Hugo Chavez Monday night backed the South American country's consul general in Miami, who was expelled by U.S. authorities over the weekend and was linked to an alleged plot to launch a cyber attack against the U.S. government. Wall Street Journal

Israeli Official Threatens Retaliation After Cyber Attack
A top Israeli official said over the weekend that cyberattacks are akin to terrorism and threatened aggressive action against those who recently posted online personal information belonging to Israelis. PC Magazine; CNN; SC Magazine

US authorities probe Indian govt spy unit for email hacking
US authorities are investigating allegations that an Indian government spy unit hacked into emails of an official US commission that monitors economic and security relations between the United States and China, including cyber-security issues. Reuters; Forbes

SEC Push May Yield New Disclosures of Cyber Attacks on Companies
China-based hackers rifled the computers of DuPont Co. (DD) at least twice in 2009 and 2010, hunting the technological secrets that made the company one of the world's most successful chemical makers. It's not something investors would have learned from DuPont's regulatory filings, or from those of other companies victimized by hackers. Bloomberg

'Anonymous' hacktivists expose the intelligence gap
Over Christmas a busy, secretive group were at work, with their own views on who had been naughty and nice. However it was not Santa's elves, but the amorphous "Anonymous" collective making the decisions. This group of hackers released a vast trove of email addresses, passwords and credit card information belonging to subscribers of the US intelligence company Stratfor – and the hangover has carried on into the new year, with the release of MoD and Nato officials' details. The Guardian

Top UK security officials exposed in hack attack
Hundreds of sensitive email addresses for UK security officials were among details stolen in a major hacking attack, it has emerged. The hackers scooped the email addresses and other information during a Christmas attack on security consultancy Stratfor, but the type of UK officials breached has only just come to light. PC Pro

Google patches Chrome, beefs up malicious file blocking tech
Google last week patched Chrome 16 and improved the download warnings in the impending Chrome 17. Last Thursday, Google updated Chrome 16 with a security update that quashed three bugs, all rated "high," the company's second-most-dire threat rating. PC Advisor

Zeus returns: FBI warns of 'Gameover' ID-theft malware
A new variant of the notorious Zeus identity-theft Trojan is making the rounds and the Federal Bureau of Investigations (FBI) says it is capable of defeating common methods of user authentication employed by financial institutions. ZDNet

Anti-spam plan lacks teeth: Prof
If you still find your e-mail in-box inundated daily with unwanted messages from faraway royalty offering you free money or companies claiming they'll send you pharmaceuticals at a fraction of their price, you were likely pleased with the federal government's announcement of anti-spam legislation. Canoe

Do you know your cyberthreats?

The watchdogs at the Government Accountability Office this week issued a report that takes a look at what information, or guidance as they call it, is available to help government agencies and public sector companies bulk up their cybersecurity efforts. PC Advisor

Williston, Sandra

From: Williston, Sandra
Sent: January-12-12 12:41 PM
To: Pitcher Robert; Moore, Bruce; Phlek, Vireak
Cc: Beaudoin, Luc S
Subject: RE: Comments? Top 10 threats of 2012

BotNets are still prevailant.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: Pitcher Robert
Sent: January-12-12 12:20 PM
To: Moore, Bruce; Phlek, Vireak; Williston, Sandra
Cc: Beaudoin, Luc S
Subject: Comments? Top 10 threats of 2012

Guys,

I've been asked to put together an overview of shit we'll face in 2012. I came up with the following. Robert Dick/Gordon are to present this in the upcoming weeks. They said interface with csis and csec, but I figure we have to collective know how to avoid that idea. Anyway, here's my top 10. Anything you guys feel is too off the mark, or feel should be in, please let me know. Thanks!

- Continuation of targeted email attacks
  - Socially engineered to succeed!
- Advance malware attacks
  - Stuxnet: "...military grade software"
- Phishing attacks
  - Banking/Financial
- Social Network exploitations
  - Facebook has 800 million users. That's a lot of potential targets...
- Patch integrity
  - Keeping systems up to date!
- Cloud computing security
  - Security "outside the wire"
- Mobile/portable devices
  - IPhone/BlackBerry/Android malware
- Socially motivated/Extremely Capable
  - "Anonymous" attacks

- Software integrity
    - 0-Day exploits
- Secondary storage devices
    - Defeating perimeters by USB

Regards,
Robert Pitcher
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 949-8318
Fax/télécopieur: (613) 996-0995
Email/Courriel: Robert.Pitcher@ps-sp.gc.ca
Website/Site Internet: http://www.ps-sp.gc.ca

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-13-12 8:47 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted]; Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 13, 2012/ le 13 janvier 2012

Print Media

Hackers fry Putin's website
Calls for Russian Prime Minister Vladimir Putin to resign and drop his presidential bid flooded his campaign website within minutes of its launch on Thursday, prompting administrators to limit public access. Putin's spokesman and campaign official Dmitry Peskov said the website fell victim to a hacker attack in its early hours and some of the anti-Putin messages were spam. He denied any messages were blacklisted. Edmonton Sun, 20

Online Media

Cybercrime is a growing threat for government and public sector organisations
Cybercrime is a growing threat for government and public sector organisations, after 14 percent admitted they have been the victim of a web-based scam. According to research by Pricewaterhouse Coppers, more than a quarter (28 percent) believe they are likely to suffer a cybercrime attack in the next 12 months while 40 percent admit they think the risk of cybercrime to be on the rise. PC Advisor

Microsoft Planning Real-Time Feed of Valuable Threat Data
Microsoft has had a great deal of success taking down botnets in recent years. A fringe benefit of those takedowns is that Microsoft gets to collect oodles of very valuable data. Now, Microsoft is preparing to offer that threat intelligence as a real-time feed that partners can use to evaluate threats and develop better defenses. PC World

Cyber insurance offers IT peace of mind -- or maybe not
If your company were hit with a cyber attack today, would it be able to foot the bill? The entire bill, including costs from regulatory fines, potential lawsuits, damage to your organization's brand, and hardware and software repair, recovery and protection? Computerworld

Fighting cyber threats with malware not ideal
Countries are increasingly taking up the option of fending off cyber threats with homebrewed malware but while this might prove effective, security insiders noted this might bring technical and ethical issues and, ultimately, not the best method to curb online threats. ZDNet

'Gaza hackers' target Israel fire service website
Hackers claiming to be from the Gaza Strip defaced the website of the Israel Fire and Rescue services, posting a message saying "Death to Israel," a spokesman told AFP on Friday. Fire service spokesman Yoram Levy said that attackers who identified themselves as the "Gaza Hackers Team" struck its website late on Thursday and posted a picture of Israel's Deputy Foreign Minister Danny Ayalon with footprints over his face. AFP

Anonymous targets Israel as it joins war between hackers
Anonymous has posted what appear to be login details for Israeli SCADA industrial-control systems, a cyber attack that marks the politically minded group's entrance into the heated battle between Israeli and Saudi Arabian hackers that has already exposed thousands of credit card numbers and personal details. MSNBC

Stratfor back online after cyber-attack steals credit card data
Global intelligence analysis firm Stratfor has relaunched its website after hackers brought down its servers and stole thousands of credit card numbers and other personal information belonging to its customers. China Post

Security trumps secrecy in cyber fight, prosecutor says
A top federal prosecutor has a message for companies: If you've been hacked, tell us. Speaking at a cyber security conference in New York on Thursday, Manhattan U.S. Attorney Preet Bharara said companies should trust in the discretion of prosecutors and the FBI and come forward with information about a security breach, rather than keep it an internal secret. Reuters

GAO: DHS floods critical industries with irrelevant cybersecurity advice
The Department of Homeland security has responded so enthusiastically and uncritically to Presidential orders that it keep companies in the "critical infrastructure" informed of cybersecurity threats and techniques that it is, instead, drowning those companies in information that is often repetitive or misdirected, according to a new report from Government Accountability Office (GAO). IT World

Cyber Crime Threat Is Top Worry of Manhattan U.S. Attorney Preet Bharara
Preet Bharara, the top federal prosecutor in Manhattan whose office has sent terrorists and inside traders to prison, told an audience that the threat of Internet-related attacks is his biggest worry. Bloomberg

Cyber attacks now fourth biggest threat to global stability, says World Economic Forum
A report from the World Economic Forum (WEF) shows cyber attacks on governments and businesses are considered to be one of the top five risks in the world. The report, Global Risks for 2012, examined 50 global risks in the areas of the economy and the environment and in geopolitics, society and technology, and was based on interviews with more than 460 experts from industry, government and specialist areas. Daily Mail

Cyber-Crimes Pose 'Existential' Threat, FBI Warns
Despite the increased frequency and severity of online crime and espionage in 2011, many American corporations and consumers are still not taking the threat seriously, the FBI's top cyber official said Thursday. Huffington Post

Phishing pays off for email security providers
Big financial institutions and other companies are finally succeeding in reducing the volume of emails sent by malicious actors who disguise messages so that they appear to come from a trusted brand, a key technique both for cyber criminals and international spies. Financial Times

Cyber defense effort is mixed, study finds
A Pentagon pilot program that uses classified National Security Agency data to protect the computer networks of defense contractors has had some success but also has failed to meet some expectations, according to a study commissioned by the Defense Department. Washington Post

Malicious Software Attacks Security Cards Used by Pentagon
Chinese hackers have deployed a new cyber weapon that is aimed at the Defense Department, the Department of Homeland Security, the State Department and potentially a number of other United States government agencies and businesses, security researchers say. New York Times

World Economic Forum puts cyber attacks in top five biggest global risks for 2012
Cyber attacks are one of the top five global risks likely to impact the planet over the coming year, according to the latest annual report from the World Economic Forum (WEF). The international organisation interviewed more than 460 experts from industry, government, academia and civil society to compile its seventh Global Risks report. V3.co.uk

Chinese attacks target US government agencies and smartcards
Evidence has been revealed that attacks are being made against US government agencies, using a new strain of the Sykipot malware to compromise smartcards. According to Security Information and Event Management (SIEM) vendor AlienVault, the attacks originate from China and target agencies including the US Department of Defense. SC Magazine

Anderson, Windy

From: Hatfield, Adam
Sent: January-13-12 8:39 PM
To: Anderson, Windy; Cameron, Bud; Bendelier, Kenneth; Klassen, Nathan; Beaudoin, Luc S
Subject: Fw: New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks - Canada Ranks High
Attachments: Cyber_Power_Index_Findings_and_Methodology.pdf; Cyber_Power_Index.xls

FYI for the SA/results reporting angle.

Adam

From: Dvorkin, Corey
Sent: Friday, January 13, 2012 03:23 PM
To: * NCSD-340 Laurier
Cc: Stanfield, Charles; Stanfield, Charles; Champoux, Martin
Subject: FW: New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks - Canada Ranks High

Report is attached, as is an interactive spreadsheet.

Canada scores #5 globally, coming 4/19 in legal frameworks, and 5/19 countries for each of econ/social; technical infrastructure and industry applications.

Lots here to digest.

From: Castonguay LCol JF@VCDS DG Cyber@Ottawa-Hull
Sent: Friday, 13, January, 2012 14:20 PM
To: Sixsmith SL@ADM(Pol) D Pol Dev@Ottawa-Hull; Anishchenko A@ADM(Pol) D Strat A@Ottawa-Hull; Yarker LCol DR@SJS Operations@Ottawa-Hull; Kendall Maj PJ@VCDS DG Cyber@Ottawa-Hull; Messier Maj RM@VCDS DG Cyber@Ottawa-Hull; Renneberg MWO MA@VCDS DG Cyber@Ottawa-Hull; Couture Maj EB@CANOSCOM OS J3@Ottawa-Hull; Leblanc JPSS@RMC ECE@Kingston
Subject: FW: New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks - Canada Ranks High

FYI.

MCLEAN, Va., Jan 12, 2012 (BUSINESS WIRE) -- A new benchmarking study of 19 of the world's 20 leading economies found that the United Kingdom and the United States lead Group of 20 (G20) countries in their ability to withstand cyber attacks and to deploy the digital infrastructure necessary for a productive and secure economy. The index also found that several major economies--Argentina, Indonesia, Russia and Saudi Arabia--do not have cybersecurity plans and do not appear to be developing them.

The index is at www.cyberhub.com

Overall, the top five countries exhibiting cyber power, as measured by the index-- the UK; the US; Australia; Germany; and Canada --illustrate that developed Western countries are

leading the way into the digital era. The top five performers also rate highly across the board, ranking in the top seven in all four categories.

The Cyber Power Index, developed by the Economist Intelligence Unit and sponsored by Booz Allen Hamilton, measures both the success of digital adoption and cyber security, and the degree to which the economic and regulatory environment in G20 nations promote national cyber power.

The Index allows visitors to compare the cyber power rankings of the G20 countries on a scale of 0-100 with 100 being most favorable. Each country's ranking is a weighted mean of scores from four categories: Legal and Regulatory Environment; Economic and Social Context; Technology Infrastructure; and Industry Application. Each category features at least four underlying indicators, many of which are composed of sub-indicators. The European Union, the newest member of the G20, was not included in the study.

"The Cyber Power Index identifies those countries that understand what it takes to operate in a digital era...and those that don't," said Booz Allen Hamilton Vice Chairman Mike McConnell. "Many define a nation's cyber power simply like other domains such as land, air or space. While cyber is a domain, a nation's capabilities must be measured by more than their military might alone. The countries able to master the uses and security requirements of emerging technologies and societal shifts brought on by the cyber revolution will emerge as the cyber powers and the winners of the 21st century."

Overall, the top five countries exhibiting cyber power, as measured by the index--the UK; the US; Australia; Germany; and Canada--illustrate that developed Western countries are leading the way into the digital era. The top five performers also rate highly across the board, ranking in the top seven in all four categories. The G20's last member, the EU, was not analyzed.

The leading emerging market countries, Brazil, Russia, India and China (the BRICs), have some room for improvement; out of the 19 economies, they rank 10th, 14th, 17th, and 13th, respectively. There is also a wide discrepancy between the top and the bottom of the index. The UK, the top performer, scores around three times the amount of points on a scale of 0 to 100 as the worst performer, Saudi Arabia. Among other conclusions from the data:

-- Cyber power relies on a solid foundation that includes technical skills for security and effective use of the cyber environment, high educational attainment levels, open trade policies, and an innovative business environment. The US has the most supportive economic and social context for fostering cyber power according to the index. This is driven by high tertiary education enrollment, research and development (R&D) investment, and an open trade environment. Asia's rising influence is also apparent in this category, as China leads the trade indicator, while Japan and South Korea fill the number one and two positions, respectively, in technical skills.

-- The gap in cyber capability between the U.S. and other countries is closing. While the U.S. has a broad and deep cyber power base, other nations such as South Korea and Japan are aggressively adopting greater levels of bandwidth and communications stability.

-- Big does not always mean powerful. China has a large population and a powerful military. As a result the nation is often considered to be a cyber power. In reality, the Cyber Index found that the country's true level of cyber power is in reality quite modest. Going forward, other countries are expected to be added to the Index, which could show the power of small countries such as Estonia. In contrast to China, Estonia is relatively tiny and hosts a modest military, yet that country's well known ability to integrate advanced technology into its society could make a telling comparison.

-- Germany's comprehensive cyber policies are a key to its success. Germany leads the legal and regulatory framework category with a near perfect score (99.3 out of 100), followed by other Western countries that also performed well in the overall index. Germany is one of only five countries (the others being the UK; the US; France; and Japan) to have both a comprehensive national cyber plan and a comprehensive cybersecurity plan.

-- Prioritisation of ICT access is higher in the developed world. There is still a clear divide between developed countries and emerging markets as measured by access to internet, mobile phones, and WiFi. The UK, US, and Germany lead

Information Communications Technology (ICT) access, while Mexico, Indonesia, India, China, and South Africa have the lowest access scores. An exception is South Korea, which is fifth, despite having strong government policy towards improving access.

-- The G20 countries have made limited technological progress within key industries. Australia is the top performer within the industry application category, which measures the ability of different industries (energy, health, transportation, government, and e-commerce) to leverage ICT developments, including security advancements. As an indication of uneven technological development across industries, Australia ranks first in the category overall, but only scores well within the electronic health indicator.

Page 1447

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 1448 to / à 1609

are withheld pursuant to section

sont retenues en vertu de l'article

19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Bonvie, Jeff

From: Bonvie, Jeff
Sent: January-16-12 3:48 PM
To: Abramczyk, Jill; Virdee, Harjit Singh
Subject: Cyber Info
Attachments: PS-SP-#438312-v1-NCSD_GLOSSARY_OF_COMMON_CYBER_SECURITY_TERMS.DOC

Hello Jill and Harjit,

Nice to meet you both; sorry I was kind of a verbal machine gun. As discussed here is some cyber information which may (I hope) be of use.

@ Jeff To Do: Introduce you to Bud – this I will do via separate email, likely tomorrow.

NCSD's existing glossary of terms (see attached file 438312): Please note that we took from existing work where we thought it was a good fit. We didn't use any one single source (this is noted via the footnotes). In rare cases we wrote it ourselves when we either couldn't find, or were not happy with what we did find in the existing work.
The GCPEDIA Cyber Lexicon Reference: http://www.gcpedia.gc.ca/wiki/Cyber_Security_Lexicon
Backgrounder on Cyber: This we can plan for the near future, some related ongoing discussion here about our internal learning events. More to follow...
Interesting Cyber Related Links (more here than you would likely have time to read):

General News Sites:
http://www.wired.com/threatlevel/
http://www.wired.com/dangerroom/
http://www.net-security.org/
http://www.darkreading.com/index
http://www.pcworld.com/businesscenter/index/security.html
http://arstechnica.com/tech-policy/
http://slashdot.org (not security specific, just technical but often w/ posts re: security issues)
http://www.csoonline.com/

Blogs:
http://krebsonsecurity.com/ (Journalist / Researcher)
http://www.schneier.com/ (Security expert, on Security and Technology – oddly on Squids too)
http://blog.trendmicro.com/ (AV Company)
http://threatpost.com/en_us (AV Company)
http://www.symantec.com/connect/symantec-blogs/messagelabs-intelligence (AV Company)
http://blogs.technet.com/b/staysafe/ (Microsoft)
http://blogs.rsa.com/ (Security Gurus)

Popular / Frequently Referenced Material:
Defending a New Domain by William J Lynn - http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain
CSIS Report, Securing Cyberspace for the 44th Presidency - http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
H. Clinton's speech on Internet Rights and Wrongs - http://www.state.gov/secretary/rm/2011/02/156619.htm
Munich Security Conference William Hague - http://www.securityconference.de/Hague-William.704.0.html?&L=1
SecDev / Munk Centre Research Reports
(Ghost Net Report) http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network
(*Shadows in the Cloud* Report) http://www.infowar-monitor.net/2010/04/shadows-in-the-cloud-an-investigation-into-cyber-espionage-2-0/
(Koobface Report) http://www.infowar-monitor.net/reports/iwm-koobface.pdf (PDF)

A Sample of Interesting / Popular Attacks, Hacks & Haxors
Anonymous vs HBGary
http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars
Albert Gonzalez (Massive Credit Card theft and was working for the FEDS)
http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html
General Article on Stuxnet (1 of 1598745015484545 articles on Stuxnet)
http://www.infoworld.com/t/malware/more-evidence-arises-stuxnet-was-created-attack-iran-306
RSA Attack
http://arstechnica.com/security/news/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated.ars

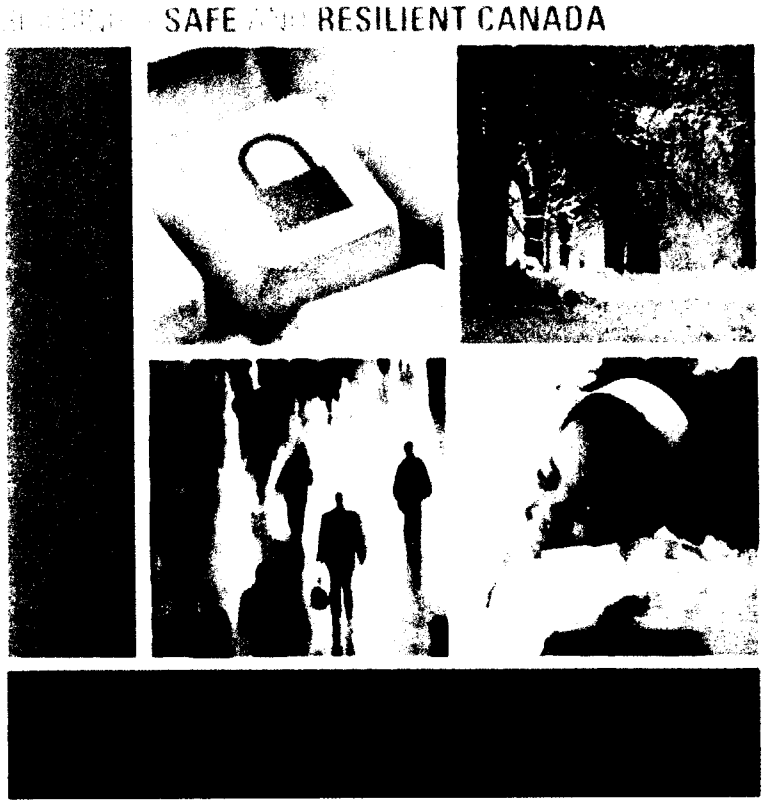
International Strategies (some of these are out of date):
Australia (PDF)
UK (It was here somewhere...)
US (PDF)
Dutch (PDF)
German (PDF)
French (PDF)

Hope this is of use!

Cheers,

Jeff
Advisor / Conseiller
National Cyber Security Directorate / Direction générale de la cybersécurité nationale
Public Safety Canada / Sécurité Publique Canada
340 Laurier Avenue West / 340, avenue Laurier Ouest
Ottawa, Ontario, K1A OP8
613-990-9380
Jeff.Bonvie@ps-sp.gc.ca

Public Safety Canada | Sécurité publique Canada



NATIONAL CYBER SECURITY DIRECTORATE
GLOSSARY OF COMMON CYBER SECURITY TERMS

JUNE 17 2011
RDIMS #438312
Version 1.1

Canada

001612

National Cyber Security Directorate
Glossary of Common Cyber Terminology

A

Anti-virus software (AVS) - software that defends against viruses, trojans, worms and spyware. Anti-virus software uses a scanner to identify programs that are or may be malicious. Scanners can detect: known viruses; previously unknown viruses; and suspicious files. [1]

B

Backdoor – a backdoor in a computer system is a method of bypassing normal authentication or securing remote access to a computer, while attempting to remain hidden from casual inspection.[2]

Beaconing – is a process whereby a system (typically a victim) sends a contact message to another system (usually an intruder's control system). [2] This process is done to notify to an intruder that a system is active and remains infected.

Bot – a program covertly installed on a user's machine to allow an unauthorized user to remotely control the targeted system through a communication channel. These channels allow the remote attacker to control a large number of compromised computers in a botnet, which can then be used to launch coordinated attacks. Attackers can use bots to perform a variety of tasks, such as setting up denial of service attacks against an organization's website, distributing spam, spyware and adware, phishing attacks, propagating malicious code, and harvesting confidential information.[1]

Botnet – a collection of compromised machines running malicious applications without the knowledge of the operator via a command and control infrastructure.[2]

Brute Force Attack - attack on a system that employs an exhaustive search of a set of keys, passwords or other data. [1]

C

Computer Emergency Response Team (CERT) – a group which is responsible for responding to computer related security incidents outside of typical information technology support roles.

Cloud Computing – the ability to access all required software, data and resources via a computer network instead of the traditional model where these are stored locally on a users computer.

Compromise – the disclosure of information or data to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosures, modification, destruction, or loss of an object may have occurred. [2]

Computer Network Attack (CNA) – actions take trough the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks of the computers and networks themselves. [2]

Computer Network Defence (CND) – actions taken through the use of computer networks to protect monitor, analyze, detect and respond to unauthorized activity within a department or organization's information systems and computer networks. [2]

Computer Network Exploitation (CNE) – enabling operations and intelligence collection acapabilit8ies conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. [2]

Computer Network Operations (CNO)– comprise computer network attack, computer network defence and related computer network exploitation enabling operations. [2]

Computer Security Incident Response Team (CSIRT) – See CERT.

Command and Control (CNC) Server – a system (often also compromised) which is used to control all of the infected computers in a distributed botnet.

Cryptography – the discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [1] The conversion of the information into this new protected form is referred to as encryption. The conversion of information back to its original form is decryption.

D

Decryption – decoding of a message which has been encrypted (see cryptography)

Denial of Service (DoS) Attack – a type of cyber attack aimed at overwhelming or otherwise disrupting the ability of the target system to receive information and interact with any other system.

Deep Packet Inspection – the detailed analysis of a data packet in order to determine if the contents of the packet contain malicious or otherwise unwanted data.

Distributed Denial of Service (DDOS) Attack – a denial of service attack which utilizes a series of computer systems which are in the form of a distributed network. In a DDOS attack, more than one system is attacking the target. Often DDOS attacks utilize botnets.

Digital Forensics - generally considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. [1]

E

Encryption – converting information from one form to another to hide its content (see cryptography)

Exploit - is a defined way to breach the security of an IT system through a vulnerability. [1]

Exfiltration – the unauthorized removal of data or files from a system by an intruder.[2]

F

Firewall - a firewall is a type of security barrier placed between network environments. It may be a dedicated device, or a composite of several components and techniques. It has the properties so that all traffic from one network environment to another, and vice versa, traverses through the firewall and only authorized traffic, as defined by the local security policy, is allowed to pass. [1]

G

H

Hacktivist – a computer attacker who undertakes malicious activity for political or other motivations related to a particular issue or position.

Honeypot - a decoy Information System used to deceive, distract, and divert an attacker and to encourage the attacker to spend time on bogus information.[1]

I

Industrial Control Systems (ICS) – the broad grouping of software and hardware that is used to control infrastructure such as those found in factories and power generation stations including supervisory control and data acquisition systems and programmable logic controllers.

Information Technology Security (ITS) - safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.[1]

Internet Engineering Task Force (IETF) - the group responsible for proposing and developing technical Internet standards.[1]

Internet Governance Forum (IGF) – a UN created forum which brings states, NGOs and other stakeholders to discuss public policy issues related to key elements of international governance in order to foster the sustainability, robustness, security, stability and development of the Internet.

Internet Corporation for Assigned Names and Numbers (ICANN) – a non-profit organization dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.

Intrusion Detection System (IDS) - technical system that is used to identify that an intrusion has been attempted, is occurring or has occurred, and possibly to respond to intrusions in IT systems and networks.[1]

Intrusion Prevention System (IPS) - a variant on intrusion detection systems that are specifically designed to provide an active response capability.[1]

J

K

Keystroke Logger – software or hardware designed to capture a users keystrokes on a compromised system. The keystrokes are stored or transmitted so that they maybe used to collect valued information.

L

M

Malware - malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

Metadata - data that describes the structure and workings of an organizations use of information, and the systems it uses to manage that data.

N

Network Administration - day to day operation and management of network processes and users.

O

P

Packet - a formatted block of information carried by a computer network. When data is formatted into a packet, the network can transmit longer messages more efficiently and reliably than unformatted bytes.

Patch - a small piece of software designed to update or fix problems with a computer program. This includes fixing bugs, reducing vulnerabilities, replacing graphics and improving the usability or performance.

Peer to Peer (P2P) Network - relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating power in a low number of servers. These networks are often used for sharing content files containing audio and video data.

Phishing - an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card

numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

Proxy - a process that accepts requests for some service and passes them on to the real server.

Q

R

Ransomware - software that denies you access to your files until you pay a ransom. [1]

Rootkit - a set of software tools intended to conceal running process, files, or system data, thereby helping the intruder to maintain access to a system without detection. Rootkits often modify parts of the operating system or install themselves as drivers or kernel modules.[2]

S

Supervisory Control and Data Acquisition (SCADA) - an industrial measurement and control system consisting of a central master station, one or more field data gathering control units, and a collection of standard or custom software used to monitor and control electromechanical devices in industrial processes such as refineries, electrical power generation or flood control.[2]

Spear Phishing - the use of spoof emails to persuade people within an organisation to reveal their usernames or passwords. Unlike phishing, which involves mass mailing, spear phishing is small-scale and well-targeted.[1]

Security Token - a set of security relevant data that is protected by integrity and data origin authentication from a source which is not considered a security authority. [1]

SPAM - junk or unsolicited e-mail sent by a third party. An annoyance to users and administrators, spam is also a serious security concern as it can be used to deliver Trojans, viruses, and phishing attempts. [1]

Sniffers - computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. [1]

Social Engineering - the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. For example, phishing is a type of social engineering technique. [2]

Spoofing - a situation in which one person or program successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage.[2]

Spyware - software that enables advertisers or hackers to gather information without the user's permission. Spyware programs are not viruses, since they do not spread to other computers, but they can have undesirable effects. Once installed, spyware tracks the infected computer's activity and reports it to others, such as advertisers. Spyware also consumes memory and processing capacity, which may slow or crash the infected computer.[1]

T

Trojan - a malicious program that is disguised as or embedded within legitimate software. The term is derived from the gift the ancient Greeks presented to the citizens of Troy during the Trojan War, as a ruse to infiltrate and sack the city.[2]

U

V

Virtual Private Network (VPN) - a private communications network usually used within a company, or by several different companies or organisations to communicate over a wider network. VPN message traffic can be carried over a public networking infrastructure (i.e. the Internet) on top of standard protocols, or over a service provider's network with a defined Service Level Agreement between the VPN customer and the VPN service provider. VPN communications are typically encrypted or encoded using SSL to protect the traffic from other users on the public network carrying the VPN.[2]

Virus - a computer program that can spread by making copies of itself. Computer viruses spread from one computer to another, by making copies of themselves, usually without the knowledge of the user. Viruses can have harmful effects, ranging from displaying irritating messages to stealing data or giving other users control over the infected computer. A virus program has to run before it can infect a computer, generally doing so by attaching itself to other programs or hide in code that is executed automatically when a user opens certain types of files.[1]

Vulnerability - a flaw or weakness in the design or implementation of an information system or its environment that could be intentionally or unintentionally exploited to adversely effect an organization's assets or operations.[2]

W

Worm - a self-replicating computer program. It uses a network to send copies of itself to other systems and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.[1]

X

Y

Z

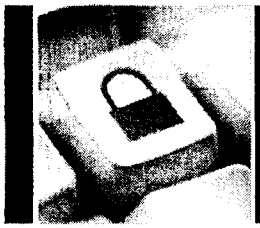
Zero Day Exploit - a zero-day exploit makes use of unrecorded vulnerabilities in a host or network that evade anti-virus and anti-spyware systems. The exploit is generally used to insert malicious code.[2]

Zombie - a computer that is remotely controlled and used for malicious purposes, without the legitimate user's knowledge. A virus or Trojan can infect a computer and open a "back door" that gives other users access. As soon as this happens, the virus sends a message back to the virus writer, who can now control the computer remotely via the Internet. The computer is now a zombie doing the bidding of others, although the user is unaware. Collectively, such computers are called a "botnet."[1]

SOURCES

[1] Cyber Security Lexicon from GCPEDIA, http://www.gcpedia.gc.ca/wiki/Cyber_Security_Lexicon
[2] Department of National Defence, Defence Intelligence Cyber Glossary.

Note: Entries without source reference have been created by NCSD. Entries which are referenced to an external source may be subsets of the complete entry found in the reference.



Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CYBER SECURITY SUMMARY FOR CIOs

Reporting Period: JANUARY 14-28, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-002

Purpose

This product is intended to provide Chief Information Officers in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations.

This product also provides contextual background information for the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Overview

Domestically, there were no significant cyber incidents reported over the last two weeks. There were reports of Canadian computers being used for malicious purposes, including attacking a US State Police website. A Canadian federal department linked to the signing of the international Anti-Counterfeiting Agreement (ACTA) was targeted through a malicious e-mail. There was also a message on the Internet by hackers to e-mail or launch a cyber attack against this Department. Internationally, hackers attacked government websites in US, Poland, Ireland and the EU to protest signing of ACTA. There are also continued reports of infected computers in Canada and around the world due to the Ghostclick fraud.

Highlights

New Events:

- A Canadian federal department with links to ACTA targeted by hackers
- File server log in credentials of a federal department posted on the Internet
- Incidents of Canadian computers hosting malicious software
- US State Police website attack traced to Canada
- Some Canadian Industrial Control Systems (ICS) reported as being exposed to potential cyber attack".
- Phishing: Fraud attempts in the Financial sector; Cyber criminals impersonating federal organizations
- Website compromises and publicized vulnerabilities in following sectors: Canadian health, non-critical infrastructure sector and a foreign Defence Department

CCIRC Products Released during the reporting period:

- Cyber Flash on cyber attacks by Anonymous related to copyrights and intellectual property (CF12-001)

Noteworthy News in the Media:

- Israeli and Palestinian hackers exchange website attacks
- Hackers around the world protest current and intended anti-piracy measures:
  - MegaUpload's shutdown prompts hacker attacks on US government and music industry websites
  - Proposed US copyright law SOPA being protested: Certain websites elect to go dark for one day in protest; Anonymous attacks US government websites such as DOJ & FBI
  - Signing of the international Anti-Counterfeiting Agreement (ACTA) prompting hacker attacks on US, Poland, Ireland and European government websites.

NEW EVENTS REPORTED IN GOVERNMENT AND OTHER CANADIAN CRITICAL INFRASTRUCTURE SECTORS

Federal Government Sector

Operation SACTA (Stop Anti-Counterfeiting Trade Agreement): An online message signed by Anonymous posted a link to a Canadian federal department website, encouraging users to join the anti-ACTA movement, and attack if necessary. This message was posted on a popular text-file sharing website often used by hackers and is presumably encouraging cyber attacks on websites.

CCIRC provided available technical details to CTEC, the federal Government's CERT, for their further investigation.

> ***Comment:*** *There are provisions in the international Anti-Counterfeiting Trade Agreement that have important implications for content sharing on the Internet. This is a multi-lateral trade agreement which Canada has signed. Canada's new proposed copy-right law, Bill C-11 (former Bill C-32), is currently in Parliament at the second reading stage. There is a great deal of opposition to this agreement around the world by the on-line community and websites of other government have recently been attacked by hackers in protest.*

File Server (FTP) Login Credentials of a Federal Department posted on the Internet. CCIRC learned that the FTP login credentials of a federal department were posted on the Internet. CCIRC advised CTEC and provided known technical details.

> ***Comment:*** *FTP login credentials are used to gain access to a file sharing server where users may upload or download files. If a threat actor used these credentials, the result could be information compromise or the use of the server as a launch point for cyber attacks.*

Non-Federal Government Sector

Canadian computers being used in cyber attacks. CCIRC has learned that a cyber attack on a US State Police website was traced to a Canadian university's computer. In addition, another Canadian university's website was found to host malicious software that could infect website visitors. There were also reports of malicious software being hosted at a website hosting service provider's server and at two other unidentified Canadian entities.

CCIRC contacted the known Canadian organizations, with mitigation advice. The RCMP was informed of items of interest. CCIRC warned the website hosting service provider that the website in question was added to various block lists, possibly resulting in reduced legitimate traffic to this website. The malicious software from the university's website has been removed and is no longer being served.

> ***Comment:*** *It is possible that cyber criminals compromised these Canadian computers to use them remotely for malicious purposes, without their owners' knowledge. Organizations that offer computers for public use, such as universities, can be particularly susceptible to such compromises.*

Some Canadian Industrial Control Systems exposed to potential cyber attacks. A trusted international partner alerted CCIRC that information that could allow remote access to certain Canadian houses and apartment buildings' heating and air conditioning systems, was posted on the Internet. CCIRC alerted those responsible for the buildings and houses, offering mitigation advice. There is no report of any cyber attack in these cases at this time.

> ***Comment:*** *Many Industrial Control Systems (ICS), such as the ones used for heating and cooling buildings, are monitored or even maintained remotely through the use of certain software. It is likely that the technicians responsible for the set-up and maintenance of the heating systems for these buildings did not take cyber security into consideration or did not know the standard practices for protecting against such exposure.*
>
> *Since the Stuxnet virus attack on an Iranian nuclear facility, there has been a heightened awareness, both domestically and internationally, of cyber security for ICS. The trusted international partner who alerted CCIRC is focussed primarily on securing ICS. CCIRC recently moderated discussion at a ICS conference in Montreal.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonating Canadian financial institutions, tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in United States and Taiwan.

Cyber criminals also attempted to solicit personal information by impersonating Service Canada and Canada Revenue Agency.

CCIRC notified the impersonated financial institutions of these fraud attempts and the Government CTEC for the federal government cases. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website compromises and publicized vulnerabilities. CCIRC discovered a small health organization's website was defaced and offered mitigation advice. CCIRC also discovered a foreign Defence Department's website was compromised and contacted the organization, as well as CCIRC's equivalent organization. There was also a list of vulnerable websites posted on the Internet, which includes a Canadian university.

There were additional website compromises in the health and non-critical infrastructure sectors. Website usernames and passwords were posted on the Internet by hackers.

> ***Comment:*** *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

Ghostclick Fraud. There were new and continued reports of infected computers in three provincial governments, three provincial health organizations, an airport authority, an energy organization, two banks, 19 Canadian universities, a national media organization and 13 telecommunications companies.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012. There are currently websites around the world for computer users to check whether their machine is infected by the malicious software used in this fraud. These sites can be found by searching with the keywords "dns-ok".

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in. CCIRC is also working with the Canadian Internet Registration Authority (CIRA) to provide notifications to affected users.

Operation Ghostclick was worldwide fraud campaign, exposed in late 2011 by the FBI. Cyber criminals hijacked users' Internet web searches and diverted them to websites that generated advertising and sales revenues. Computers across multiple sectors, in organizations large and small, and those belonging to the general public have been affected.

> ***Comment:*** *Organizations should ensure they have taken the mitigation measures outlined in CCIRC's Information Note. CCIRC noted that the type and size of affected organizations varied, and were spread across Canada. The number of affected telecommunications companies more than likely indicates number of infected client computers of Internet via Service Providers. These Internet Service Providers receive information from CCIRC.*
>
> *Organizations that offer Internet access, including those that provide publically accessible wireless networks, may be particularly vulnerable. In addition to the cooperative effort underway between CCIRC and CIRA, the Canadian government has launched a website for cyber security public education..*

CCIRC PRODUCTS RELEASED:

Hacktivist attacks related to proposed anti-piracy legislation. There have been coordinated distributed denial-of-service (DDoS) attacks on websites by hacktivists, claiming to be associated with Anonymous. There were multiple international targets, which included governments (Canada, US, Poland, Ireland and EU) and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA).

In response, CCIRC issued Cyber Flash CF12-001, titled *"Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property"*. This Cyber Flash, was sent to technical and security contacts within stakeholder organizations in government and other critical infrastructure

sectors . Government and industry organizations involved with the Copyright legislation and copyrighted material were encouraged to assess their risk exposure to coordinated DDoS attacks on their networks.

NOTEWORTHY NEWS IN THE MEDIA:

Israeli and pro-Palestinian hackers exchange website attacks. Open sources reported that the websites of Israel's main stock exchange, several banks and the national airline were attacked. Pro-Palestinian hackers claimed responsibility and even claimed to have posted the login credentials for several industrial control systems in Israel on the Internet. Shortly thereafter, there were reports of suspected Israeli hackers bringing down the Saudi Stock Exchange, interfering with the Abu Dhabi Security Exchange, and publishing e-mail addresses & passwords of 30,000 Arab Facebook users.

> *Comment: It is now becoming commonplace to carry real-world grievances into the cyber world. There could be an adverse impact from these attacks for Canadians and Canadian businesses that do business with the stock exchanges or banks involved. There were some media reports that some of the Israeli banks could block international access to their sites.*

Hackers around the world attack government websites to protest anti-piracy measures.

- **Retaliation for file-sharing service Mega Upload's shutdown:** Hackers, claiming to be with Anonymous, attacked the websites of the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music.

- **Signing of the international Anti-Counterfeiting Agreement (ACTA) and proposed US copyright laws:** Wikipedia shut down for one day to protest the proposed SOPA and PIPA bills. SOPA and PIPA were also cited by Anonymous as a reason for their attacks on the DOJ and FBI websites. Operation STOP ACTA by Anonymous also prompted hacker attacks on websites for US, Poland, Ireland governments as well as for the European Parliament.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

OUR ORGANIZATION

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest.

CCIRC operates in conjunction with the Government Operations Centre within Public Safety Canada, and is a key component of the government's all-hazards approach to emergency management and national security.

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-17-12 8:00 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 17, 2012 / le 17 janvier 2012

MINISTER / MINISTRE

Naval officer accused of sharing secrets
A Royal Canadian Navy intelligence officer stands accused of sending top secret information to a foreign entity as recently as last week in one of the rarest and most closely guarded investigations to have rocked the military. Court documents filed in Halifax allege that Sub-Lieut. Jeffrey Paul Delisle, 40, broke the federal Security of Information Act and committed criminal breach of trust when he passed restricted information to a foreign agency over the span of more than four years. A **spokesperson for Public Safety Minister Vic Toews** said the **minister** had been briefed on the arrest. "***Minister Toews has been briefed and congratulates the RCMP and security agencies for their collaboration. As this matter relates to national security and is before the courts, we have no further comment,***" **Julie Carmichael** said Monday. Waterloo Region Record, A1 (Toronto Star)

Pot legalization
An editorial states, "he single concrete policy proposal to emerge from the weekend Liberal convention - a resolution urging the legalization of marijuana - is being touted as "controversial." But it shouldn't be. For the last quarter century, a majority of Canadians have supported the decriminalization of simple marijuana possession...In 2006, when asked whether the Tories would do anything to advance the issue of pot decriminalization, then justice **minister Vic Toews** responded: "***It is a very short answer, and the answer is no.***" That's a retrograde attitude. But at least the Tories are forthright about their position on the issue...In her capacity as health minister, and then **public safety minister** under Mr. Martin, Anne McLellan was particularly hawkish in her opposition to marijuana reform - for similar U.S.-centric reasons..." National Post, A12

Police can now confiscate private property!
An opinion piece states, "When Bill C-68, the gun registry bill, was being debated, opponents said the registration of firearms would lead to their eventual confiscation. Now that is happening. Just before Christmas 2011, owners of certain firearms were informed by letter that their rifles had been reclassified as prohibited weapons in Canada and that they must be turned over to police officials. **Public Safety Minister Vic Toews** was asked about this gun registry mess on the Sun News Network, and defended the current situation. "***It is not a decision that I make as a politician; it's something that the police and classification experts make***," **Toews** said...It's time for **Toews** and the rest of the Harper government to wake up and fix this mess." Whitehorse Star, 6

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Blueprint for a plague**
An opinion piece states, "H5N1, a variant of avian influenza, is nasty stuff. It kills somewhere between 50% to 60% of the humans it infects. The good news, if you can call it that, is that while extremely lethal, H5N1 isn't particularly communicable. Fewer than 600 people are known to have contracted it. So if you get it, you're probably in a bad way, but the odds of getting it are long indeed..." National Post, A12

*** Sorting out banned bird flu study**
The World Health Organization says it will take a role in helping sort through an international scientific controversy over two bird flu studies that the U.S. government deemed too dangerous to publish in full. Red Deer Advocate, C3

*** Le système d'alerte de Pointe Lepreau sera mis à l'essai jeudi**

Le système d'alerte en cas d'urgence sera mis à l'essai jeudi prochain dans la région de Pointe Lepreau. La mise à l'essai sera dirigée par l'Organisation des mesures d'urgence du Nouveau-Brunswick en partenariat avec la centrale nucléaire de Pointe Lepreau et Énergie NB. L'Acadie Nouvelle, 10

*** It's not the time to reduce research**
A letter states, "Tucked away on page B6 of the Jan. 12 Times Colonist was a disturbing article reporting that 60 scientists and researchers were being "declared surplus" (fired) at Environment Canada. They are part of 776 personnel to be cut. I wonder why Environment Canada is cutting scientists when Canada is facing serious environmental challenges. The Cohen Inquiry into the failing stocks of salmon in B.C. waters showed the need to monitor and identify viruses in fish from farms and wild salmon, imported or endemic..." Times Colonist, A11

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Navy officer faces espionage charges
A member of the Royal Canadian Navy has become the first person charged under the country's post-9/11 secrets law for allegedly passing protected government information to an unknown foreign body. Sub-Lt. Jeffrey Paul Delisle, 40, was charged Monday under the Security of Information Act, which came into effect in 2001. The navy intelligence officer is charged with communicating information that may "increase the capacity of a foreign entity or a terrorist group to harm Canadian interests." Ottawa Citizen, A1 (Windsor Star, Vancouver Sun, Daily Gleaner, Calgary Herald, Winnipeg Free Press, Chronicle-Herald); Globe and Mail; Edmonton Sun (Calgary Sun, Toronto Sun, Winnipeg Sun, Ottawa Sun); * The Guardian (Hamilton Spectator); * Le Soleil (Le Droit, La Presse); * Journal de Montréal

CYBER SECURITY / CYBERSÉCURITÉ

*** Spying on cyber crime**
The end of the Cold War combined with the advent of the Internet gave rise to an unprecedented wave of electronic espionage and crime. Michel Juneau-Katsuya witnessed first-hand the rise of cyber crime as a senior manager with the Canadian Security Intelligence Service (CSIS) at the time. In 2000, Mr. Juneau-Katsuya left public service to become founding chief executive of security consulting firm Northgate Group. He recently spoke with Financial Post technology reporter Jameson Berkow about the growing digital threat and how companies should respond. The following is an edited transcription of their conversation. National Post, FP8

*** Websites going dark to fight anti-piracy bill**
In the digital world, it's the equivalent of going on strike. Tomorrow, a number of high-profile websites, including Wikipedia, Reddit, Cheezburger Network and Boing Boing, will go dark for up to a day to protest against contentious anti-piracy legislation proposed by the U.S. Congress. The pending legislation would boost the power of the Justice Department to punish foreign websites that infringe copyright. It has also pit Hollywood, which has lobbied for the legislation as a tool to protect content, against Silicon Valley, which sees it as a menace to free speech. Online lobbying efforts to kill the bill already appear to have paid off. On Saturday, the Obama administration signalled it does not support aspects of the pending legislation - the Stop Online Piracy Act - and depicted it as a threat to global innovation. The digital dust-up, however, continues with media baron and Twitter newbie Rupert Murdoch jumping into the fray decrying the Obama administration's stance with a tweet. Globe and Mail, A12

*** Hacker attacks Israeli websites**
The website for Tel Aviv's stock exchange was shut down for hours on Monday after a hacker who identified himself as a Saudi announced that a pro-Palestinian group called Nightmare had targeted the site. El Al Airline, also named by the hacker OxOmar as a target, pre-emptively closed down its own website, directing visitors to a page with a statement that it was under maintenance. In addition, problems were reported on the sites of a few small Israeli banks. Monday's incidents were the latest in a series of attacks on Israeli websites kicked off earlier this month by a hacker who snagged thousands of credit card numbers from a poorly protected site associated with online shopping. Ottawa Citizen, A11; National Post; Telegraph Journal; Le Devoir

*** Online shoe site hacked**
Online shoe retailer Zappos told customers it has been the victim of a cyber attack affecting more than 24 million customer accounts in its database. The popular retailer, owned by Amazon.com, said customers' names, email addresses, billing and shipping addresses, phone numbers and the last four digits of credit cards numbers and scrambled passwords were stolen. But it said the hackers had not been able to access servers that held customers critical credit card and other payment data. Times Colonist, B2

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

Kakeeway arrested near Swift Current
Sgt. Paul Dawson says it was "good police work" on Saturday that led to RCMP in Swift Current arresting a Winnipeg man wanted for murder in his hometown. Leader-Post, A3

What you said ...
Q. Does Canada need a national DNA databank for missing people? Yes 53% No 47%...The mother of an Edmonton Edmon man who vanished more than three years ago is helping push a bill into Parliament that could create a national DNA bank for missing people...That DNA bank would collect and store samples of the missing, or their relatives, and allow investigators to cross-reference DNA with remains. London Free Press, B4 (Kingston Whig-Standard)

*** Mountie investigated**
A seven-year RCMP veteran, currently posted with the Combined Forces Special Enforcement Unit, is being investigated for impaired driving following a crash on Highway 1 late Sunday. The single-vehicle crash involving the off-duty female Mountie happened at 10: 45 p.m. on Highway 1, eastbound in the area of the 160th Street overpass. The Province, A8

*** RCMP won't pay vet bills for shot dog**
Nancy Stevenson was devastated last summer when her beloved dog was shot twice by a police officer in front of her Shediac home. However, Stevenson is left owing more than $5,000 from veterinarian bills. She has sought reimbursement from the RCMP, but was informed on Friday that they have denied her claim. She complained to police and the RCMP investigated, but Cst. Chantal Farrah, spokesperson for the RCMP's J Division in Fredericton, said yesterday that the investigation revealed that there was no negligence on the part of the officer. Times & Transcript, A3

*** Investigation finds police shooting justified**
A lengthy investigation into a March 2011 shootout that left a 24-year-old man dead and a Fort McMurray RCMP officer wounded has found police acted in self-defence. Edmonton Journal, A4 (Calgary Herald)

*** Un policier du SPVM aurait tenté de vendre de l'information secrète à la mafia**
Un policier du Service de police de la Ville de Montréal (SPVM) aurait tenté de vendre des informations confidentielles concernant les informateurs de la police au crime organisé. Selon ce qu'a rapporté Radio-Canada hier, le policier en cause était un sergent-détective au service des renseignements criminels. Il a pris sa retraite en janvier de l'année dernière après une trentaine d'années de service au sein du SPVM. La Voix de l'Est, 22 (Le Soleil, La Tribune); Journal de Montréal; Journal de Montréal

*** Council beefs up services, approves charters**
Red Deerians will see some differences when it comes to major services approved under the 2012 operating budget. The snow and ice removal budget was beefed up by just over $572,000, boosting the total amount to $2.9 million. Policing and crime prevention were also forefront on the minds of civic leaders. The RCMP's member fee agreement with the city, which pays for about 128 officers, rose by $617,000. A funding request of just over $92,500 was approved to pay for a provincial government shortfall of three Mounties. The RCMP requested a number of new positions - two community peace officers, a criminal analyst position, a court liaison officer position, video capture technician/training and development facilitator, and four RCMP officers (three school resource officers, and one additional officer dedicated to the Mental Health project)... Red Deer Advocate, A3

*** Mountie on trial for fraud**
The first witnesses take the stand today in the trial of an RCMP officer charged with criminal harassment, extortion and mortgage fraud. Const. Hoa Dong La, 47, currently on paid leave, is being tried before Justice David Gates in Red Deer Court of Queen's Bench on 15 counts relating to tenants and properties located in Innisfail and Bowden. At the request of his lawyers, Ian McKay and Heather Ferg, La was allowed to sit with his wife in the public gallery rather than in the box normally reserved for the accused. La served with the RCMP Innisfail detachment before transferring to Calgary to work in the Immigrant and Passport Section. Red Deer Advocate, A1

*** Six pounds of pot seized in Labrador bust**
The RCMP street level drug enforcement team seized a quantity of marijuana recently as part of an investigation into the movement and distribution of illegal drugs into central Labrador and the isolated communities along the Labrador coast. According to police, this investigation resulted in the arrest of a man from Happy Valley-Goose Bay on Jan. 13 and the the seizure of approximately six pounds of marijuana. No charges have been laid. The Telegram, A3

*** New Nanaimo RCMP unit reports major drug bust**
A special unit of the Nanaimo RCMP recently created to target powder drugs is being credited with one of the largest drug busts ever seen in the area. A vehicle stop Friday led to the execution of a search warrant on a Strickland Street home and turned up more than eight pounds of cocaine, crack cocaine, heroin and crystal meth, police said. The RCMP's White Team also found $50,000 in Canadian currency. Times Colonist, A4

*** Ripou**
Un article d'opinion déclare, « Ce que les policiers redoutent plus que le crime organisé c'est qu'un des leurs les trahit. Quand un irréductible policier des enquêtes ou du renseignement décide de changer de camp, les conséquences peuvent en être dramatiques...Merci aux policiers honnêtes qui le pourchassent. On aimerait tous que nos policiers soient parfaits, mais malheureusement certains font exception." Journal de Montréal, 3

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Pickton, Bernardo probes plagued by same failings
The same systemic problems that allowed sex killer Paul Bernardo to rape and murder women undetected in Ontario in the late 1980s and early 1990s contributed to the failure of the Vancouver police and RCMP to catch serial killer Robert Pickton, a public inquiry heard Monday. Deputy Chief Jennifer Evans of Ontario's Peel Regional Police was asked to review the Pickton file for the inquiry, writing a critical report that concluded investigations by both the Vancouver police and the RCMP were plagued by poor communication and a lack of leadership. Globe and Mail, S3 (Waterloo Region Record, Chronicle-Herald, Red Deer Advocate); Leader-Post (The Province, Calgary Herald, Times Colonist); * Vancouver Sun; * Times & Transcript

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Mexican journalist fights deportation
Mexican journalist Karla Berenice Garcia Ramirez, her husband and her two young Canadian-born daughters, are fighting deportation from Canada - and, as they see it, for their lives. She and her husband fled to Canada from Mexico in 2008 after she and her family received death threats that had escalated from less threatening intimidation starting in 2003, the apparent result of her efforts to uncover corruption at a government ministry. She was working at the ministry at the time, but had previously been employed as a journalist. Globe and Mail, S2

*** Tofino man grounded by U.S. border rigidity**
Even the judge rolled his eyes, gave Adrian Dorst a suspended sentence when the then 24year-old got busted for having marijuana resin in a decorative pipe way back in 1967. But American authorities were dead serious when they discovered the Tofino man's 45-year-old conviction last week. They refused to let him fly through the U.S., costing the well-known nature photographer a $1,250 airline ticket and a "dream trip" to the cloud forest village of Mindo, Ecuador. Times Colonist, A3

*** Mugesera reste détenu**
Le présumé criminel de guerre rwandais, Léon Mugesera, qui fait l'objet une ordonnance d'expulsion vers son pays d'origine, devra demeurer détenu en attendant son renvoi prévu pour vendredi, a décidé hier après-midi la Commission de l'immigration et du statut de réfugié (CISR). Le gouvernement conservateur estime toutefois qu'il sera bien traité et qu'il doit être expulsé du Canada. Le gouvernement rwandais a également assuré Ottawa que Mugesera sera traité humainement. Journal de Montréal, 12; Le Soleil; The Guardian; Le Devoir (Le Droit); Globe and Mail; Montreal Gazette; London Free Press (Toronto Sun, Kingston Whig-Standard); Vancouver Sun

*** MP protests border toll 'gouge'**
Differences in the currency exchange rate are costing travellers millions of dollars at Windsor's two border crossings, says MP Brian Masse (NDP - Windsor West). Despite a currency exchange that has been close to par the past couple of years, the loonie is undervalued compared to the U.S. dollar at the Ambassador Bridge and Windsor-Detroit tunnel. Windsor Star, A3

*** Refugees may look south**
For years, Canada has had one of the most generous immigration policies in the world, welcoming tens of thousands of asylum applicants who claim to be fleeing persecution in their homelands. But Canada's Conservative government has begun rolling up the welcome mat, increasing efforts to track down and deport thousands of asylum-seekers whose

applications have been denied. The clampdown is likely to be felt not just across Canada, but in the United States. Vancouver Sun, B4

*** 7,5 kg de cocaïne déjà en janvier**
L'année 2012 n'est vieille que de deux semaines et, déjà, les employés de l'Agence des services frontaliers du Canada (ASFC) ont effectué deux importantes saisies de cocaïne à l'aéroport Montréal-Trudeau. Au total, 7,5 kg de cette drogue ont été interceptés, pour une valeur de 340 000 $. Journal de Montréal, 5

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

It's a perilous - and political - road from 'evidence' to policy
An opinion piece states, "Too much is being made of Liberals voting 77% in favour, at this past weekend's convention, to legalize marijuana. It is an excellent idea, and the resolution ticks all the correct boxes by way of justifying it: marijuana's widespread and safe use, revenue savings and generation through taxation, and the fact it would make Canadians safer from criminal violence... But as Mr. Rae illustrated with his comments on marijuana, the road from evidence to policy will always be long, perilous and political. To pretend otherwise is to insult Canadians' intelligence." National Post, A15; * Red Deer Advocate, * L'Acadie Nouvelle

Dorval man says daughter's killer needs to stay in jail
Almost 18 years after finding his daughter, Tara Manning, fatally stabbed inside their Dorval home, Michael Manning is flying to Winnipeg to try to persuade the Parole Board of Canada to keep her killer behind bars. Manning said he wants to tell the parole board on Wednesday that Gregory Bromby, 34, is not ready for parole and should not be permitted to live in a halfway house. Gazette, A4

Killer abandons plan to seek early parole
A man convicted of killing his distant cousin in London 15 years ago has abandoned his application for early parole. Lang Nguyen, 47, was supposed to begin his so-called "faint hope clause" hearing this week. Middlesex Crown Attorney Geoff Beasley confirmed that the case would not be going forward. Nguyen, convicted of first-degree murder, won his chance to apply for parole almost a year ago. London Free Press, A7

You don't know Carjacking
An opinion piece states, "The number of auto thefts in Winnipeg may be down, but carjackings a steady pace last year. The Winnipeg Sun has learned there were 44 carjackings in Winnipeg in 2011. That's up slightly from the 43 recorded the previous year, according to the Winnipeg Police Service. And it's about twice as many carjackings as Winnipeg used to experience before government made after-market immobilizers mandatory for high-risk vehicles... The problem with car thefts and carjackings is we don't do enough to target the offender. We force victims and would-be victims to install after-market immobilizers in their vehicles. But we treat the actual criminals who steal the cars with kid gloves." Winnipeg Sun, 5

*** Prison farm protesters get day in court**
Eight holdout protesters, charged in the summer of 2010 over their attempts to stop the final dismantling of Frontenac Institution's farm program, began their trial Monday in Kingston's Ontario Court of Justice on charges of mischief by interfering with the lawful use of property. Kingston Whig-Standard, 1

*** Vancouver crime rate shows drop**
Crime is going down in Vancouver, police statistics indicate. Vancouver Mayor Gregor Robertson said the statistics indicate a decrease in crime over the past five years and that the VPD's crime strategy is working. The Province, A11

*** Crime Stoppers appeals to students for help, tips**
New Brunswick Crime Stoppers and the Government of New Brunswick have joined forces to make schools and communities safer with a new Crime Stoppers program for students. The program offers high school and college students a confidential and anonymous medium to report crimes without fear of reprisal or retaliation. Times & Transcript, A6

*** Tough love**
A letter states, "...The fact is drug prohibition supporters are responsible for the adulterated drugs presently killing our children. All this is eerily similar to the adulterated alcohol that caused death and blinding in the '30s. Prohibitionists seem to be callous people who would sooner send moral messages with the law to save souls than to repeal drug prohibition and save lives. In a free country, there should be no such thing as a crime against the state." Calgary Herald, A9

*** Fossilized thinking**
A letter states, "Much like Ronald Reagan's Just Say No policy of the 1980s, Dave Reesor's idea of harsh minimum penalties for drug producers belongs in a museum. Claiming that illegal organizations produce and distribute illegal drugs for anything but profit is an opinion-biased argument. Using the case study of the United States as an example for failed drug policy, it is clear that harsher prohibition has not affected the consumer demand for drugs in any way... How many more deaths will happen before our elected officials open their eyes to the true dangers of drug prohibition?" Calgary Herald, A9

*** Pas un danger?**
Un article d'opinion déclare, « Depuis l'énoncé de la sentence de Guy Turcotte, je suis totalement outré... Supposer qu'il puisse exister des circonstances atténuantes, en l'occurrence la folie, pour justifier un tel geste est aberrant et inacceptable... La société dans laquelle je veux vivre ne doit en aucun cas cautionner un tel comportement. Il ne faut d'aucune façon laisser à quiconque l'impression qu'il peut commettre un tel crime et pouvoir s'en tirer. Guy Turcotte ne doit pas recouvrer sa liberté avant longtemps, point final... » La Presse, A16

*** Murderer back in jail for violating his parole**
A man convicted of second-degree murder is headed back to prison after violating his parole. Christopher Alexander Falconer, 29, pleaded guilty Monday in Pictou provincial court to charges of possession of a prohibited weapon and possession of marijuana. He was sentenced to three months and one month, respectively, to be served concurrently. Chronicle Herald, A6

INTERNATIONAL / INTERNATIONAL

*** Tempest in a pee-pot**
NATO soldiers can shoot Taliban terrorists. They can bomb them from the air. They can fire missiles at them from remote-controlled drones. But they can't pee on their dead bodies. Edmonton Sun, 15 (Toronto Sun, Calgary Sun, Whig-Standard, Winnipeg Sun, Ottawa Sun)

*** The world must intervene in Syria**
A letter by Maher Arar states, "The signs are clear: Bashar al-Assad is in a state of desperation, and his latest speech in front of Syrian parliament proves it: having played most of the cards at his disposal in attempting to crush the Syrian uprising (including the murder of peaceful protesters), he is now playing his final card, the "patriotism" card, by insisting that the turmoil taking place in Syria is the result of a "foreign conspiracy." He has promised that he will resort to an "iron-first" approach to deal with the "terrorists" (i.e. peaceful protesters). If anything, this ad hominem attack shows how truly bankrupt his regime has become, to be so completely unable to offer any meaningful solutions to a nation that so badly wants freedom and political change..." Ottawa Citizen, A13

*** UN chief urges action on Syria**
UN chief Ban Ki-moon on Monday urged the Security Council to act on Syria as President Bashar al-Assad came under new pressure with defections and signs of increasing co-operation among his foes. Ottawa Citizen, A11

OTHER / AUTRE

Canada loses an Afghan ally
One of Canada's best Afghan friends was assassinated in Kandahar last Thursday. Haji Fazluddin Agha, the governor of Panjwaii district, was killed when his car was struck by a vehicle driven by a suicide bomber on a road funded and paved with Canadian help and protection. Two of Agha's sons, two policemen and a civilian, also died in the blast. A charismatic bear of a man with a booming voice and a lush black beard, Agha was a deeply pious Muslim. He detested Islamist zealots and was a fierce opponent of the Taliban and al-Qaeda. Ottawa Citizen, A6 (Windsor Star, Vancouver Sun, Calgary Herald)

*** Naval crew helps recover submarine packed with cocaine from sea floor**
Last fall, Canadian navy crews assisted in the recovery of a scuttled Caribbean submarine packed with more than 6,700 kilograms of cocaine, according to a weekend release by the Royal Canadian Navy. The submarine is a "self-propelled semisubmersible," a category of custom-built drug-smuggling vessels that have emerged over the past 10 years, largely in the hands of Colombian drug cartels. National Post, A5

Williston, Sandra

From: CYBERDO
Sent: January-18-12 2:34 PM
To: [redacted]
Cc: CTEC
Subject: RE: CE2012-272

s.15(1) - Def
s.16(2)(c)

CTEC;

CCIRC obtained the list from a public website; http://dazzlepod.com/stratfor/ which we used wildcard searches (ie: gc.ca) to find the information we sent you.

Therefore, we confirm that this information is releasable to the requestor.

Thanks!

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: [redacted]@CSE-CST.GC.CA]
Sent: January-18-12 2:13 PM
To: [redacted]
Cc: [redacted]
Subject: CE2012-272

Classification: UNCLASSIFIED

Good Afternoon CyberDO,

CBSA is requesting information for the Stratfor hack and for a list of Canadian Federal Depts. We received the information from you and I would like to verify with you whether or not we can release that information to them. Thanks.

[redacted]
Cyber Threat Evaluation Centre
[redacted]
ctec@cse-cst.gc.ca

From: CBSA/ASFC-IT SECURITY/SECURITE TI [mailto:CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca]
Sent: January 18, 2012 12:14 PM
To: [redacted]

Cc: Samulak, George
Subject: RE: Stratfor hack affects Government of Canada users

Can CTEC provide the following information regarding this hack:

# of Canadian Federal departments affected
List of the # of Canadian Federal departments affected

Regards,

s.15(1) - Def
s.16(2)(c)

George Samulak
Cyber Protection Centre/Centre de Cyber Protection
IT Security Division / Division Sécurité de la TI
Infrastructure Services Directorate / Services d'infrastructure
Information Science & Technology Branch / Direction Générale de l'information, des sciences & de la technologie
Canada Border Services Agency | Agence des services frontaliers du Canada
Government of Canada | Gouvernement du Canada
100 Metcalfe Street (1659), Ottawa, Ontario, K1A 0L8
george.samulak@cbsa-asfc.gc.ca
Telephone | Téléphone 613-952-6717
Facsimile | Télécopieur 613-952-7900
Teletypewriter | Téléimprimeur 1-866-335-3237

From: (redacted)
Sent: December 29, 2011 10:25 AM
To: (redacted)
Cc: (redacted)
Subject: Stratfor hack affects Government of Canada users
Importance: High

Classification: UNCLASSIFIED

Hello,

(redacted)

The hashes for all Stratfor accounts were released allegedly by Anonymous. Some passwords were discovered via a dictionary attack and posted on pastebin (redacted)

(redacted)

It is recommended that users immediately change any passwords on Government of Canada systems if they used the same or similar passwords. Please remind users that this illustrates the importance of using different passwords on different accounts and especially not to reuse passwords that are used on GC systems.

(redacted)

Regards,

[redacted]

s.15(1) - Def

[redacted]

GC-CTEC Cyber Duty Officer

Williston, Sandra

From: [redacted]@CSE-CST.GC.CA>
Sent: January-18-12 2:13 PM
To: CYBERDO
Cc: CTEC
Subject: CE2012-272

s.15(1) - Def

Classification: UNCLASSIFIED

Good Afternoon CyberDO,

CBSA is requesting information for the Stratfor hack and for a list of Canadian Federal Depts. We received the information from you and I would like to verify with you whether or not we can release that information to them. Thanks.

[redacted]
Cyber Threat Evaluation Centre
[redacted]
ctec@cse-cst.gc.ca

From: CBSA/ASFC-IT SECURITY/SECURITE TI [mailto:CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca]
Sent: January 18, 2012 12:14 PM
To: CTEC
Cc: Samulak, George
Subject: RE: Stratfor hack affects Government of Canada users

Can CTEC provide the following information regarding this hack:

# of Canadian Federal departments affected
List of the # of Canadian Federal departments affected

Regards,

George Samulak
Cyber Protection Centre/Centre de Cyber Protection
IT Security Division / Division Sécurité de la TI
Infrastructure Services Directorate / Services d'infrastructure
Information Science & Technology Branch / Direction Générale de l'information, des sciences & de la technologie
Canada Border Services Agency | Agence des services frontaliers du Canada
Government of Canada | Gouvernement du Canada
100 Metcalfe Street (1659), Ottawa, Ontario, K1A 0L8
george.samulak@cbsa-asfc.gc.ca
Telephone | Téléphone 613-952-6717
Facsimile | Télécopieur 613-952-7900
Teletypewriter | Téléimprimeur 1-866-335-3237

Page 1638

is a duplicate

est un duplicata

Dincoy, Rana

From: Bendelier, Kenneth
Sent: January-18-12 10:35 AM
To: Dincoy, Rana
Subject: Re: [redacted]

s.16(2)(c)

Ok, this was just for level of content reference anyway, not specific content

From: Dincoy, Rana
Sent: Wednesday, January 18, 2012 10:31 AM
To: Bendelier, Kenneth
Subject: RE: [redacted]

What's missing from this synopsis is that Anonymous claims they are not responsible for this hack... I found an "emergency Christmas Anonymous press release" in Pastebin stating this. I put that in the Weekly Summary...

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

From: Bendelier, Kenneth
Sent: January-18-12 10:21 AM
To: Dincoy, Rana
Subject: FW: CIIT Update - STRATFOR Breach

From: Scott Foster [mailto:Scott.Foster@rcmp-grc.gc.ca]
Sent: January-03-12 11:04 AM
To: Scott Foster
Subject: [redacted]

Good day,

Pages 1640 to / à 1641

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-18-12 9:06 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; [redacted] Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; CYBERDO; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted]; Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 18, 2012/ le 18 janvier 2012

Print Media / Médias imprimés

Cyber threats likely to increase
Any organization that believes it has shuttered all of the back door channels that hackers used to breach millions of systems last year should double check the locks in 2012, according to security experts. A cyber threat forecast by Kaspersky Lab, a Moscow Internet security firm, warns there is little doubt the cloud-based storage hack that took down Sony's PlayStation Network for more than a month will spread beyond gaming companies. The June hack of U.S.'s Citibank's database that stole information from more than 200,000 customers might not be an anomaly, the forecast said. And cyber weapons such as the Stuxnet worm that took down Iran's nuclear weapons program are expected to increase in numbers, even as hacks made in protest by so-called hacktivist organizations such as Anonymous will continue unabated. Even as the report warns everyone to gird for the attacks that are all too familiar, it also outlines emerging threats to mobile phones and energy company infrastructure. Red Deer Advocate, D7

Microsoft phone scam to blame for 70% of reports

A scam where callers pretend to be Microsoft employees offering to solve computer problems now accounts for 70 per cent of all fraud complaints in Canada, reports the Canadian Anti-Fraud Centre. The fraud artists claim they are with Microsoft and offer to help people rid their computers of malicious software. In the process, they charge as much as $400, collect credit card information and gain access to all of the personal files and contents on their victim's hard drive. According to the RCMP, the scam has been operating since February 2011. The RCMP said fraud has been elevated to new levels thanks to the emergence of the digital era. It is believed that Canadians are defrauded of between $10 billion and $30 billion annually. Ottawa Citizen, A1

Nouveaux outils de censure
L'encyclopédie collaborative en ligne Wikipedia a annoncé qu'elle suspendrait l'accès à sa version anglophone sur le Web toute la journée d'aujourd'hui pour protester contre une loi antipiratage examinée par le Congrès américain. Wikipedia, qui reçoit des millions de visites chaque jour, est considérée comme l'un des sites Web les plus populaires d'Internet. La fondation Wikipedia a fait valoir dans un communiqué que la loi «causerait du tort à Internet gratuit et libre et fournirait de nouveaux outils de censure des sites internationaux aux États-Unis». D'autres acteurs de poids d'Internet, comme Google, Facebook, Yahoo, Twitter, eBay et AOL sont contre la nouvelle législation. Plusieurs communautés en ligne, dont Reddit et Boing Boing, ont également prévu des opérations écran noir. Le Soleil, 35; Montreal Gazette

Father, son blamed for credit thefts
U.S. authorities on Tuesday unsealed criminal charges accusing a father and son team, both Russian citizens, of hacking into U.S. bank accounts and illegally snatching credit card numbers and stealing hundreds of thousands of dollars. Windsor Star, C2

Online Media / Médias en ligne

Trojan may have stolen data from Japanese space agency
Japanese space engineers have discovered a Trojan on an employee's computer and confirmed that hackers may have smuggled out login information to gain access to a cargo shuttle that carries food and equipment to the International Space Station (ISS). The compromised information may have included up to 1,000 email addresses, login details for the Japanese space agency's intranet, and NASA documents covering operation of the ISS, according to a statement from the Japanese Aerospace Exploration Agency (JAXA). On January 6th, JAXA found the virus on a terminal used by an employee who works with the H-II Transfer Vehicle (HTV), an unmanned cargo shuttle. Naked Security

Context warns of sophisticated new Trojans
Security consultancy, Context Information Security, has issued a warning regarding the sophisticated structure of financial malware, such as the Carberp Trojan, which is both difficult to detect and eliminate. Carberp targets log-in and account information, and harvests credentials for both email and social networking sites. Like its predecessors Zeus and Spyeye, Carberp operates through drive-by downloads and malicious files. Carberp remains undetected by antivirus software due to its advanced stealth, anti-debugging and rootkit techniques, composed of multiple layers of obfuscation and encryption. Context researchers have published a series of blogs that detail the process of their analyses. ARN Net

New stealthy botnet Trojan holds Facebook users hostage
A new strain of cybercrime Trojan is targeting Facebook users by taking over their machines and shaking them down for cash. Carberp, like its predecessors ZeuS and SpyEye, infects machines by tricking punters into opening PDFs and Excel documents loaded with malicious code, or attacks computers in drive-by downloads. The hidden malware is designed to steal account information, and harvest credentials for email and social-networking sites. A new configuration of the Carberp Trojan targets Facebook users to ultimately steal e-cash vouchers. Previous malware attacks on Facebook have been designed purely to slurp login info, so this latest skirmish, spotted by transaction security firm Trusteer, can be considered something of an escalation. The Carberp variant replaces any Facebook page the user navigates to with a fake page notifying the victim that their Facebook account is temporarily locked. Effectively holding Facebook users hostage, the page asks the mark for their first name, last name, email, date of birth, password and a Ukash 20 euro ($25) voucher number to verify their identity and unlock the account. Trusteer warns the cash voucher attack is in some ways worse than credit card fraud, because with e-cash it is the account-holder, not the financial institution, who assumes the liability for fraudulent transactions. The Register; Techworld

Microsoft hit by email scam
Fraudsters have attacked customers of the oft-targeted Microsoft with a phishing scam offering a £500,000 ($A739,000) financial reward. The scammers, masquerading as representatives of "Microsoft Office", offered the "financial aid award" to email recipients while requesting their personal information. The email purported to originate from an "LGHealth Email Service" in association with Microsoft. It mimicked the nature of legitimate email communication with a "confidentiality

notice" urging victims to contact the sender by reply email and destroy all copies of the original message if not the intended recipient. The scam is the latest in a series of phishing operations targeting Microsoft users. CRN

Phishing your employees in the name of security
A new open source toolkit makes it ridiculously simple to set up phishing websites and lures. The software was designed to help companies test the phishing awareness of their employees, but as with most security tools, this one could be abused by miscreants to launch malicious attacks. The Simple Phishing Toolkit includes a site scraper that can clone any web page — such as a corporate intranet or webmail login page — with a single click, and ships with an easy-to-use phishing lure creator. Sydney Morning Herald

Flaw in Facebook & Google Allows Phishing, Spam & More
Here's a nasty little Null Byte. An open redirect vulnerability was found in both Facebook and Google that could allow hackers to steal user credentials via phishing. This also potentially allows redirects to malicious sites that exploit other vulnerabilities in your OS or browser. This could even get your computer flooded with spam, and these holes have been known about for over a month. Normally, holes like this are fixed within a few hours, but Google and Facebook don't seem to care too much. Google does not offer their regular Vulnerability Reward for this kind of exploit. So, we will be going over how this exploit could be used against us and how to protect ourselves from it. Maybe this will encourage Google and Facebook to push their developers into fixing these holes as soon as possible. Business Insider

McAfee software lets scammers hijack PCs to send spam
McAfee is looking into a problem with a service in its SaaS Endpoint Protection software that appears to be allowing computers to serve as open proxies for sending spam, the company told CNET today. The problem was reported by McAfee customers on the Web who complained that their e-mails were being blocked by e-mail providers and their IP addresses were being blacklisted for sending spam. The problem appears to be in the RumorServer Service myAgtSvc.exe, McAfee Peer Distribution Service, which is part of McAfee SaaS Endpoint Protection Suite, previously known as Total Protection Service, according to the Kaamar Blog. The technology, used for delivering updates to computers without a direct Internet connection, serves as an Open Proxy on Port 6515, which effectively opens the computer up to being used by spammers to use the computer to send spam to other sites that looks like it is coming from that IP address, the blog post says. CNet; eSecurity Planet; IT Pro Portal

Phishing your employees in the name of security
A new open source toolkit makes it ridiculously simple to set up phishing websites and lures. The software was designed to help companies test the phishing awareness of their employees, but as with most security tools, this one could be abused by miscreants to launch malicious attacks. The Simple Phishing Toolkit includes a site scraper that can clone any web page — such as a corporate intranet or webmail login page — with a single click, and ships with an easy-to-use phishing lure creator. Sydney Morning Herald

Facebook "Free Mobile Recharge" scam hijacks accounts
A phishing and survey scam rolled into one is currently targeting Facebook users and ends up hijacking their accounts and making it difficult for users to get them back, warns a McAfee researcher. The victims are lured with messages seemingly posted by their friends claiming that they have received a "100rs free recharge". Following the offered link, they land to a page asking them to enter their Facebook login credentials in order to get it. The scammers then use the login credentials to access the victims' Facebook accounts, change information contained in them (including the password and the email address) and post the same message that lured in the victims in the first place. Help Net Security

Phishing E-mail Scam Attacks US-CERT
US-CERT the United States Computer Emergency Readiness Team reports that it's presently a target of an enormous phishing campaign. SCMagazine.com.au published this on January 11, 2012. It's worth noting that US-CERT coordinates security measures as well as deals with cyber assaults all over the USA. Moreover, it's run under the U.S. DHS (Department of Homeland Security). The Computer Emergency Response Team, following the latest phishing scam's appearance on January 10, 2012, issued an online security alert to all Internauts, stating that the cyber-criminals had impersonated the electronic mail addresses of US-CERT so they could target many local, state and federal governments along with private sector companies. Also an e-mail handler working at US-CERT stated that the phishing e-mail scam had been causing him trouble in receiving messages. The phishing message reportedly, has a .zip file as an attachment, which carries one malicious .eml.exe executable named "US-CERT Operation Center Reports." Captioned as "Phishing incident report," the e-mail contains one telephone number too. The sender's id displayed as soc@us-cert.gov is spoofed to make the e-mail appear from US-CERT; however, the agency points out other illegitimate ids that are also included. SPAMfighter

Malware targets smart ID cards, say researchers

Cybersecurity researchers say they've uncovered a variant of malicious software known as Sykipot that specifically targets smart identity cards used by a number of federal agencies, including the departments of Defense and Homeland Security. In a July 12 blog post, researchers from alienvault labs say the variant appears to have been compiled in March 2011. Once downloaded onto a computer via a phishing attack (in which an email containing an infected attachment or link to a malware-controlled website appears to originate from a legitimate source), the Sykipot variant uses a keylogger to steal PINs users enter to authenticate their identity, the Campbell, Calif.-based company says. Fierce Homeland Security

Israël: des pirates affirment avoir touché le site de la bourse saoudienne
Un groupe de pirates informatiques israéliens a affirmé mardi s'être introduit sur les sites des bourses de Ryad et d'Abou Dhabi, pour répliquer à des cyberattaques lancées la veille contre plusieurs sites israéliens, ont rapporté des médias israéliens. La Presse; Arutz Sheva; Financial Times

Saudis deny stock exchange website infiltrated by Israeli hackers
Saudi Arabian authorities on Wednesday denied claims that Israeli hackers had crippled the website of the oil-rich country's capital market, saying the system was operating normally. Israeli hackers claimed they brought down the websites of both the Saudi Stock Exchange (Tadawul) and the Abu Dhabi Securities Exchange (ADX) on Tuesday, in the latest episode of a continuing cyber war between hackers in Israel and other countries. The Israeli hackers, who go by the name IDF-Team, said on Tuesday they were able to paralyze the Tadawul website, while causing significant delays to the ADX exchange site. Haaretz

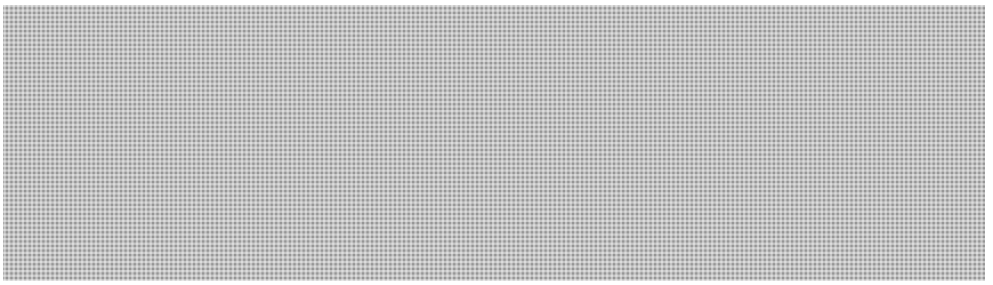
Facebook, Researchers Reveal Gang Behind Koobface Virus
Facebook said Tuesday that it will share the data it has collected about the group of people behind the Koobface virus that hit the social network in 2008. Koobface targeted Facebook users via fake friend messages that encouraged people to click on links that installed a malicious worm. Facebook said Tuesday that it will share the data it has collected about the group of people behind the Koobface virus that hit the social network in 2008. Koobface targeted Facebook users via fake friend messages that encouraged people to click on links that installed a malicious worm. Security researcher Dancho Danchev has also posted his analysis of the Koobface gang online. According to the research, Koobface scammers basically got sloppy. The "Koobface Mothership" was found to be in Prague, but researchers also found that daily stats were being sent via text messages to Russian telephone numbers. Ultimately, the Koobface gang was identified by the researchers as Anton Korotchenko, Alexander Koltyshev, Roman Koturbach, Syvatoslav Polinchuk, and Stanislav Avdeik. PC Magazine; The Register; redOrbit; Herald Sun; ZDNet; Forbes; The Telegraph (UK)

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From: Beaudoin, Luc S **s.16(2)(c)**
Sent: January-18-12 9:49 AM
To: Phlek, Vireak
Cc:
Subject: Activity 3402

[redacted]



s.16(2)(c)

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: January-18-12 12:06 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous publishes hacked Stratfor emails

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Inquirer
Complete item: http://www.theinquirer.net/inquirer/news/2139335/anonymous-publishes-hacked-stratfor-emails

Description:
HACKTIVIST GROUP Anonymous has released two sets of teaser emails retrieved from a recent attack on servers at the security intelligence firm Stratfor.

The well-known group successfully targeted the firm recently and managed to access its customers' credentials including unencrypted credit card details. It also got hold of internal emails. which it has started to publish online.

Anonymous has posted two teaser emails on Pastebin that were obtained in the hacking attack. The first is a strange set of emails containing abuse and even a marriage proposal involving Michael McCullar, senior editor of special projects at Stratfor.

E-Secure-IT
https://www.e-secure-it.com

Hayward, Jane

From: Glazer, David on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-18-12 8:01 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 18, 2012 / le 18 janvier 2012

MINISTER / MINISTRE

Pilot dies in RCMP chopper crash
RCMP pilot Dave Brolin died Tuesday after a training exercise with the emergency response team turned into a real-life emergency. **"I would like to extend my heartfelt condolences and deepest sympathy to the family, friends and colleagues of Dave Brolin who lost his life today," Public Safety Minister Vic Toews said in a statement.** The Province, A3

Letters to the Editor Column
A letter states, "Brian Lilley is right on the money when he says "it's time for **(Vic) Toews** and the rest of the Harper government to wake up and fix this mess." Confiscating legally owned property without compensation is the kind of thing one would see in banana republics..." Winnipeg Sun, 8

EMERGENCY MANAGEMENT AND NATIONAL SECURITY / GESTION DES MESURES D'URGENCE ET SÉCURITÉ NATIONALE

*** It was a long dam wait**
Sakimay First Nations could receive a $21-million settlement to satisfy a longstanding flood claim, following years of negotiations with the federal and provincial governments, Chief Lynn Acoose said Tuesday. The federal government has also made an offer to settle with Cowessess First Nation, although it has not make the dollar figure public. Leader-Post, A3

*** 500 000 masques dorment chez Élections Canada**
La peur de la grippe A (H1N1) durant la pandémie, en 2009, a poussé Élections Canada à surprotéger les électeurs, si bien que près de 500 000 masques chirurgicaux et des milliers de bouteilles de désinfectants pour les mains dorment toujours dans les bureaux de l'agence gouvernementale. Selon les informations obtenues par le Journal en vertu de la Loi d'accès à l'information, Élections Canada cherche d'ailleurs à se départir de ces articles, dont la plupart sont périmés ou sur le point de l'être. Journal de Montréal, 6

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Canada joins military satellite program**
The federal government will spend more than $337 million on military satellites designed to help soldiers in the field stay informed, and keep government information secret. Defence Minister Peter MacKay said Tuesday that by joining the $10-billion Global Wideband Satellite program, or Mercury Global, Canada will be able give soldiers in the field real-time analysis as events unfold anywhere around the globe. The federal government will spend $337.3 million to buy Canada 20 years of access to the satellite network, effective immediately, and fund the construction of one of 10 satellites planned for the network. Leader-Post, B7 (Starphoenix, Windsor Star, Times & Transcript)

CYBER SECURITY / CYBERSÉCURITÉ

*** Cyber threats likely to increase**
Any organization that believes it has shuttered all of the back door channels that hackers used to breach millions of systems last year should double check the locks in 2012, according to security experts. A cyber threat forecast by Kaspersky Lab, a Moscow Internet security firm, warns there is little doubt the cloud-based storage hack that took down Sony's PlayStation Network for more than a month will spread beyond gaming companies. The June hack of U.S.'s Citibank's database that stole information from more than 200,000 customers might not be an anomaly, the forecast said. And cyber weapons such as the Stuxnet worm that took down Iran's nuclear weapons program are expected to increase in numbers, even as hacks made in protest by so-called hacktivist organizations such as Anonymous will continue unabated. Even as the report warns everyone to gird for the attacks that are all too familiar, it also outlines emerging threats to mobile phones and energy company infrastructure. Red Deer Advocate, D7

*** Microsoft phone scam to blame for 70% of reports**
A scam where callers pretend to be Microsoft employees offering to solve computer problems now accounts for 70 per cent of all fraud complaints in Canada, reports the Canadian Anti-Fraud Centre. The fraud artists claim they are with Microsoft and offer to help people rid their computers of malicious software. In the process, they charge as much as $400, collect credit card information and gain access to all of the personal files and contents on their victim's hard drive. According to the RCMP, the scam has been operating since February 2011. The RCMP said fraud has been elevated to new levels thanks to the emergence of the digital era. It is believed that Canadians are defrauded of between $10 billion and $30 billion annually. Ottawa Citizen, A1

*** Nouveaux outils de censure**
L'encyclopédie collaborative en ligne Wikipedia a annoncé qu'elle suspendrait l'accès à sa version anglophone sur le Web toute la journée d'aujourd'hui pour protester contre une loi antipiratage examinée par le Congrès américain. Wikipedia, qui reçoit des millions de visites chaque jour, est considérée comme l'un des sites Web les plus populaires d'Internet. La fondation Wikipedia a fait valoir dans un communiqué que la loi «causerait du tort à Internet gratuit et libre et fournirait de nouveaux outils de censure des sites internationaux aux États-Unis». D'autres acteurs de poids d'Internet, comme Google, Facebook, Yahoo, Twitter, eBay et AOL sont contre la nouvelle législation. Plusieurs communautés en ligne, dont Reddit et Boing Boing, ont également prévu des opérations écran noir. Le Soleil, 35; Montreal Gazette

*** Father, son blamed for credit thefts**
U.S. authorities on Tuesday unsealed criminal charges accusing a father and son team, both Russian citizens, of hacking into U.S. bank accounts and illegally snatching credit card numbers and stealing hundreds of thousands of dollars. Windsor Star, C2

LAW ENFORCEMENT AND POLICING BRANCH / SECTEUR DE LA POLICE ET DE L'APPLICATION DE LA LOI

La commission Charbonneau devra se pencher sur la mafia
La commission d'enquête Charbonneau devrait élargir son mandat et se pencher sur l'infiltration de la mafia dans certains corps publics de la société, souhaite le Parti québécois. Journal Montreal, 2

Retired Montreal cop tried to sell secrets to Mafia
Montreal's police chief is promising swift action after reports that a retired officer allegedly tried to sell information on stoolies to the Mafia. Marc Parent said Tuesday the 33-year veteran of the force worked in the intelligence unit and was one of a handful of people who had access to a confidential list of names. The Guardian, A5 (Globe and Mail, The Record); Journal Montreal; * The Gazette (Windsor Star, Edmonton Journal); * Le Devoir; * Le Soleil; * La Presse

No public inquiry into death
There will be no public inquiry into the death of Paul (Poncho) Henderson, the Miramichi Leader Liberal Miramichi-Bay du Vin MLA Bill Fraser revealed Monday **Department of Public of Safety** officials confirmed they would not push for an inquiry. Months ago, Fraser submitted a petition bearing 2,000 signatures in the legislature calling for the provincial government to order a review of the investigation into the teen's death in 1981. Daily Gleaner, A6

Pilot of RCMP helicopter dies in crash
The pilot and sole occupant of an RCMP helicopter died Tuesday in a crash in British Columbia. He was a civilian member with "several" years of experience with the RCMP and "extensive" experience as a pilot, said Chief Supt. Wayne Rideout, the RCMP E Division's deputy criminal operations officer. Times Colonist, A2 (Leader-Post, Edmonton Journal); The Telegram; * Globe and Mail (Vancouver Sun); * Windsor Star; * Calgary Sun

Experts say spy case could be damaging
The Harper government hunkered down Tuesday in an attempt to weather an unfolding spy drama involving a naval officer who worked at one of the most sensitive and secure military intelligence centres in the country. Prime Minister Stephen Harper, Defence Minister Peter MacKay, the military and the RCMP turned aside questions on the case of Sub.-Lt. Jeffrey Paul Delisle, who's charged with communicating information to a foreign entity. Defence experts said, given where the suspect worked, the potential damage to national security was immense. The Guardian, A5 (Red Deer Advocate, Hamilton Spectator, Chronicle-Herald); * Globe and Mail; * Windsor Star (Telegraph-Journal); * Whig-Standard; * The Record; * Chronicle-Herald; * Chronicle-Herald; * Chronicle-Herald; * Journal Montreal

Bank documents questioned in trial of Mountie accused of fraud
Admissibility of a bank of evidence has been called into question in the trial of a Mountie accused of extortion, criminal harassment and fraud. RCMP Const. Hoa Dong La, in a judge-alone trial before Justice David Gates in Red Deer Court of Queen's Bench, is accused of using a variety of tactics for monetary gain involving five different properties in Innisfail and Bowden and in the rural area near Bowden Institution. He faces 15 counts altogether, including three counts of extortion, two of criminal harassment and 10 of mortgage fraud. Red Deer Advocate, A3

*** New police watchdog hits ground running**
A dinner conversation with his father years ago helped set Richard Rosenthal, the new director of B.C.'s independent police investigations office, down a path that would one day see him investigate judges and take on the Los Angeles Police Department. As the head of an office that probes police incidents that result in serious harm or death, Rosenthal will inevitably be thrust into an adversarial role with B.C.'s municipal police forces and, perhaps more dramatically, with a provincial RCMP force that's still seeing double after a string of black eyes. The Province, A4

*** Le député de Manicouagan appelle la GRC en renfort**
Ottawa doit demander à la GRC d'intervenir "de manière musclée" contre les trafiquants d'amphétamines (speed) dans les communautés innues du Québec, affirme le député fédéral de Manicouagan, Jonathan Genest-Jourdain. La Presse, A6

*** Roberval**
Neuf arrestations ont été faites à Roberval, hier, au terme de 12 perquisitions menées par la Sûreté du Québec et la Gendarmerie royale du Canada. L'opération Intérim a mobilisé 90 policiers. Les personnes ont été mises en état d'arrestation pour leur participation à un réseau organisé de trafic de stupéfiants au Lac-Saint-Jean. La Presse, A14

*** L'enquête s'est échelonnée sur plus d'un an**
L'opération de lutte antidrogue "Intérim", qui a été menée hier par la Sûreté du Québec et la Gendarmerie royale du Canada (GRC), est le fruit d'une enquête qui s'est échelonnée sur une période de plus d'un an. Le Quotidien, 6

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Affaire Pickton
Le fait que la GRC ait possédé pendant cinq ans des preuves liant Pickton à deux prostituées disparues a été présenté comme une preuve que les policiers travaillant sur l'affaire ont été incapables d'empêcher le tueur en série d'assassiner davantage de femmes. L'avocate de la GRC Cheryl Tobias a cependant indiqué qu'il n'y avait jamais eu de raison d'examiner les vêtements pour y trouver de l'ADN, puisque l'identité du suspect et celle des victimes étaient connues. Pickton n'a jamais nié son implication, mais a plutôt clamé l'autodéfense. La Presse, A14

No reason for DNA test in 1997: lawyer
Suggestions that the RCMP should have tested clothing seized from Robert Pickton in 1997 for DNA sooner are hindsight, but the facts are there was no reason for investigators working on an attempted murder case at the time to test them, a federal government lawyer told a public inquiry. Mr. Pickton's clothing and a pair of handcuffs were seized after a brutal attack on his farm in Port Coquitlam, B.C., which left a prostitute from Vancouver's Downtown Eastside near death with severe stab wounds. Globe and Mail, S2 (Red Deer Advocate)

*** RCMP made mistake refusing Pickton's offer, inquiry told**
Two RCMP officers should have followed up on an offer by serial killer Robert Pickton to let them search his farm as early as 2000, the Missing Women Inquiry heard Tuesday. Leader-Post, B10 (Edmonton Journal, Times Colonist)

*** Ontario cop at odds with RCMP lawyer**

An Ontario deputy police chief on the stand at the Missing Women Commission of Inquiry refused Tuesday to agree with an RCMP lawyer that there was no point in the Mounties accepting Robert Pick-ton's invitation to search his farm in 1999. Jennifer Evans, Peel Region-al Police deputy chief who analyzed the police probe into Pickton, produced a 2010 report that documents that cops knew for years that Pickton's farm was rife with evidence. The Province, A14

*** Gaps in policing must be bridged**
An editorial states, "Jennifer Evans, the deputy police chief in the Peel regional police in Ontario, didn't offer much that we didn't already know when she spoke at the Missing Women Commission of Inquiry this week. We already knew what she had to say. There is really only one question: Will police act on that knowledge? Evans told the inquiry that it is still possible for serial killers such as Robert Pickton and Paul Bernardo to escape detection by operating in more than one police jurisdiction..." Times Colonist, A12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** Yank busted for kid porn**
A Minnesota man has been arrested and detained in Manitoba to face allegations he was trying to smuggle explicit child pornography into Canada. Kirk Douglas Therneau, 54, was arrested by Canada Border Services Agency investigators at the Emerson border crossing Sunday and transported to Winnipeg where his charges appeared in court Tuesday. Winnipeg Sun, 7

*** Legal aid being cut off to Roma, lawyer says**
An Ottawa refugee lawyer says Legal Aid Ontario has started to deny funding to most Roma asylum-seekers, but won't explain why. Without legal representation, Kaplan said, his Roma clients, who are illiterate and speak no English, have little chance of success before the IRB. If their claim is denied, they'll be deported back to Poland, where Kaplan said they'll face violent threats from neo-Nazis and systemic discrimination in education, employment and health services. Ottawa Citizen, C1

*** Refugee bid felled by crimes in Punjab**
A refugee claimant who settled in Montreal with his wife after leaving his long-time job with a paramilitary force in India has been ordered out of Canada for complicity in crimes against humanity during the brutal suppression of a separatist insurgency in the Punjab. National Post, A6

*** Une autre voix s'élève contre la déportation de Mugesera**
Alors que Léon Mugesera est toujours détenu au Centre de prévention de l'immigration de Laval en attendant son éventuelle déportation, une autre voix s'est élevée hier contre la décision d'Ottawa de retourner le Rwandais accusé d'incitation au génocide dans son pays d'origine pour qu'il soit jugé devant ses pairs. Le Soleil, 4

*** Send Mugesera back**
A letter states, "...The obvious thing to do, of course, is to send Léon Mugesera back to Rwanda, to be judged by the people of his own country. If the Anti-Torture Committee is worried that he will be mishandled there, let it insist on being allowed to appoint its own representatives to follow the judicial proceedings there. But this might, of course, be too much real work for said committee." The Gazette, A18

*** Seeking new life, finding gang life**
They come from a war-torn nation looking for a fresh start in Friendly Manitoba. Yet, some African immigrants have learned the kindness only extends so far, and a failure to comply with the law can mean a ticket back home. As a boy in Somalia, Yassim Ibrahim saw his father murdered. He immigrated to Winnipeg in 1999 with his mother and four siblings, and in less than 10 years, at age 23, he was the godfather of the Mad Cowz street gang. His criminal record included the attempted murder of a rival gang member. Ibrahim was deported back to Somalia. Winnipeg Free Press, A4

*** Pharma boss faces U.K. extradition for stolen drugs**
The former head of a Richmond pharmaceutical company is facing extradition to the United Kingdom after being caught allegedly possessing $9-million worth of stolen drugs in 2007. A committal hearing for Mahmood Sheraly Aziz is scheduled for B.C. Supreme Court in Vancouver next week. Aziz, who was arrested in Canada last March, is out on bail, according to the federal justice branch. Vancouver Sun, A2

*** Deportation order deferred**
Lucene Charles's removal from Canada has been deferred, according to a letter received by Charles and her supporters. On Monday, the Canadian Border Services Agency (CBSA) faxed the reprieve letter to one of her supporters. It reportedly says her deportation to the Caribbean island has been deferred until further notice. The letter was read aloud

to The Spectator by Charles and two of her supporters, including Archdeacon Rick Jones of St. Paul's Anglican Church. Hamilton Spectator, A2; Hamilton Spectator

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Stiffer ecstasy laws spark turn to new pills
New tough laws cracking down on ecstasy production in British Columbia have had the unintended consequence of opening the door to more toxic, fake ecstasy pills, a criminologist says. The synthetic drug PMMA wasn't on the radar for police or the public until last week, when the BC Coroners Service announced the "new" unregulated chemical had been linked to at least five ecstasy-related deaths in B.C. in the past six months, and a number of deaths in Alberta. Leader-Post, B7

*** Haitian-born killer granted aboriginal parole hearing**
When convicted murderer Gregory Bromby faces a Winnipeg parole board on Wednesday, the hearing will be conducted in a circle rather than across a table, the smell of burning sweetgrass, cedar or tobacco will likely fill the room due to a ceremonial process known as "smudging" and an aboriginal elder will open and close the hearing with a prayer. Bromby has requested an "aboriginal elder-assisted parole board hearing." The thing is, the Haitian-born 34-year-old is not aboriginal. National Post, A1, Edmonton Sun (Winnipeg Sun), La Voix de l'Est

*** Legal pot**
An editorial states... "In the meantime, on The Gazette's Facebook page (facebook.com/ montrealgazette), we asked readers whether they think there should be a Gazette editorial endorsing legalization. Here are some responses: 'I don't use it myself but yes, it should be legalized. Regulate and tax it as we do alcohol. When drugs are available in prison, you know you've pretty much lost the war on drugs. If marijuana is going to remain illegal then you'll have to ban alcohol, too. End the hypocrisy.'..." The Gazette, A19

*** City sex offender jailed**
A sex offender who admitted to failing to apprise authorities he'd moved was sentenced to 30 days behind bars Tuesday. Toby Peter Lloyd Forrest, 38, of 72 Regent St., Apt. 123, pleaded guilty in provincial court Tuesday failing to register as a sex offender as required by a court order between March 31, 2010, and Oct. 12, 2011, and failing to notify the sex offender registry of a change of address. Daily Gleaner, A6

*** Violent gangster may be in Manitoba: RCMP**
A violent gang member is eluding cops and could be in Manitoba. Thomas Gordon Bear was released from Saskatchewan Penitentiary on Aug. 2, on parole for a 45-month sentence. Police say he walked away from his halfway house Sept. 19. RCMP then issued a Canada-wide warrant for his arrest. Bear is a known member of the Native Syndicate, Mounties say. Winnipeg Sun, 13

*** Judge reserves decision on defence of necessity**
Justice Rommel Masse will give his decision in March on whether eight hold-out Save Our Prison Farm protesters are entitled to a defence of necessity, covering their methods in trying to prevent removal of the dairy herd from Frontenac Institution in August 2010. The eight were all charged individually with mischief by inter-f ering with the lawful use of property, during a two-day demonstration centred on the main access road into Collins Bay Penitentiary and the adjacent Frontenac Institution. Kingston Whig-Standard, 1

*** Database opens door to drug dens' pasts**
A new Ottawa company will list homes that housed former drug operations on the first registry of its kind in the country. HomeProof, set to launch next month, will provide insurance claim information, as well as the criminal pasts of houses to realtors -- for a fee. Ottawa Sun, 6

*** Warrant out for sex offender**
Vancouver police are searching for Kevin Scott Miller, wanted Canada-wide for breach of a long-term supervision order. Miller has a history of sex offences involving women and teenage girls. Police believes he is at high risk to re-offend violently and sexually. Toronto Sun, 30

*** Judge spares lifetime con lengthy prison sentence**
Joseph Davis has spent a lifetime proving he can't function in society for long before turning back to crime and ending up behind bars. But the Winnipeg drifter's grim history and bleak outlook wasn't enough to stop a Manitoba judge from giving

him one more chance to succeed. Davis, 43, was spared an indefinite prison sentence Friday after the Crown lost its battle for a rare dangerous offender designation. Winnipeg Free Press, B3

*** Hallelujah! Canadians agree it's time to legalize marijuana**
An opinion piece states, "A new poll suggests Canada may have reached the tipping point and a 66-per-cent majority favours legalizing marijuana. Hallelujah! Finally we might get a sensible public policy discussion in this country about what to do about a relatively benign substance that has been demonized and outlawed for a century yet is as readily available in schoolyards as cigarettes... Let's treat marijuana and other drugs as a health issue rather than a crime. It's cheaper, better for our communities and safer for kids. It would let police focus on real criminals, ease the burden of overloaded, backlogged courts and save a fortune in expensive legal and penal costs..." Vancouver Sun, A5

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Un fardeau de 143 milliards $**
Les divers régimes de pension des employés du gouvernement canadien les fonctionnaires, les policiers, les militaires, les juges, les députés et les sénateurs représentent un imposant boulet financier pour les contribuables canadiens: 143 milliards de dollars. Cette somme représente la totalité des engagements financiers non capitalisés du gouvernement fédéral envers les caisses de retraite de ses employés au 31 mars 2010, selon des documents obtenus par La Presse en vertu de la Loi sur l'accès à l'information. Le Nouvelliste, 18 (Le Droit)

*** Tory spending cuts are welcome news**
An editorial states, "Those concerned with the Harper government's rather liberal spending patterns -- that would be us -- were somewhat pleased with the new report coming out of the Parliamentary Budget Office that the brakes have already been applied. The credit card has been put away... Parliamentary budget chief Kevin Page has now told us that Ottawa has cut back on its spending -- very quietly, obviously -- by 3% over the first six months of the current fiscal year. If this holds true, it puts the Harper government on the right path towards its promised 5% cut to its estimated $80-billion direct program funding budget by 2013-14. Spending on operating expenditures, for example, is down 4%, and capital spending is down a whopping 15%....Unlike critics from the left, however, we do not mind the spending of money to bolster public safety -- like more than doubling the money spent on the border security agency that is now tracking down and deporting wanted criminals from foreign lands who have found sanctuary within our too-soft borders. Or spending serious dollars to build more prisons so that more violent criminals and sexual offenders get a jail cell rather than a laugh track to undeserved freedom." Kingston Whig-Standard, 4

INTERNATIONAL / INTERNATIONAL

*** Terror suspect avoids deportation**
The radical cleric Abu Qatada won his case to avoid being deported to Jordan Tuesday after judges ruled his human rights would be breached. The European Court of Human Rights said that Qatada, once described as Osama bin Laden's righthand man in Europe, could not be sent to Jordan because there was a risk he would be tried with evidence gained by torture, which would amount to a "flagrant denial of justice." However, the Strasbourg court upheld Britain's policy of attempting to deport terrorist suspects to countries that have given assurances that they will not use inhuman treatment. Ottawa Citizen, A13; National Post; Edmonton Journal

OTHER / AUTRE

*** UN gang's key cartel contact gunned down in Mexico**
A B.C. man executed in the Mexican state of Sinaloa this week was a high-ranking member of the United Nations gang who had direct contact with Mexican cartels, The Vancouver Sun has learned. Salih Abdulaziz Sahbaz, 37, spent much of the last three years in Mexico and was the key cartel contact for the notorious B.C. gang, police sources confirmed. Vancouver Sun, A4

*** Suspect charged with trying to kill Obama**
A man accused of firing shots at the White House in November has been formally charged with attempting to assassinate U.S. President Barack Obama, according to an indictment unsealed Tuesday. A preliminary psychiatric evaluation in December found Oscar Ortega-Hernandez, 21, competent to stand trial, but federal prosecutors are asking for more extensive tests to ensure he can be held legally liable. Edmonton Journal, A19

*** Canadian on death row in Iran**

Hope is fading for a Richmond Hill man, Saeed Malekpour, who has lost his final appeal against a death sentence in Iran. "The branch of the Supreme Court responsible for (his) case announced to one of his lawyers that the court reached the decision to have the death sentence carried out," says Maryam Nayeb Yazdi, a Toronto-based human rights activist. Malekpour, a 35-year-old Canadian permanent resident, was awaiting citizenship when he was arrested. Hamilton Spectator, A8

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-19-12 8:12 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 19, 2012 / le 19 janvier 2012

MINISTER / MINISTRE

Police need more online surveillance power, Ottawa says
Canadian law enforcement officials have never been hindered by having to abide by the country's current privacy laws, say documents revealed Wednesday, yet Ottawa remains adamant police need more online surveillance powers. Vancouver-based advocacy group OpenMedia.ca published details of an internal Canadian Association of Chiefs of Police (CACP) email message to its members who represent more than 90% of the country's police community. The message, OpenMedia says, asks CACP members to provide examples, even those with "confidential operational information," of investigations thwarted by Canada's privacy legislation. The goal of the call for case studies would appear to be to justify the federal government's proposed lawful access legislation. Responding to criticism from a Liberal Party MP during question period in the House of Commons last November, **Public Safety Minister Vic Toews** said opponents to lawful access were "***putting the rights of child pornographers and organized crime ahead of the rights of lawabiding citizens***." Despite the obvious need to respond to digital crimes, no systematic case has yet been made to justify Canada's government legislating new surveillance powers over the Internet, federal Privacy Commissioner Jennifer Stoddart said in a recent letter to **Mr. Toews**. The only case presented as justification was presented by then **Public Safety Minister** Peter Van Loan in 2009, who mentioned a kidnapping incident where police had to wait 36 hours to obtain a warrant. **Public Safety Canada** has said the legislation follows similar policies recently adopted by the United States, Australia, Germany and Sweden and "***strikes an appropriate balance between the investigative powers used to protect public safety and the necessity to safeguard the privacy of Canadians.***" "***No legislation proposed by our Conservative Government will allow police to unlawfully read emails without a warrant. Claims to the contrary are baseless,***" **Public Safety spokesperson Julie Carmichael** said via email Wednesday. "***As technology evolves, many criminal activities - such as the distribution of child pornography - become much easier. We are proposing measures to bring our laws into the 21st century and provide police with the tools they need to do their job.***" "***Rather than making things easier for child pornographers and organized criminals, we call on all Canadians to support these balanced measures***," she said. National Post, FP12

Police identify pilot killed in RCMP chopper crash
Police have identified the pilot who was killed Tuesday in the crash of an RCMP helicopter as 46-year-old David Brolin. Brolin, a civilian RCMP member, was Air 5's sole occupant during a training exercise east of Cultus Lake, B.C. "***This is a very sad day for all Canadians***," **Public Safety Minister Vic Toews** said in a statement late Tuesday. "***The death of a member of our national police force is a sobering reminder of the sacrifices and bravery of the men and women who serve each day to keep our communities safe.***" London Free Press, B3 (Edmonton Sun, Kingston Whig-Standard)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** No clear evidence Tamiflu works, researchers say**
Concerns are emerging that governments around the world may have wasted billions of dollars and even put people at risk by stockpiling Tamiflu to treat influenza. Globe and Mail, L6; Edmonton Sun

*** Non-vaccinated staff killing us, expert warns**
Thousands of Canadians die needlessly each year because health-care workers won't get flu shots, a leading expert says. London Free Press, A1

*** Protecting wetlands key in flood defence**

An opinion piece states, "Flooding was a problem not only in Manitoba this past year, but it was also a major issue in Saskatchewan. Both provinces faced enormous costs associated with lost crops, washed out roads and culverts, and in some cases, people lost their homes. In fact, flooding in Manitoba will cost taxpayers $1 billion in damages and flood-fighting efforts. This wasn't the first year Manitoba was forced to deal with water issues. We've been plagued by a number of consecutive wet years in areas throughout the province, affecting people's livelihoods and causing tremendous emotional stress and hardship for hardworking Manitobans -- those enduring the real costs of the flood. Yet, as a province, we haven't done nearly enough in terms of implementing real solutions to this recurring issue..." Winnipeg Sun, 9

*** Could La Nina predict flu pandemics?**
The weather phenomenon known as La Nina, or the appearance of waters that are cooler than normal in the eastern and central Pacific Ocean, may be responsible for more than just changes to global weather patterns. It could also play a role in worldwide flu pandemics, according to a researcher at Columbia University whose study has been published in the journal Proceedings of the National Academy of Sciences. Toronto Star, A26

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Man files human rights claim against Gatineau
A man has filed a complaint with Quebec's Human Rights Commission after he says he was singled out by the City of Gatineau for criticizing a controversial immigrant values guide. Kamal Maghri, who has lived in Canada for 11 years and works for the federal government, said he was shocked when he discovered that a city official had been investigating him. Maghri said the official was digging up details on his finances and even mentioned to other government officials that he had come to Canada just after the Sept. 11, 2001, terrorist attacks in the United States. The official also called a mosque in Gatineau to see if the caretakers knew Maghri. Ottawa Citizen, C4 (National Post)

Da? Nyet?
A letter states, "Has our Defence Ministry become so secretive that Peter MacKay doesn't dare say out loud that Canada's latest spy scandal involves Russia, when even the usually very secretive Russians are saying it (Accused Spy Would Have Had Top-Level Clearance - Jan. 18)?..." Globe and Mail, A14

Accused in spy case known as a loner
At high school in Lower Sackville, Nova Scotia, Jeffrey Paul Delisle was known as a bit of a geek, a loner who kept to himself. A clearer picture is emerging of the 40-year-old naval intelligence officer who was charged on Monday with passing government secrets to foreign interests, and who one military expert says was likely under police surveillance for months or years. Fellow students in Sackville High School's graduating class of 1990 had few recollections of the ordinary kid with the low profile now enmeshed in what could be Canada's biggest spy scandal in more than half a century. Globe and Mail, A4; National Post (Edmonton Journal, Times Colonist); Calgary Sun (London Free Press, Edmonton Sun, Ottawa Sun, Toronto Sun, Whig-Standard, Winnipeg Sun); * Whig-Standard; * Toronto Sun; * Toronto Sun; * The Record; * Chronicle-Herald; * Hamilton Spectator (Red Deer Advocate)

CYBER SECURITY / CYBERSÉCURITÉ

*** A black day for Internet privacy in Canada: expert - U.S. anti-piracy laws called heavy-handed**
Canadians would be affected if online anti-piracy laws proposed south of the border get passed by Congress, say advocates of free speech and privacy. The laws - The Stop Online Piracy Act and the PROTECT IP Act, known as SOPA and PIPA - would require Internet-service providers to block access to any site accused of posting, or linking to, copyrighted content. It also would force search engines to remove the offending sites from their databases and prevent advertisers from giving the site their business. Critics say the law would make media companies judge and jury of copyright infringement, rather than having the process resolved in court. They also say it's a blatant attack on freedom of expression. "The goal, in many ways, of SOPA is to reach beyond the borders of the United States," said Michael Geist, a University of Ottawa law professor and copyright expert. "It's Canadian sites and sites around the world that would find themselves a target for these kinds of actions." Montreal Gazette, B1

*** Day without Wikipedia just a glimpse**
If a day without Wikipedia was a bother, think bigger. In this plugged-in world, we would barely be able to cope if the entire internet went down in a city, state or country for a day or a week. And most of civilization went along until the 1990s without the internet. But now we're so intertwined socially, financially and industrially that suddenly going back to the 1980s would hit the world as hard as a natural disaster, experts say. No email, Twitter or Facebook. No buying online. No

stock trades. No just-in-time industrial shipping. No real-time tracking of diseases. It's gotten so that not just the entire internet but individual websites such as Google are considered critical infrastructure, experts said. Waterloo Region Record, A6

*** Court gives legal recourse to privacy theft victims**
Ontario's top court has created a new way for individuals to sue people who invade their private information, a new step in the legal system's attempts to come to terms with the digital age of online record-keeping and communications. Crafted by the Ontario Court of Appeal on Wednesday, the change will provide a legal avenue for those whose sexual practices, private correspondence or personal records have been snooped on for no legitimate reason. The court said information is being generated and stored at a staggering rate, but legislation has not kept pace - leaving aggrieved parties no recourse against those who violate their privacy. In his ruling, Judge Sharpe created a new legal tort - a basis for a lawsuit - called "intrusion upon seclusion." Globe and Mail, A6

*** Lock your online doors - Stopping Internet crime is a constant game of digital cat and mouse for Web heavyweight Google**
Even Google Inc. cannot guarantee your safety online. So last summer, when the company behind the world's largest search engine noticed computers all over the world were being infected with a specific type of malware (malicious software), Google went public with its discovery. Because the warning asked users to conduct a Google search to see if they were among the victims, some people derided the company for what they perceived as an attempt to promote its own service. Others claimed announcing the threat to the world would only give those responsible time to adapt. Four months later, Fabrice Jaubert, a Montreal-based software engineer who works on Google's anti-malware team, stood by the move. "We could turn the question around and ask if it would have been ethical to know someone was infected and not tell them," he said in an interview. Mr. Jaubert expects to continue playing his digital cat and mouse game "where the bad guys try to stay one step ahead of us and we come up with better, more complex algorithms to try and identify them." National Post, FP12

*** Zappos, Amazon sued over hacking**
Online retailers Zappos.com and Amazon.com are being sued in Kentucky by a Texas woman alleging that she and millions of other customers were harmed by the release of personal account information. Officials representing Zappos in Nevada and parent company Amazon in Seattle declined comment Wednesday on the lawsuit filed in U.S. District Court in Louisville, Ky. The lawsuit was filed Monday, after Zappos chief executive officer Tony Hsieh alerted employees and customers by e-mail Sunday that names, phone numbers and e-mail addresses of the shoe retailer's customer may have been accessed in a hacker attack. The company said customers' credit card and payment information weren't stolen. Zappos urged customers to reset passwords. Globe and Mail, B10

*** Internet anti-piracy bills throw lasso too widely**
An opinion piece states "If you tried to use Wikipedia yesterday and were met by a black screen with the chilling caution 'Imagine a World Without Free Knowledge,' welcome to the world of copyright debate. That debate is peaking in the U.S. Congress, where two proposed laws would force Internet providers to shut down 'pirate' sites selling illegal movies, music or books -- cutting off those sites, refusing to accept advertising from them and disabling any payment processing links. The crackdown is necessary. Free knowledge doesn't include freedom to break the law. However, the laws are a big lasso intended to corral a rogue horse. They could also catch cart horses just doing their jobs -- delivering information. Canada's proposed new copyright law takes a halfway approach. Internet providers would have to inform customers that they have downloaded illegal material. The implied threat of a criminal charge for the next offence is intended to have a 'scared straight' effect. That's a potentially effective approach, but if it doesn't work, something closer to the U.S. model will be necessary." Kingston Whig-Standard, 4 (London Free Press)

*** Brake the Internet pirates**
The following editoral, reprinted from The Wall Street Journal, states: "Wikipedia and many other websites are shutting down today to oppose a proposal in Congress on foreign Internet piracy, and the White House is seconding the protest. The covert lobbying war between Silicon Valley and most other companies in the business of intellectual property is now in the open, and this fight could define - or reinvent - copyright in the digital era. Everyone agrees, or at least claims to agree, that the illegal sale of copyrighted and trademarked products has become a worldwide, multibilliondollar industry and a legitimate and growing economic problem. Often consumers think they're buying copies or streams from legitimate retail enterprises, sometimes not. Either way, the technical term for this is theft. The Internet has been a tremendous engine for commercial and democratic exchange, but that makes it all the more important to police the abusers who hijack its architecture. SOPA merely adapts the current avenues of legal recourse for infringement and counterfeiting to new realities. Without rights that protect the creativity and innovation that bring fresh ideas and products to market, there will be far fewer ideas and products to steal." National Post, FP11

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

Former officer accused of Mafia ties found dead
By the time Detective Sergeant Ian Davidson retired a year ago from the Montreal police, the 33-year veteran had built up a reputation as a meticulous analyst in the intelligence unit, responsible for handling highly sensitive information. Within months, that reputation began to unravel. The Montreal native had fallen under investigation for explosive allegations: that he tried to sell the names of secret police informants to the Mafia. The 57-year-old is believed to have committed suicide. Globe and Mail, A4; * Toronto Sun; * Toronto Star; * Le Droit (Le Soleil, La Tribune, Le Devoir); * Le Quotidien; * Journal de Montréal; * Journal de Montréal

*** A police force that does less with more**
An opinion piece states, "Police chief Marc Parent is seeking to reassure Montrealers. He said on Tuesday that a retired police detective had failed in his attempt to sell to the Mafia a top-secret list of undercover officers and other police informants. As it happens, the ex-detective died the next day. So, end of story? Hardly. It's a relief to hear that no informants lost their lives. But the larger matter - the overall performance by police against organized crime - is not reassuring at all. Montreal police appear to have been helpless to prevent the Mafia from maintaining a decades-long grip on parts of Montreal Island's economy. And when intra-Mafia politics produce high-profile murders, it's striking how seldom local police make arrests. (Do last month's arrests of five men linked to the slaying of Salvatore Montagna suggest improvement? No. The Sûreté du Québec, not the Montreal force, nailed them.)..." Montreal Gazette, A2

Mountie faces charges
A Rimbey. Alta., Mountie is on leave after being charged with assault and uttering threats in connection with at least three incidents in 2011, RCMP say. Const. Charles Lambright faces two counts of assault, one count of uttering threats and one count of breach of a court order, RCMP spokesperson Tim Taniguchi said. The charges stem from alleged incidents between Lambright and a woman he had a personal relationship with, he said. An RCMP code of conduct investigation is also underway. Starphoenix, A4 (Edmonton Journal)

Fourth special prosecutor takes Bountiful case
A new special Crown attorney has been appointed to look into allegations of sexual exploitation and other offences against minors in the polygamous community of Bountiful, B.C. Peter Wilson was appointed to represent the province in the case against religious leaders in the closed fundamentalist Mormon community, who have been accused of sexual exploitation of a young person, sexual assault and procurement in allegations dating back to the early 1980s. Wilson is the fourth special Crown attorney appointed to the case. He replaced Richard Peck, who dismissed himself earlier this month. London Free Press, B8

*** Cocaine trial tied to publisher's 1998 murder**
The cocaine conspiracy trial of a Montreal man suspected by police of being involved in the assassination of Vancouver publisher Tara Singh Hayer opened in Vancouver on Wednesday. In her opening statement, federal prosecutor Martha Devlin told the judge that the background to the drug conspiracy case began in 2005, when RCMP launched Project Expedio. The Province, A12

*** Mayor suggests expanding RCMP headquarters**
Queens District RCMP may be looking for a new home and Charlottetown Mayor Clifford Lee has a suggestion. RCMP Sgt. Andrew Blackadar said Wednesday the person who owns the building which currently houses the detachment (Maypoint Plaza) wants to sell the building. The RCMP have the space leased until May 2013. The towns of Stratford and Cornwall have already expressed interest in having the district headquarters come their way but the capital city mayor has another suggestion. The Guardian, A1

*** Profilage: le SPVM ne reçoit pas une note parfaite**
La Commission des droits de la personne et des droits de la jeunesse du Québec (CDPDJQ) déplore à nouveau le manque de collaboration de la police de Montréal dans le traitement des plaintes pour profilage racial. Le président de la Commission, Gaétan Cousineau, est heureux que le Service de police de la Ville de Montréal (SPVM) s'attaque sérieusement au problème du profilage racial et social, mais il se réserve bien d'accorder une note parfaite au nouveau plan stratégique dévoilé mardi. Le Devoir, A2

*** Mountie 'terrified' woman**
An Innisfail woman says she was terrified of the Mountie who rented a property to her about seven years ago. RCMP Const. Hoa Dong La, in a judgealone trial before Justice David Gates in Red Deer Court of Queen's Bench, is accused of using a variety of tactics for monetary gain, involving five different properties in Innisfail and Bowden and in the rural area near Bowden Institution. La, 47, faces 15 counts altogether, including three counts of extortion, two of criminal harassment and 10 of mortgage fraud. Red Deer Advocate, C1

*** Man charged with possessing 50,000 contraband cigarettes**
A 40-year-old man from Clarenville was arrested Tuesday for possession of contraband tobacco when the vehicle he was operating was stopped by the RCMP Customs and Excise Section and found to contain 50,000 contraband cigarettes. The man will appear in provincial court in March to answer to charges under the Excise Act and the Provincial Revenue Administration Act. The Telegram, A5

*** Gangster ducked earlier bullets**
Sandip "Dip" Singh Duhre, 36 - killed Tuesday in a hail of bullets at a downtown Vancouver restaurant - was a notorious gangster marked for death since 2005. Sandip, along with his brothers Balraj, 38, and Paul, 35, headed the powerful Duhre Group - whose 50 to 100 "street soldiers" have con-trolled much of the drug trade in the Fraser Valley since the 2010 arrests of rival leaders from the United Nations and Red Scorpions. The shooting comes less than a week after well-known Vancouver gangster Ranjit Singh Cheema was released from a U.S. prison. The Province, A3

*** Youth's cop car theft sentencing delayed**
Sentencing for a Moncton teen who stole a police car last fall and injured a police officer was adjourned yesterday morning so the Crown can call the Mountie to the witness stand. The 16-year-old boy appeared in Moncton youth court before Judge Irwin Lampert on Jan. 4 and pleaded guilty to a long list of charges, including obstructing Const. Kevin Tremblay by giving him a false name, stealing a police car, dangerous driving, impaired driving causing bodily harm to Tremblay and three breaches of court orders. Times & Transcript, A3 (Telegraph-Journal)

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Inquiry hears B.C. RCMP failed to 'take ownership'
An Ontario deputy police chief told the Missing Women Commission of Inquiry Wednesday that if British Columbia police leaders had "taken ownership" of the issue, "many women's lives may have been saved." Deputy Chief Jennifer Evans of Peel Regional Police concluded in her 2011 report to the inquiry that "the (Vancouver Police Department) and the RCMP initially failed to recognize the missing women issue. Leader-Post, A7 (Times Colonist)

*** Pickton claims he's innocent of murders, officer tells inquiry**
An Ontario deputy police chief who interviewed serial killer Robert Pick-ton in jail says he claims he's innocent of murdering women. "He said he didn't do anything, he maintained his innocence," Jennifer Evans, Peel Regional Police deputy chief, told the Missing Women Commission of Inquiry on Wednesday. Evans interviewed Pickton in prison as part of her review of how police con-ducted their investigations into the dozens of women who went missing from Vancouver's Downtown Eastside. The Province, A8

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Lawyers doubt genocide evidence
The federal government has information that proves the Rwandan government is criminal and that fabrication of evidence about the 1994 genocide is a common occurrence sanctioned by authorities there, claim lawyers trying to stop the deportation of suspected war criminal Leon Mugesera. Starphoenix, D5

*** Waiver to cross U.S. border isn't a simple affair**
A letter to the editor states, "Mike Milne, a spokesman for U.S. Customs and Border Protection, refers to the need for a waiver to enter the U.S. if someone has a conviction for a narcotics offence. The waiver is an "Application for Advance Permission to Enter as Non-immigrant" which requires finger-prints taken by the RCMP for a Canadian record check, also sent to the FBI and the U.S. Justice Department, details of the offence, court records, family history, letters of character reference, evidence and/or a written account demonstrating rehabilitation, advance request for date(s) of entry, and fingerprints taken again (by U.S. officials)...Six hundred thousand Canadians have criminal records of possession of marijuana. Even if you don't have a criminal record in Canada any more, because of a conditional discharge or a pardon, Uncle Sam neither forgets nor forgives." Vancouver Sun, A12

*** 30 jours de prison pour un Américain arrêté au N.-B.**
Un homme âgé de 20 ans de l'Oregon a plaidé coupable à des accusations liées à son entrée illégale au Canada. Il a écopé d'une peine de 30 jours d'emprisonnement. David Allen Sankey a été arrêté vendredi par des membres du District 7 de la GRC après avoir traversé la frontière sans être passé par un poste de douane. Il a ensuite été confié à l'Agence des services frontaliers du Canada. L'Acadie Nouvelle, 6; Telegraph-Journal

*** The border**
On this issue, many of the report's recommendations mimic the ongoing work of the Canada-U.S. Regulatory Cooperation Council. That work was recently endorsed by Mr. Harper and U.S. President Barack Obama, and business and government officials on both sides of the border are hammering out the specifics of how to speed up border crossings for business by reducing duplication. The report calls for the Canada Border Services Agency to make Free and Secure Trade (FAST) lanes more widely available at the border for shippers. Globe and Mail, A6

*** New wrinkle in Mugesera case**
Ottawa has information that proves the Rwandan government is criminal and that fabrication of evidence about the 1994 genocide is a common occurrence sanctioned by the authorities, claim lawyers trying to stop the deportation of suspected war criminal Léon Mugesera. In a motion to be presented in Quebec Superior Court Friday, law firm Roy Larochelle Avocats Inc. says that documentation never before presented shows it's impossible for Mugesera to have a fair trial in Rwanda and that the judiciary is not impartial. Montréal Gazette, A6

*** Léon Mugesera case**
An editorial states, "There is much about Rwanda that Montrealers know little or nothing about because mainstream Western news media do not report it. This is why, regardless of what one thinks of the man, The Gazette's editorial "Léon Mugesera and justice in Rwanda" (Jan. 14) is out of touch with reality. Mugesera is facing deportation to Rwanda over allegations that he was in part responsible for precipitating the 1994 genocide in that country. He argues that he faces torture or summary execution there...Let's not kid ourselves into believing that deporting him to Rwanda would be legal." Montreal Gazette, A15

*** L'ONU et Mugesera...**
Un article d'opinion déclare, « Dites-moi que je rêve! En 1994, l'ONU n'a pas voulu intervenir pour empêcher le massacre de 800 000 personnes. Là, elle trouve important de demander au Canada de surseoir à l'extradition de Mugesera pour s'assurer qu'il soit bien traité dans son pays. Depuis plus de 15 ans, Mugesera a bénéficié de tous les recours juridiques de notre pays pour se faire entendre et cela ne suffit pas?... » Le Soleil, 25

*** Muslim wife fears for her life**
A Muslim wife who claims she'll be killed by her in-laws for not being able to bear children has been temporarily spared deportation to her native Bangladesh in a precedent-setting case. Mosammat Monowara Khatun, who lives in Toronto, was spared removal on Jan. 8 after a last-ditch appeal to the Federal Court of Canada stayed her deportation. London Free Press, B8 (Toronto Sun)

*** Le Canada appuie l'appel à la clémence de Ronald Smith**
Les avocats du seul Canadien condamné à mort aux États-Unis ont officiellement déposé une demande de clémence aux autorités de l'État du Montana. Leur client, Ronald Smith, maintenant âgé de 54 ans, est dans le couloir de la mort aux États-Unis depuis près de 30 ans pour les meurtres de deux hommes en 1982. Tous les appels précédents de l'homme originaire de Red Deer, en Alberta, ont été jusqu'ici rejetés. La Presse, A14 (La Voix de l'Est, L'Acadie Nouvelle); Calgary Sun; Toronto Star (Red Deer Advocate, The Guardian)

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Getting high on renewal
An editorial states, "...There has been no public clamour for a war on drugs in Canada, yet the Tories are pursuing one as part of their costly crime agenda, with measures such as legislating mandatory minimum prison terms for people caught growing a handful of pot plants. Even in the U.S., some conservatives are disowning the Reaganite policy, as the crackdown has had little impact on actual use, has proved enormously costly in fiscal and human terms and created fertile ground for drug gangs. Whether legalization is the best solution is open to debate. This newspaper has previously favoured decriminalization. But the Liberals are right to make it a political issue." Globe and Mail, A14

Killer denied day parole in aboriginal hearing
On the grounds that he is "no farther ahead" than he was when he killed 15-year-old Tara Manning, convicted murderer Gregory Bromby was denied day parole Wednesday in an aboriginal elder-assisted hearing. Although the Haitian-born Bromby is not aboriginal, he qualified for an elder-assisted hearing by demonstrating a "commitment to aboriginal spirituality." National Post, A6; * Winnipeg Sun, * Winnipeg Free Press

The legalization of pot

A letter states, "Arguments for and against the legalization of marijuana have been going on for the past decade, with weak arguments presented for maintaining the status quo... To further extrapolate that slapping a tax on marijuana would result in a black market for private dealers (as I suppose has happened in the liquor industry) is speculation gone wild. Prohibition gave rise to organized crime; illegal drug use spawned the drug cartels and countless crimes and murders. Society implicitly condones the use of marijuana. To legalize it and put it on the same footing as alcohol and tobacco is something that any progressive government should do. Discouragement of its use should follow the same programs that are now in effect for tobacco." The Gazette, A14

*** Weeding out trouble**
City officials and cops are concerned about risks posed by legal marijuana grow ops, those sanctioned by the federal government, running anonymously in Calgary communities. Despite being given the nod by Health Canada to see pot plants produced, the operations can pose the same peril seen with illegal outfits. A southwest house was shuttered Wednesday after officials from the city's safety response unit and health officials deemed it unfit for human habitation. Calgary Sun, 3

*** Getting high on the Grits' pot plank**
An editorial, "The Liberal party convention last weekend revived the old debate on whether or not we should legalize marijuana. While our prisons are jam-packed, our public finances in the red and almost everyone admits that the war on drugs is a "complete failure," the time may have come to re-open that bag of pot... Don't get me wrong. I do approve of the Conservatives' policy of being tough on crime. I just don't believe that an adult who freely decides to have six plants of marijuana in his backyard or basement and who smokes a joint or two a day is a criminal. The Conservatives do not understand that but now the Liberals do. I am quite sure that Bob Marley's spirit could inspire the Grits for their next election campaign slogan: No victim, no crime ..." Calgary Sun, 15 (Edmonton Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun)

*** Move to legalize pot looks set to heat up**
An opinion piece states, "When you just can't win a war, it's a good idea to consider whether you should still be in there, fighting it. Smoking marijuana and taking other products of the cannabis plant are all illegal in this country. But many otherwise law-abiding people do it anyway, and we are now at the point where political leaders are almost embarrassed if they haven't taken a toke or two. Federal Liberal leader Bob Rae says he has smoked marijuana. So has Ontario Premier Dalton McGuinty. And U.S. President Barack Obama, when asked if he had inhaled, quipped: "Frequently ... That was the point!" It seems that everywhere, except the federal Conservative government, we're ready to shrug off our anti-dope laws..." The Record, B1

*** Hearings poorly understood**
There are many misconceptions about aboriginal parole board hearings. Among them is that offenders do not have to be aboriginal to get one. About 10 per cent of the 500 or so aboriginal hearings held every year across Canada are at the request of non-aboriginal offenders. The latest case involves Haitian-born convicted killer Gregory Bromby, who received an aboriginal parole board hearing Wednesday at Stony Mountain Institution. Another misconception? An offender won't necessarily know the elder who sits in on the hearing, nor is the elder an advocate for the offender. Winnipeg Free Press, A4

*** Man nabbed after halfway house escape**
A 38-year-old man who police say walked away from a halfway house in Nova Scotia was arrested in Charlottetown without incident Wednesday. Hartley Coleman was wanted on a Canada-wide warrant. Chronicle Herald, A3 (The Guardian)

*** Proctor killer must go to adult institution**
One of the teens who brutally raped and murdered Kimberly Proctor in March 2010 will be transferred from Victoria's youth detention centre to a federal penitentiary on Monday, his 18th birthday. On Wednesday, Kruse Hendrik Wellwood applied to B.C. Supreme Court Justice Robert Johnston to extend his stay at the youth facility until June 30 to allow him to complete his Grade 12. Times Colonist, A6

*** Barrel's a few fish shy of a load**
An opinion piece states "Cataloguing all the ways governments waste tax dollars is the journalistic equivalent of shooting fish in a barrel: It's easy and not very sporting...Now, the feds are talking about cuts, of between five and 10 per cent, to government services and programs it considers only peripherally relevant to most Canadians even as it plans to spend billions on crime, defence and heritage projects for which it either cannot or will not make a cogent case. Lawlessness is decreasing in every category of major offense almost everywhere in the country. But the Tories are determined to send more people to jail for longer just as soon as they liberate enough money from Treasury (that is, borrow enough dough from taxpayers) to build more penitentiaries. They say their share of the price tag will amount to a comparatively measly

$79 million over five years. Quebec's Minister of Public Security says, however, it expects the crime bill will cost the province more than $300 million, alone..." Moncton Times and Transcript, D6

PUBLIC SERVICE / FONCTION PUBLIQUE

MP pensions 'a ripoff on a massive scale'
The Canadian Taxpayers Federation says it's high time MPs stopped making Canadians pick up the tab for their "gold-plated" pension plan. "This is a ripoff on a massive scale," the advocacy group's federal director, Gregory Thomas, said at a news con-ference on Parliament Hill Wednesday announcing its report on parliamentarians' pensions. Treasury Board President Tony Clement said he is examining the issue of MP pensions as part of the larger government-wide spending review. He said the government's first step was to freeze MP salaries. Ottawa Citizen, A1 (Daily Gleaner)

INTERNATIONAL / INTERNATIONAL

*** Where's my copy of Good Cavekeeping?**
A copy of an al-Qaida-linked magazine was delivered to the Guantanamo detention camp for suspected terrorists, a military prosecutor revealed on Wednesday during a court discussion of mail security. The camp commander, Rear Admiral David Woods, issued orders last month tightening the screening of mail sent by lawyers to their clients at the camp that holds 171 captives on the Guantanamo Bay U.S. naval base in Cuba. Toronto Sun, 45

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

SECRET

Bradley, Kees

From: [redacted]
Sent: Friday, January 20, 2012 9:40 AM
To: Bradley, Kees
Subject: Hacking / [redacted]

s.15(1) - Def

Attachments: IA 201199E.pdf; IA201128E.pdf

IA 201199E.pdf
(294 KB)

[redacted]

Hi Kees,

Please find [redacted] assessments, [redacted] on Anonymous (could be related to your cyber file), [redacted]

Regards,

[redacted] NHQ/AC

[redacted]

SECRET

Intelligence Assessment

SECRET
CSIS IA 2011-12/99
2012 01 16

ANONYMOUS: An Overview

ANONYMOUS

Key Judgments

- ANONYMOUS is the new hacktivist (hacker-activist) model. The global reach of the Internet, the availability of numerous open-source/free attack tools, and the flourishing of social networking venues facilitates the organization and carrying out of cyber-attacks by hacktivist groups. The purpose of these attacks is to bring media and public attention to their issues of concern. Thus, cyberspace is both a venue and vector for activists.
-
-
- In June 2011, ANONYMOUS publicized its goal of launching cyber-attacks against governments, major organizations and financial institutions. The purpose is to obtain classified information from these organizations and publicly disclose it.

•

Head, IAB

CSIS_PUBLICATIONS / SCRS_ PUBLICATIONS

CAVEAT

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the Security of Information Act. It is loaned to your agency/department in confidence. The document must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Canadian departments, agencies or organizations: This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

Foreign agencies or organizations: This document is loaned to your agency/department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

ANONYMOUS CANADA

1. The impetus for this assessment was ANONYMOUS' 2011 11 13 threat to "remove Toronto from the Internet" due to the city's plans to remove *Occupy Toronto* protesters from their St. James Park encampment.

2. In a video posted on YouTube on 2011 12 02, ANONYMOUS took credit for redirecting traffic from 50+ Toronto-area business websites to that of *Occupy Toronto*. The latter denounced this action and claimed that it played no part in its planning and/or execution. ANONYMOUS also stated it had "taken down" the Canadian version of Craigslist and gained access to what it claimed is a "very important email address and address book" that they plan to publicly release should the City of Toronto continue to oppose the *Occupy Movement*.[1]

4. ANONYMOUS has shown some interest in Canada and Canadian targets, especially since the 2011 06 08 defacement and hack of the Conservative Party's website. The attacker, going by the name LulzRaft , posted a fake alert claiming PM Harper had been rushed to hospital due to his choking on hash browns. LulzRaft also broke into the Party's donor database, parts of which he/she posted on *Pastebin*.

5. ANONYMOUS has recently trained its sights on the Alberta Oil Sands and the corporations involved in its associated extraction, transportation, refining and financing operations. Anonymous has thrown its support behind Project TARMAGEDDON, via #OpGreenRights, which identified specific Canadian targets including Canadian Oil Sands Ltd., the Canadian Association of Petroleum Producers and other corporations that have a presence/involvement in the Oil Sands.

ANONYMOUS – Current Situation

6. In June 2011, ANONYMOUS publicised its goal of launching cyber-attacks against governments, major organizations and financial institutions. The purpose is to obtain classified information from these organizations and publicly disclose it.

[1] www.youtube.com/watch?v=NLm-YFyjMC&feature=player_embedded#!

7. On at least two occasions, insiders identifying with ANONYMOUS' goals released sensitive corporate information to the collective. Moreover, on 2011 12 24, as part of the AntiSec (Anti Security) campaign, ANONYMOUS claimed responsibility for a cyber-attack against STRATFOR, the national security think tank. An unofficial spokesman for the group said the attackers sought to access the millions of emails held on STRATFOR's servers; emails the group reckoned would shed light on the alleged "state-corporate alliance against the free information movement."[2]

8. In spite of arrests of its members in many countries - including Australia, the US, Spain, France, the UK, the Netherlands and Turkey - throughout 2011, ANONYMOUS continues to launch operations in multiple countries, including Canada, and primarily against governmental and corporate targets.

9. ANONYMOUS' continuing cyber and real-world activities underscore the fact that it is, first and foremost, a social movement, one that has such strong "brand recognition" that it continues to attract as media attention.

[2] Barrett Brown, "On Stratfor," http://pastebin.com/WPE73rhy.

ANONYMOUS: A GROUP?

11. Currently, ANONYMOUS defines itself as an international cyber-activist collective that is leaderless and animated by the spirits of *Wikileaks* and the *Occupy Movement* as it challenges any and all attempts by the powerful (i.e. governments, corporations and other major organizations) to curtail free speech and the free-flow of information.

12. ANONYMOUS did not, however, start off as a hacktivist group. ANONYMOUS germinated (circa 2003) on an Internet Relay Chat (IRC) message board known as 4chan/b/ (www.4chan.org). To this day, the channel's central ethos is anonymity; users do not have to register using their personal information – thus remaining anonymous and having *#anonymous* as their username – and no archives are kept. At first, most people who joined 4chan/b/ were looking for "Lulz", which roughly translates into laughs derived from the misfortunes of others. These misfortunes were the result of digital pranks that 4chan/b/ participants, known as ANONS, would play on targets such as gamers. It is over time, and as a result of specific incidents, that ANONYMOUS became more politically motivated.

13. Thus, ANONS are not reformed criminal hackers seeking redemption or an ideological justification for their actions. Rather, they are individuals who were drawn by the group's ethos, which is not profit-driven.

15. In January 2008, the Church of Scientology, using the pretext of copyright infringement, sought to remove all traces of a leaked internal video[4] from the Internet. This effort galvanized individuals on 4chan/b/ into organizing a response against what they considered to be an abuse of copyright enforcement and an egregious example of the Church's attempts to silence opponents. As a result, ANONYMOUS launched *#OpChanology*[5] which sought to disrupt, through a number of measures, the

[4] This is the infamous video in which the actor and church member Tom Cruise extols the virtues of Scientology and its followers, www.youtube.com/watch?v=oM-LeRLiqA0

[5] The use of the hash-tag # preceding the operation's name is standard for ANONYMOUS and reflects the fact that each one can be followed on Twitter.

Church's operations. To do so, ANONYMOUS used Distributed Denial of Service (DDoS)[6] attacks, prank calls, black faxes[7] and protests in cities around the world.[8] It was at these protests that ANONS started wearing the now infamous Guy Fawkes mask[9] (as seen in picture) as they feared retribution from the Church, which they claim deals aggressively (including illegal harassment) with critics. This operation is ongoing, with protests being organized and held around the world, including Canada.[10] Thus, *#OpChanology* marks ANONYMOUS' political and operational awakening.

16. *#OpChanology* also cemented the mythology that continues to surround ANONYMOUS in terms of it being a collective, a social movement in which all are equal irrespective of their tenure and dedication or their technical skills. In this view, ANONYMOUS resembles a leaderless hive in which each is given a role in accordance with their skill-sets and, driven by a sense of common purpose, members swarm those that threaten it, its members, its core values or have otherwise been identified as targets by ANONYMOUS.

17. ANONYMOUS is a collective[11], a big tent in which one finds individuals and cells (usually city-based) that share the same basic ethos of Internet freedom and free speech.

18. That being said, to become an ANON one only needs to login to the chat-rooms and participate in an operation.

[6] A DDoS attack is one in which a multitude of compromised systems flood a single target with so many incoming messages that the target can no longer respond and essentially shuts down, thereby causing a denial of service for users of the targeted system.

[7] This refers to the faxing of entirely black documents in order empty the target's toner cartridge.

[8] Including: Kitchener, Montreal, Edmonton, Ottawa, Toronto, Vancouver and Winnipeg.

[9] The mask was made popular by the movie *V for Vendetta* (2006) in which an anarchist revolutionary dons a Guy Fawkes mask in his violent campaign against a totalitarian state.

[10] See: http://forums.whyweprotest.net/events/

[11] It is very difficult to estimate how many core ANONS there are worldwide, but if one takes the turnout to anti-Scientology protests as a proxy there are likely in the high hundreds.

19. As a result, smaller more goal-oriented splinter groups can emerge. This was the case with *LulzSec*, which went on a 50-day (Spring/Summer 2011) hacking spree against law enforcement, security intelligence, private security, government and corporate targets including the CIA, the FBI and the UK Serious and Organized Crime Agency (SOCA). As a result, sensitive data including intelligence reports, usernames and passwords, and the personal information of police officers and their families was posted on *The Pirate Bay*, one of the largest illegal downloading websites on the Internet.

21. ANONYMOUS' success lies in its ability to communicate its message to a world audience. Its media capabilities are impressive, but are more a reflection of the greater availability, and effective use, of media-making software than "deep pockets". ANONYMOUS does ask for donations, however. ANONYMOUS largely takes advantage of free services like *4chan, Pastebin, Twitter, Tumblr, Youtube* to communicate with each other and the world;

22. ANONYMOUS' tool of choice is the DDoS attack. The latter can take many forms depending on the target system and the attackers' objectives, and exploit either network (hardware/connection) or application (software) vulnerabilities. It is very difficult and expensive to defend against a DDoS attack because of its distributed nature; in other words a victim can block traffic from one or a handful of distinct Internet Protocol (IP) addresses, but not necessarily from hundreds let alone thousands. A DDoS attack produces one of three outcomes: 1) consume all your bandwidth by flooding your network with so much traffic that all communications to and from you are impossible; 2) exhaust your resources by overloading/targeting specific services (i.e. email, web site access) with bogus requests; and 3) exploit an application weakness or vulnerability to render them unusable for a period.

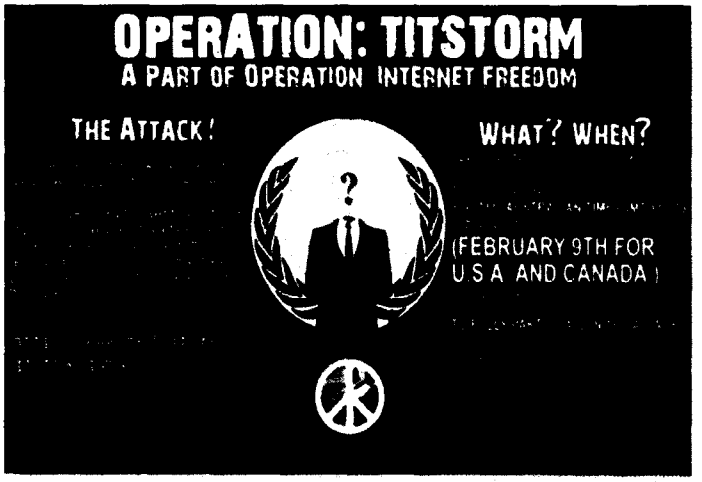
23. Returning to *#OpChanology*, it is clear that it was the first of several events that have helped crystallize ANONYMOUS' ideology, which is centered on the protection of free speech and unfettered access to all information even if it is protected by copyright or government security classifications.

24. Deeply anti-authority and libertarian at its inception, it was only in 2011 that the group adopted the more stringent anti-capitalist, animal rights, environmentalist (with frequent references to Aboriginal rights) and anti-law enforcement/security service attitudes more commonly associated with left-wing activists.

25. In the period between *#OpChanology* (January 2008) and the start of the *Wikileaks* scandal (October 2010), ANONYMOUS launched a number of operations, all aided by the use of social networking and micro-blogging services like *Facebook*, *Twitter*, *Reddit* and *Tumblr*. For instance, ANONYMOUS claims to have assisted Iran's Green Movement in the wake of Mahmood Ahmadinejad's controversial June 2009 election win. Another example is *#OpTitstorm*, which targeted Australian government websites because of Canberra's efforts to introduce a national Internet filter, thus threatening free speech and the free flow of information in Australia. From the advertising poster, it is clear that organizers expected Canadian and American members to participate. *#OpTitstorm* resulted in certain Australian government websites being inaccessible for several hours.

Julian Assange, Aaron Barr & Kalle Lasn

26. In December 2010, ANONYMOUS launched *#opPayback/Avenge Assange* against Amazon.com for no longer hosting *Wikileaks* on its servers, as well as PayPal, Visa and MasterCard for refusing to process donations to the website.



27. In February 2011, ANONYMOUS focused its attention on Aaron Barr, CEO of *HBGary Federal*, an offshoot of the well-known technology security company *HBGary*. At the time, Barr made public the fact that he had been "investigating" *#opPayback* by mining social networking and micro-blogging sites to identify key members and understand the inner workings of ANONYMOUS. He had also intimated that this investigation was conducted for the FBI. Before he could present the results at a conference, ANONYMOUS defaced *HBGary*'s website, broke into its servers and stole some tens of thousands confidential company emails and posted them on *The Pirate Bay*. ANONYMOUS also disclosed Barr's social security number, home address and cell phone number, as well as compromised his personal email, *Twitter* and *LinkedIn* accounts. Some members even claimed to have erased one Terabyte of information off the *HBGary's* servers and gotten hold of the STUXNET worm among other things.

28. The impact of ANONYMOUS' cyber-attack on *HBGary Federal* was dramatic for all parties. *HBGary* had to reassure clients that their source codes to proprietary malware and other software (crown jewels) were never accessed by ANONYMOUS; in spite of its denials, *HBGary*'s reputation was damaged. The attack underscored how ANONYMOUS can mount operations targeting one individual, and the extent to which a determined actor can use open-source information and well-known vulnerabilities –

29. The emails stolen from *HBGary* showed how closely it was working with US Federal authorities, as well as with large financial institutions to whom *HBGary* had proposed doing a cyber-attack against the *Wikileaks* in an effort to stop it from leaking documents pertaining to their activities. This confirmed many of the ANONYMOUS' worst fears about what *Wikileaks* is now describing as a growing "international mass surveillance industry" in which private companies provide tools and techniques for state entities such as law enforcement and security intelligence to more effectively capture and follow individuals' and groups' digital trails online. These technologies allow users to map social networks, track cell phones, do locational tracking and deep packet inspection (i.e. capture and look at the content of messages).[12] From an ANONYMOUS perspective, these revelations reinforce the notion that it is not only authoritarian regimes that seek to censor the Internet and persecute those who seek to exercise their rights to free speech and assembly, but Western corporations and democracies as well; as *Wikileaks* states "[i]n the last ten years systems for indiscriminate, mass surveillance have become the norm."

30. Vancouver-based Kalle Lasn's call to *Occupy Wall Street* (OWS), in *Adbusters* magazine, was heeded early on by ANONYMOUS as evidenced by the presence of members in most, if not all the occupations that have taken place in Europe, Australia, North and South

[12] "The Cyber-security Industrial Complex," Technology Review, 2011 12 06; "Big Data meets big brother," PrivacyInternational.org, 2011 11 30; "The Spyfiles," http://wikileaks.org/the-spyfiles.html

America. It is not happenstance that the Guy Fawkes mask is now seen by many as the emblem of the *Occupy Movement*. Moreover, ANONYMOUS claimed it was releasing a new attack tool, RefRef, to coincide with the "Day of Rage" (2011 09 17) which officially launched the *Occupy Movement*.

31. The ANON developer claimed that RefRef exploited known vulnerabilities and that it precluded the need for the heavy firepower of a botnet[13] as it essentially turns the target server against itself, leading to resource exhaustion.

32. ANONYMOUS remains committed to the *Occupy Movement*. It has launched a number of operations in support of the movement, especially after evictions of OWS participants from most occupation sites. For instance, ANONYMOUS has announced *#opHorizon* which calls for protests to take place on 2011 12 17 in order to commemorate the death of Mohamed Bouazizi and the start of the Arab Spring, the three month anniversary of the *Occupy Movement* and the birth of Pfc. Bradley Manning. The following statement sums it up:

We are Anonymous
We are Bradley Manning
We are Arab Spring, European Summer, American Autumn
We are 99%
We do not forgive
We do not forget
Expect us

[13] A botnet is a network of computers that have been infected with malicious software and is being instructed to accomplish automated tasks on the Internet unbeknownst to the owners. Criminals use botnets to send out spam email, spread viruses and attack computers and servers.

Outlook

33. ANONYMOUS is the face of modern hacktivism. Though hacktivism has existed since the time of the first dial-up connections, it is only now - with the ubiquity of the Internet, the greater availability of free attack tools and techniques, and the flourishing of social networking tools - that groups can bring media and public attention to issues that concern them.

38. Foreign governments may view groups like ANONYMOUS either as serious national security threats that must be dealt with using "muscular" means or as an extension of Western governments' and intelligence services' operations. The potential for negative diplomatic impacts is a reality as certain governments may see the hidden hand of Western governments and intelligence services behind the actions of ANONYMOUS. (C)

Pages 1677 to / à 1683

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - Subv, 16(1)(a)(iii), 16(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Klassen, Nathan

From: Murphy, Gregg
Sent: January-20-12 1:09 PM
To: Klassen, Nathan
Subject: RE: Brief **s.20(1)(c)**

Tar sands;

Anonymous also announced "Operation Green Rights/Project Tarmaggedon," against Exxon Mobil, ConocoPhillips, and others. http://news.cnet.com/8301-27080_3-20078963-245/anonymous-targets-monsanto-oil-firms/

-----Original Message-----
From: Klassen, Nathan
Sent: January-20-12 1:05 PM
To: St-Louis, Danielle
Cc: Murphy, Gregg
Subject: Brief

Hi Danielle,

Today's brief for RD is attached. Ken and Luc are happy with the final product. Could you please read it over for grammar / spacing J / ect? Once done please prepare the official brief and send it over. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca <mailto:Nathan.Klassen@ps-sp.gc.ca>

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-20-12 8:42 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; Houston, Laura; Jones, Scott; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 20, 2012/ le 20 janvier 2012

Print Media

Le FBI ferme le site Megaupload
La justice américaine a ordonné hier la fermeture du site Megaupload.com, plateforme emblématique et controversée du téléchargement direct sur Internet, accusé de violation des droits d'auteur, s'attirant aussitôt une cyberattaque des pirates d'Anonymous. Quatre responsables du site basé à Hong Kong, dont son fondateur, Kim Dotcom, 37 ans, ont été interpellés à Auckland, en Nouvelle-Zélande, sur la base de mandats d'arrêt délivrés par les États-Unis. Le FBI (police fédérale américaine) et le ministère de la Justice américain ont estimé, dans un communiqué commun, qu'il s'agissait de l'une des plus "grandes affaires de violation de droits d'auteur jamais traitées aux États-Unis". Journal de Montréal

Hackers attack FBI, Justice Department websites after Megaupload shutdown
Minutes after the U.S. Department of Justice shut down notorious file-sharing site Megaupload.com, the department's own website was brought down in a cyber attack orchestrated by the hacker group Anonymous. "The government takes down Megaupload? 15 minutes later Anonymous takes down government & record label sites," a member of Anonymous said via Twitter. The group also disabled the sites of Universal Music, the RIAA, the U.S. Copyright Office, Broadcast

Music Inc., the FBI and the Motion Picture Association of America in what it called its "largest attack ever." By late evening, however, most sites were back online. National Post

The evasive 'Koobface gang' - Despite Facebook publicizing their names and faces, the Russian cyber criminals have yet to be brought to justice, Christopher Williams reports
Facebook took a very unusual step for a multinational web company this week, when it publicly accused five Russian men of running a multi-million-dollar scam against hundreds of thousands of its users. The "Koobface gang", as the quintet is known to Internet security experts, stand accused of infecting social network users' computers with a malicious software "worm". The global network of up to 800,000 remotely-controlled machines became a lucrative business for the gang. Other cyber criminals would pay them to bombard their victims with ads for fake antivirus software, or to hijack searches to deliver traffic to rogue pharmacy websites. Ottawa Citizen

If Wiki were wishes, trolls might surf
An opinion piece states "In the crosshairs are two bills introduced before Congress last year - the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA) - that would give content owners the legal tools with which to choke off business to sites they claim infringe on their rights. The proposed Acts are ludicrously blunt instruments that are far more likely to damage the myopic lawmakers who now support them rather than a 'free and open Internet.' Beyond this, they are virtually unenforceable, and any law that can't be enforced gets what it deserves: It gets ignored as tens of thousands of online denizens operate their various workarounds to popular acclaim." Moncton Times and Transcript

Copyright debate moving north
An opinion piece states "If you tried to use Wikipedia Wednesday and were met by a black screen with the chilling caution 'Imagine a World Without Free Knowledge,' welcome to the world of copyright debate. That debate is peaking in the U.S. Congress, where two proposed laws would force Internet providers to shut down 'pirate' sites selling illegal movies, music or books -- cutting off those sites, refusing to accept advertising from them and disabling any payment processing links. The crackdown is necessary. Free knowledge doesn't include freedom to break the law. Canada's proposed new copyright law takes a halfway approach. Internet providers would have to inform customers they have downloaded illegal material. That's a potentially effective approach, but if it doesn't work, something closer to the U.S. model will be necessary." Winnipeg Sun

Digital intruders have been warned
An editorial states "The Ontario Court of Appeal's decision on Wednesday recognizing a right to sue for damages for outrageous violations of privacy is a good example of sensible judicial innovation. It is an adaptation that reflects life in the digital age. Laws against trespass, breaking and entering, burglary, and unreasonable search and seizure - protecting bricks-and-mortar rights, one might say - remain very important, but the same principles that underlie those older rights need to be complemented, in order to deal in an analogous way with what Mr. Justice Robert Sharpe - who wrote the three-judge panel's decision - calls informational privacy. The result is a new tort - that is, the civil-lawsuit equivalent of a crime - by the name of 'intrusion upon seclusion.'" Globe and Mail

Online Media

Anonymous goes nuclear; everybody loses?
An opinion piece states "In the aftermath of Wednesday's SOPA/PIPA blackout protests, the Internet community amassed quite a bit of goodwill, flexed its muscles in a friendly, humorous, civil-disobedience kind of way, and, remarkably, even managed to change quite a few minds. Just 24 short hours later, Anonymous legions nuked that goodwill and took cyber security into thermonuclear territory. The real question now is: were they played? As I write this, #OpMegaUpload is in full effect. The Internet is seemingly coming down all around me. Global Internet traffic is fluctuating between 13 percent and 14 percent above normal, and, as you can see from the above image, global network attacks were up 24 percent. Affected sites include the White House, the FBI, the Department of Justice, multiple record label sites, the MPAA, and RIAA, and the U.S. Copyright Office." CNET

Google Expands Hacked Sites Label In Search Results
A year ago, Google began labeling hacked sites and sites with malware as sites that may compromised in the search results snippets. Yesterday, Google's Matt Cutts announced on Google+ that Google has expanded that feature. Matt said the change they just launched will "expand our [Google's] coverage of labeling search result pages." Search Engine Roundtable

Spammers target childrens' games
With adults wising up to the dangers of clicking unknown links, spammers are increasingly targeting children. Anti-virus firm Avast says it's identified more than 60 individual sites during the last month containing 'game' or 'arcade' in their URL

address, all aimed squarely at children. The most visited site was cutearcade.com, a collection of online games with dressing up and coloring games - and even Hello Kitty. Avast says its users have reported an infection at this site over 12,600 times. The malicious Trojan redirects viewers to linuxstabs.com, a known distribution point for malware. TG Daily

Facebook users targeted by transformed Carberp Trojan
A new form of the Carberp Trojan, which tricks users into committing financial fraud via e-cash vouchers, is now targeting Facebook users, according to researchers at Trusteer. The malware is used in a man-in-the-browser (MitB) attack, which exploits the trust users have with Facebook and the anonymity of e-cash vouchers, wrote Amit Klein, CTO of Trusteer, in a recent blog post about the Carberp Trojan. Klein said the Trojan replaces a Facebook page with a fake page that notifies users that their account has been "temporarily locked" and can be unlocked by providing personal information and an e-cash voucher worth approximately $25. Search Security

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From: Moore, Bruce
Sent: January-20-12 1:25 PM
To: Beaudoin, Luc S; [redacted]
Subject: RE: anonymous and the US

s.16(2)(c)

Done - Jan 20, 2012 1:23:51 PM - via the [redacted]

Bruce

-----Original Message-----
From: Beaudoin, Luc S
Sent: January-20-12 12:38 PM
To: CYBERDO
Cc: Moore, Bruce
Subject: anonymous and the US

Could we please send to US CERT via u5 portal something like that:

/////

CCIRC has been monitoring media and mailist reports about Anonymous actions against US government and private sites. Do not hesitate to contact us to mitigate/coordinate any Canadian nexus of these attacks.

Regards

//////

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Williston, Sandra

From: Gregg.Murphy@ps-sp.gc.ca
Sent: January-20-12 1:09 PM
To: Klassen, Nathan
Subject: RE: Brief

s.20(1)(c)

Tar sands;

Anonymous also announced "Operation Green Rights/Project Tarmaggedon," [redacted] and others. http://news.cnet.com/8301-27080_3-20078963-245/anonymous-targets-monsanto-oil-firms/

-----Original Message-----
From: Klassen, Nathan
Sent: January-20-12 1:05 PM
To: St-Louis, Danielle
Cc: Murphy, Gregg
Subject: Brief

Hi Danielle,

Today's brief for RD is attached. Ken and Luc are happy with the final product. Could you please read it over for grammar / spacing J / ect? Once done please prepare the official brief and send it over. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca <mailto:Nathan.Klassen@ps-sp.gc.ca>

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-20-12 8:06 AM
To: [redacted]
Cc: Phlek, Vireak; Moore, Bruce; Murphy, Gregg; Williston, Sandra; Melanson, Daryl; Turbide, Frank; Clow, Patrick
Subject: Anonymous and SOPA

$ python twitter.py
Results for search term: [redacted] **s.16(1)(b)**
URLS **s.16(2)(c)**
[redacted]
http://t.co/cebkzP9p -> http://www.fbi.gov
[redacted] -> http://www.techdirt.com/articles/20120119/17203417480/mpaa-uses-anon-attacks-to-make-nonsensical-comments-about-free-speech.shtml
[redacted] -> http://anonops.blogspot.com/2012/01/internet-strikes-back-opmegaupload.html?spref=tw
-> [redacted]

TARGETS

HIVE SERVERS

JSLOIC URLS
[redacted]

MOBILELOIC URLS
[redacted]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Williston, Sandra

From: Bendelier, Kenneth
Sent: January-20-12 6:59 AM
To: Beaudoin, Luc; [redacted]
Subject: Fw: Important: Anonymous downs government, music industry sites in largest attack ever

For the daily? s.16(2)(c)

----- Original Message -----
From: E-Secure-IT [mailto:alert@e-secure-it.com]
Sent: Friday, January 20, 2012 03:30 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous downs government, music industry sites in largest attack ever

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: RT
Complete item: http://rt.com/usa/news/anonymous-doj-universal-sopa-235/

Description:
Hacktivists with the collective Anonymous are waging an attack on the website for the White House after successfully breaking the sites for the FBI, Department of Justice, Universal Music Group, RIAA and Motion Picture Association of America.

In response to todays federal raid on the file sharing service Megaupload, hackers with the online collective Anonymous have broken the websites for the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music Group.

It was in retaliation for Megaupload, as was the concurrent attack on Justice.org, Anonymous operative Barrett Brown tells RT on Thursday afternoon.

E-Secure-IT
https://www.e-secure-it.com

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-20-12 6:45 AM
To: [redacted] s.16(2)(c)
Subject: For daily: Anonymous ddos related to SOPA

Using LOIC and twitter links, anonymous is conducting SOPA related DDOS. We need to research this. This is FYI only from mailing list:
/////
Do *not* click on the pastehtml.com links displayed via this search, else you'll load up LOIC and join the fun:

[redacted]
////

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

Williston, Sandra

From: Klassen, Nathan
Sent: January-20-12 11:46 AM
To: Bendelier, Kenneth; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today

Hi Ken and Luc,

The requested brief is attached. Comments due by 1:30 PM today in order to get this to RD before the weekend. FYI, Gregg has reviewed the draft and he is happy with it. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

Williston, Sandra

From: Gregg.Murphy@ps-sp.gc.ca
Sent: January-20-12 10:54 AM
To: Klassen, Nathan
Subject: Anonymous

http://www.kctv5.com/story/16558352/anonymous-takes-down-doj-fbi-sites
http://www.firstpost.com/tech/fbi-shuts-down-megaupload-com-anonymous-shut-down-fbi-188266.html

"Federal officials confirmed it was down on Thursday evening and that the disruption was being "treated as a malicious act." " This is all I have as far as confirmation...

Gregg Murphy
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-3579 Facsimile | Télécopieur +1 613-991-3574 gregg.murphy@ps-sp.gc.ca
www.publicsafety.gc.ca Government of Canada | Gouvernement du Canada

Williston, Sandra

From: Bergeron, Dominic
Sent: January-20-12 8:51 AM
To: Clow, Patrick
Subject: Re: Interesting day?

You watch traditional news??? :p

----- Original Message -----
From: Clow, Patrick
Sent: Friday, January 20, 2012 07:42 AM
To: Bergeron, Dominic
Subject: RE: Interesting day?

First story on CBC news last night.

-----Original Message-----
From: Bergeron, Dominic
Sent: January-19-12 9:48 PM
To: Clow, Patrick
Subject: Interesting day?

You've been following the news about anonymous' rampage today?

Its pretty amazing the amount of nodes these guys could get together for ddos. At least 11 sites went down including the fbi.

Makes you wonder what can be done to stop such embarrassing attacks.

Dom.

Klassen, Nathan

From: Klassen, Nathan
Sent: January-20-12 9:37 AM
To: Anderson, Windy
Cc: Bendelier, Kenneth
Subject: Weekly work plan -- January 23 to January 27 -- 2012 -- Nate Klassen

Hi Windy / Ken

Here is my tentative work plan for January 23 - 27. The review for the past week is also below. Cheers,

Nate

Weekly Work Plan (January. 23 - January. 27):

1. ***PIA***
   - ***a.*** Start working on section 6 of the PIA – the PIA is my priority for January;
   - ***b.*** Once received -- input comments from Bud, Rob, Ken, ATIP, and PS legal into the draft; and
   - c. Start briefing note for LC;

2. ***Situational Awareness***
   - a. Produce weekly stats report WRT CCIRC's products – use the new template;
   - b. Explore using publication tool for stat report / posting stat report on the portal on a monthly basis;
   - c. Provide comments on the weekly SA report;
   - d. Create decks / briefs as required by Windy / Ken; and
   - *e.* Help out on any other SA product as determined by Windy / Ken.

3. ***Other***
   - ***a.*** Continue to get up to speed WRT CCIRC

Last week in review (January. 16 – January 20):

1. ***PIA***
   - a. Start working on section 5 of the PIA – the PIA is my priority for January; -- Finished and circulated for comments
   - b. Circulate sections 1-4 of PIA to Ken / Bud / Rob / PS legal / PS ATIP for comment; and -- Finished and circulated for comments
   - c. Contact PS document management to: (1) set up CCIRC 'retention schedule; and (2) obtain Record Disposition Authority from the Librarian and Archivist of Canada – Contacted PS document management and they are in the process of providing us the required information.

2. ***Situational Awareness***
   - f. Produce weekly stats report WRT CCIRC's products -- Done
   - g. Provide comments on the weekly SA report; -- Done, provided Rana with comments
   - h. Fixed the 1 page feedback form we will circulate with our new weekly product;
   - i. Wrote two briefs – Israeli – Palestine 'cyber war' and Anonymous attacks on US Government and private sector
   - j. Set up meeting with RCMP

3. ***Other***
   - a. Continue to get up to speed WRT CCIRC;
   - b. Send training request for next fiscal year to Ken -- Done

Nathan Klassen
Canadian Cyber Incident Response Centre

Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

Klassen, Nathan

From: Bendelier, Kenneth
Sent: January-20-12 11:58 AM
To: Klassen, Nathan; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Re: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today

Good.

Send.

From: Klassen, Nathan
Sent: Friday, January 20, 2012 11:45 AM
To: Bendelier, Kenneth; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today

Hi Ken and Luc,

The requested brief is attached. Comments due by 1:30 PM today in order to get this to RD before the weekend. FYI, Gregg has reviewed the draft and he is happy with it. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

Bendelier, Kenneth

From: Klassen, Nathan
Sent: January-20-12 11:46 AM
To: Bendelier, Kenneth; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today
Attachments: PS-SP-#549586-R-Briefing_Note_-_HACKERS_ATTACK_UNITED_STATES_GOVERNMENT_AND_PRIVATE_SECTOR_WEB_SITES_-_to_DG_-_2012_-01-20.DOC.DRF

☺

From: Klassen, Nathan
Sent: January-20-12 11:46 AM
To: Bendelier, Kenneth; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today

Hi Ken and Luc,

The requested brief is attached. Comments due by 1:30 PM today in order to get this to RD before the weekend. FYI, Gregg has reviewed the draft and he is happy with it. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

UNCLASSIFIED

DATE: January 20, 2012

File No.: 385245
RDIMS No.: 549586

MEMORANDUM FOR THE DIRECTOR GENERAL

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Nate Klassen
Gregg Murphy

Klassen, Nathan

From: Klassen, Nathan
Sent: January-20-12 1:05 PM
To: St-Louis, Danielle
Cc: Murphy, Gregg
Subject: Brief
Attachments: PS-SP-#549586-R-Briefing_Note_-_HACKERS_ATTACK_UNITED_STATES_GOVERNMENT_AND_PRIVATE_SECTOR_WEB_SITES_-_to_DG_-_2012_-01-20.DOC.DRF

Hi Danielle,

Today's brief for RD is attached. Ken and Luc are happy with the final product. Could you please read it over for grammar / spacing ☺ / ect? Once done please prepare the official brief and send it over. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

UNCLASSIFIED

DATE: January 20, 2012

File No.: 385245
RDIMS No.: 549586

MEMORANDUM FOR THE DIRECTOR GENERAL

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Nate Klassen
Gregg Murphy

Weir, Sarah

From: Fortunato, Stephanie
Sent: January-20-12 4:31 PM
To: St-Louis, Danielle
Cc: Weir, Sarah
Subject: RE: Memo to DG: Hackers Attack United States Government and Private sector Websites

Hey!

Robert just read it, he'd like us to send it to the DM on Monday morning. There are a few changes that need to be made. First of all, after FBI in the background section, there should not be any punctuation. Also, in the 3rd paragraph under the consideration header, the word "internet" should be spelt "Internet". Please make these changes and then have the memo signed by the acting Director on Monday.

Thanks!!

Steph

From: St-Louis, Danielle
Sent: January-20-12 4:22 PM
To: Fortunato, Stephanie
Cc: Klassen, Nathan; Murphy, Gregg; Bendelier, Kenneth
Subject: Memo to DG: Hackers Attack United States Government and Private sector Websites

As discussed. please show to Robert and we will have it sent to DGO formally on Monday.
If you have any questions, please let me know. Have a nice weekend!

Thank you Steph

Danielle St-Louis
Administrative Assistant | Adjointe administrative
Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 rue Slater St | Ottawa ON K1A 0P9
Telephone | Téléphone: **613-991-7738** Fax | Téléc.: 613-991-3574
E-mail | Courriel: danielle.st-louis@ps-sp.gc.ca

UNCLASSIFIED

DATE: January 20, 2012

File No.: 385245
RDIMS No.: 549586

MEMORANDUM FOR THE DIRECTOR GENERAL

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19th, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

CCIRC is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Nate Klassen
Gregg Murphy

UNCLASSIFIED

DATE: January 20, 2012

File No.: 385245
RDIMS No.: 549586

MEMORANDUM FOR THE DIRECTOR GENERAL

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Nate Klassen
Gregg Murphy

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE:

File No.: 385262
RDIMS No.: 550276

MEMORANDUM FOR THE DEPUTY MINISTER

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEBSITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) websites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, 2012, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of Friday, January 20, 2012, most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these websites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Gregg Murphy

Klassen, Nathan

From: Murphy, Gregg
Sent: January-20-12 10:54 AM
To: Klassen, Nathan
Subject: Anonymous

http://www.kctv5.com/story/16558352/anonymous-takes-down-doj-fbi-sites
http://www.firstpost.com/tech/fbi-shuts-down-megaupload-com-anonymous-shut-down-fbi-188266.html

"Federal officials confirmed it was down on Thursday evening and that the disruption was being "treated as a malicious act." " This is all I have as far as confirmation...

Gregg Murphy
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-3579 Facsimile | Télécopieur +1 613-991-3574 gregg.murphy@ps-sp.gc.ca
www.publicsafety.gc.ca Government of Canada | Gouvernement du Canada

Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-20-12 8:07 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 20, 2012 / le 20 janvier 2012

MINISTER / MINISTRE

Top Mountie gagged: senator
A Liberal senator is accusing the government of trying to "muzzle" the RCMP commissioner after learning of guidelines that require all meetings between the top officer and parliamentarians to be approved first by government officials. Internal emails obtained by Postmedia News show that when Senator Colin Kenny attempted to schedule a meeting recently with Commissioner Bob Paulson, Paulson replied, "I apologize for any delay, but I've become aware of some guidelines from the **Department of Public Safety** in terms of engaging with Parliamentarians and Senators and so I may have to respectfully ask you to route your request for a meeting through the Minister's Office or the Department." Kenny said in an interview Thursday that the government was improperly trying to muzzle a senior public servant and that the guidelines will have the effect of shutting down communication between parliamentarians and officials. **Julie Carmichael, a spokeswoman for Public Safety Minister Vic Toews**, said in a statement that allegations the commissioner is being muzzled are "***baseless and inaccurate***" and that it is "***standard practice across government to ensure a co-ordinated approach between departments and agencies***." Ottawa Citizen, A1 (National Post, Starphoenix, Montreal Gazette, Calgary Herald, Vancouver Sun); Hamilton Spectator (Red Deer Advocate)

Mounties on tight leash: MPs, senators wishing to meet RCMP brass must go through Toews
The federal Conservatives are directly exerting strict communications control over the RCMP and its new top cop, documents obtained by the Star reveal. Documents released under Access to Information show top political staff of **Public Safety Minister Vic Toews** oversaw and approved the design of a new RCMP communications protocol that put the national police force on a tighter leash. As the Star first reported, that protocol requires the RCMP to flag anything that might "garner national media attention" to **Public Safety Canada**. New **Public Safety** documents show **Toews's** office had a direct hand in crafting the policy, working with the RCMP's new public affairs director - Daniel Lavoie - a former associate assistant deputy minister in **Toews'** department. Lavoie, who moved to the RCMP from **Public Safety** last summer, advised former colleagues that implementing the new protocol "will require a change of mentality" at the RCMP, even though the force was already flagging important media issues to the government. Lavoie's emails show he met with outgoing RCMP boss William Elliott as the protocol was developed. None of the emails suggests Lavoie or Elliott raised any concerns about the RCMP's independence. The documents show it was developed under the watchful eyes of **Toews's chief of staff Andrew House and communications director Michael Patton**, contrary to initial suggestions to the Star by Patton that he was unaware of a new policy. On top of that comes a new edict from **Toews's** office that requires Elliott's replacement, Commissioner Bob Paulson, to vet all his meetings with MPs and senators first through his political bosses. Paulson replied he'd since become aware of "guidelines" from the **Department of Public Safety** on his dealings with MPs and Senators. Toronto Star, A10

*** Pour un registre québécois**
«Nous préconisons le maintien du registre [des armes à feu]. Nous sommes convaincus que c'est indispensable.» Le dg de la Sûreté du Québec (SQ), Richard Deschesnes, fonde son opinion sur le fait que le registre que veut abolir le gouvernement Harper est consulté 711 fois par jour au Québec, tous corps policiers confondus. Avec 1,7 million d'armes enregistrées en province, la SQ veut savoir qui sont ceux qui les possèdent. «Prenez le cas de l'homme barricadé à Saint-Malachie, mercredi. Dans ce genre d'opération, il faut détenir cette information. C'est pourquoi nous appuyons **le ministre [de la Sécurité publique]** dans ses démarches auprès du gouvernement fédéral.» Québec tente de récupérer les données du registre que veut détruire Ottawa. Le Soleil, 3

*** Des enfants dans les centres de détention**
En moyenne, depuis 2005, au moins 430 enfants par année sont détenus dans des prisons canadiennes. Ce ne sont pourtant pas des criminels. Ce sont des demandeurs d'asile politique, qui sont détenus comme plusieurs milliers de leurs semblables, selon le pouvoir discrétionnaire d'un agent de l'Agence des services frontaliers du Canada. On dit 430

enfants, mais c'est peut-être beaucoup plus. Certains enfants ne sont pas comptabilisés dans les statistiques parce qu'ils accompagnent simplement en prison leurs parents demandeurs de statut. Bientôt, ces demandeurs de statut seront détenus pour une période d'un an ferme, sans possibilité de révision de détention, et sans accès à un tribunal, si le projet C-4 défendu par le gouvernement fédéral est adopté. Malheureusement, rien n'indique que **le ministre canadien de la Sécurité publique** fasse beaucoup mieux une fois C-4 adopté, s'inquiètent les chercheurs du CSSS de La Montagne, dans un mémoire qu'ils prévoient soumettre au Parlement sous peu. Le Devoir, A1

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

La Nina could set stage for flu pandemic
Now, two U.S. scientists - Jeffrey Shaman at Columbia University and Marc Lipsitch at Harvard University's school of public health - have identified a climatic pattern that could set the stage for the emergence of a new and deadly strain of influenza. Globe and Mail, L6

*** Release data on Tamiflu**
An editorial states, "Over the past three years, Ontario has spent $26 million stockpiling Tamiflu to treat people in the event of a pandemic. During the last big scare - H1N1 in 2009 - there were shortages of the children's antiviral dose and cases of frantic parents racing between drug stores trying to fill what they believed could be a life-saving prescription. Around the world, the bill for this one drug has been in the billions as governments built up supplies..." Toronto Star, A18

*** Not prepared for emergencies**
In the wee hours of the morning, a water valve at the high school failed and most of the city's water supply spilled onto the ground, almost draining the reservoir. Millions and millions of gallons of water, flowing out into a dark and cold Arctic night in the middle of a community can make quite a mess. YellowKnifer

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Russian embassy staff expelled
The Harper government has expelled staff at Russia's embassy in the wake of charges filed against a Canadian military intelligence officer for allegedly passing secrets to a foreign power, The Globe and Mail has learned. The names of two Russian diplomats - including a defence attache - and two technical staff at the embassy have been dropped from the Department of Foreign Affairs' list of diplomatic, consular and foreign government representatives recognized by Ottawa. Globe and Mail, A1; Ottawa Citizen (Times Colonist); Toronto Star; London Free Press (Whig-Standard, Ottawa Sun, Calgary Sun, Edmonton Sun, Toronto Sun, Winnipeg Sun); * Winnipeg Sun (Edmonton Sun); * Winnipeg Free Press

Top court rejects Almalki appeal
Ottawa's Abdullah Almalki vows to continue his fight for justice after the Supreme Court of Canada rejected his bid to force the government to reveal more of its secrets. Almalki is one of three former terror suspects - all of whom were tortured in overseas prisons - suing the government for $180 million. Ottawa Citizen, A3; National Post (Windsor Star); * Hamilton Spectator; * La Presse (Le Droit)

*** The new age of local espionage has just begun**
An editorial states, "...By Monday, Halifax had become a hub - and a hubbub - of international intrigue as a 40-year-old naval intelligence officer was charged with passing along military secrets to a "foreign entity." In this instance, the latter is code for Russia. The Herald has confirmed this through its own spy network... Sub.-Lt. Jeffrey Paul Delisle worked at such a top-secret nerve centre in Halifax, dubbed Trinity. Even if the allegations against him stand up to scrutiny, we'll never know how much damage may have been done... If anything, analysts say there are more Russian spies deployed in North America now than there ever were. And the sort of tactical and strategic intelligence that can be gleaned from sites like Trinity would be of great value to a great power that still likes to play the Great Game... Expect more of the same as the shipbuilding contract gets into full swing. "Foreign entities" will be very interested in these ships' design, capabilities and components. Much of the high-end stuff will be developed out-of-province, but it will all have to be assembled here at some point. FYI, we aren't the only ones building a modern navy. So is Russia. So is China. Stealing technology is hardly beneath them, and there will always be well-placed people hanging around who are not above betraying their country." Chronicle-Herald, A9

*** PACKAGE WAS EXPLOSIVE**

A suspicious package that prompted London police to close a stretch of Southdale Rd. for almost four hours Wednesday contained an explosive device, police said. The package was found in an isolated wooded area in the southwest part of the city on Southdale near Wickerson Rd. The explosive disposal unit was called in. Police closed Southdale between Bramblewood Rd. and Wickerson from about 7:30 p.m. to 11:30 p.m. The device was destroyed and no one was injured. Police did not release details. London Free Press, A7

CYBER SECURITY / CYBERSÉCURITÉ

*** Le FBI ferme le site Megaupload**
La justice américaine a ordonné hier la fermeture du site Megaupload.com, plateforme emblématique et controversée du téléchargement direct sur Internet, accusé de violation des droits d'auteur, s'attirant aussitôt une cyberattaque des pirates d'Anonymous. Quatre responsables du site basé à Hong Kong, dont son fondateur, Kim Dotcom, 37 ans, ont été interpellés à Auckland, en Nouvelle-Zélande, sur la base de mandats d'arrêt délivrés par les États-Unis. Le FBI (police fédérale américaine) et le ministère de la Justice américain ont estimé, dans un communiqué commun, qu'il s'agissait de l'une des plus "grandes affaires de violation de droits d'auteur jamais traitées aux États-Unis". Journal de Montréal, 37; Halifax Chronicle-Herald; Toronto Sun

*** Hackers attack FBI, Justice Department websites after Megaupload shutdown**
Minutes after the U.S. Department of Justice shut down notorious file-sharing site Megaupload.com, the department's own website was brought down in a cyber attack orchestrated by the hacker group Anonymous. "The government takes down Megaupload? 15 minutes later Anonymous takes down government & record label sites," a member of Anonymous said via Twitter. The group also disabled the sites of Universal Music, the RIAA, the U.S. Copyright Office, Broadcast Music Inc., the FBI and the Motion Picture Association of America in what it called its "largest attack ever." By late evening, however, most sites were back online. National Post

*** The evasive 'Koobface gang' - Despite Facebook publicizing their names and faces, the Russian cyber criminals have yet to be brought to justice, Christopher Williams reports**
Facebook took a very unusual step for a multinational web company this week, when it publicly accused five Russian men of running a multi-million-dollar scam against hundreds of thousands of its users. The "Koobface gang", as the quintet is known to Internet security experts, stand accused of infecting social network users' computers with a malicious software "worm". The global network of up to 800,000 remotely-controlled machines became a lucrative business for the gang. Other cyber criminals would pay them to bombard their victims with ads for fake antivirus software, or to hijack searches to deliver traffic to rogue pharmacy websites. Ottawa Citizen, F9

*** If Wiki were wishes, trolls might surf**
An opinion piece states "In the crosshairs are two bills introduced before Congress last year - the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA) - that would give content owners the legal tools with which to choke off business to sites they claim infringe on their rights. The proposed Acts are ludicrously blunt instruments that are far more likely to damage the myopic lawmakers who now support them rather than a 'free and open Internet.' Beyond this, they are virtually unenforceable, and any law that can't be enforced gets what it deserves: It gets ignored as tens of thousands of online denizens operate their various workarounds to popular acclaim." Moncton Times and Transcript, D6

*** Copyright debate moving north**
An opinion piece states "If you tried to use Wikipedia Wednesday and were met by a black screen with the chilling caution 'Imagine a World Without Free Knowledge,' welcome to the world of copyright debate. That debate is peaking in the U.S. Congress, where two proposed laws would force Internet providers to shut down 'pirate' sites selling illegal movies, music or books -- cutting off those sites, refusing to accept advertising from them and disabling any payment processing links. The crackdown is necessary. Free knowledge doesn't include freedom to break the law. Canada's proposed new copyright law takes a halfway approach. Internet providers would have to inform customers they have downloaded illegal material. That's a potentially effective approach, but if it doesn't work, something closer to the U.S. model will be necessary." Winnipeg Sun, 10

*** Digital intruders have been warned**
An editorial states "The Ontario Court of Appeal's decision on Wednesday recognizing a right to sue for damages for outrageous violations of privacy is a good example of sensible judicial innovation. It is an adaptation that reflects life in the digital age. Laws against trespass, breaking and entering, burglary, and unreasonable search and seizure - protecting bricks-and-mortar rights, one might say - remain very important, but the same principles that underlie those older rights need to be complemented, in order to deal in an analogous way with what Mr. Justice Robert Sharpe - who wrote the

three-judge panel's decision - calls informational privacy. The result is a new tort - that is, the civil-lawsuit equivalent of a crime - by the name of 'intrusion upon seclusion.'" Globe and Mail, A12

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

Tasers most likely to be used on 'downtrodden,' published study asserts
The use of Tasers by Canada's police forces represents a "teething new urban terrorism" that targets society's "downtrodden," says a study published this month that looked at more than two dozen deaths involving the stun guns. Those most likely to get "tased" include the poor, mentally ill and chronic drug users, according to the study, led by Temitope Oriola, who received a Governor General's Gold Medal for academic excellence upon the completion of his doctoral studies at the University of Alberta last year. Leader-Post, A7 (Edmonton Journal, Calgary Herald, The Province, Vancouver Sun)

First guns. Then food processors?
An opinion piece states, "Pierre Perron of the Canadian Firearms Program wrote "the Armi Jager AP80 rifle is a prohibited firearm and always has been." While this may be correct, I can't help but think that a larger issue might have been overlooked. The Armi Jager AP80, a prohibited variant of the AK-47, has been circulating as a non restricted firearm for well over a decade, yet there have been no incidences with this firearm that would indicate it is any more of a risk to public safety than a regular non-restricted rifle..." National Post, A9; National Post

* **Charged ex-Mountie arrested again**
A former Mountie charged with second-degree murder is back behind bars for flouting his bail conditions. Keith Gregory Wiens, 57, is accused of killing his common-law wife, Lynn Kalmring, in their home in Penticton, B.C., on Aug. 16. Edmonton Journal, A11; The Province

* **Way off target**
An opinion piece states, "The Mounties aren't too happy with me after my last column. It seems the men and women in red serge don't like it being pointed out that they have the ability to seize private property with no government oversight. Last week I wrote about the RCMP's reclassification of a .22-calibre semi-automatic rifle as a prohibited firearm because it looks like another rifle that is already banned...So while the Harper government crows about scrapping the gun registry, the RCMP, which they control, will continue to seize private property without compensation all because something looks scary to a paper pusher in Ottawa." Toronto Sun, 23 (Winnipeg Sun, London Free Press, Calgary Sun, Kingston Whig-Standard, Edmonton Sun)

* **Dirty police officers hurt ex-drug dealer, court told Thursday**
Rather than being beaten by dirty cops, an ex-drug dealer hurt himself by going "berserk" on police who had no choice but to restrain him, a defence lawyer argued as part of a cop corruption trial. Former pot dealer Christopher Quigley has testified several members of the once-illustrious Team 3 of the Toronto Police Central Field Command drug squad beat him to a bloody pulp in 1998 because he wouldn't tell them where they could find his money. The trial continues Friday. Kingston Whig-Standard, 10; Toronto Sun

* **Gangster talked of getting out shortly before shooting: Heed**
Just months before his public execution Tuesday, gangster Sandip Duhre admitted he regretted his choices and would get out of the life if he could. Duhre spoke frankly to Vancouver-Fraserview MLA Kash Heed during a chance encounter at a south Surrey restaurant in late summer, Heed recalled Wednesday. Vancouver Sun, A5

* **La «taupe du SPVM» voulait aussi vendre des renseignements à des trafiquants kurdes**
L'ex-policier Ian Davidson n'aurait pas seulement tenté de vendre sa liste ultrasecrète d'informateurs à la mafia italienne. Il aurait aussi essayé de faire affaire avec un redoutable gang de Kurdes turcs actif dans le trafic de drogue au centre-ville, croit la police. Celui que plusieurs surnomment maintenant "la taupe du SPVM" aurait engagé ces tractations devant le peu d'empressement de la mafia à répondre à son offre. La Presse, A5 (La Tribune, La Voix de l'Est); Le Soleil (Le Devoir)

* **Quatorze arrestations pour trafic de drogue**
La Sûreté du Québec (SQ) a frappé mercredi et hier un réseau impliqué dans le trafic de stupéfiants, actif sur le territoire de la MRC de Manicouagan. La frappe policière, qui découle d'une enquête qui a duré près d'un an, a conduit à neuf perquisitions et à 14 arrestations à Baie-Comeau et à Chute-aux-Outardes. Le Soleil, 20

* **Constable had woman fearing for her life**

A woman testified Thursday in Red Deer court during a Mountie's trial that she feared he had set her home on fire. The 2006 fire caused structural damage and killed a dog, cat and cockatiel. RCMP Const. Hoa Dong La, in a judge-alone trial before Justice David Gates in Red Deer Court of Queen's Bench, is accused of using a variety of tactics for monetary gain, involving five different properties in Innisfail and Bowden and in the rural area near Bowden Institution. Red Deer Advocate, A1

*** Police keeping tabs on toxic form of ecstasy**
Though it has not yet turned up in Newfoundland and Lab-rador, police in the province are keeping tabs on fatal overdoses in Western Canada linked to a form of the drug ecstasy laced with a toxic additive. Paramethoxymethamphetamine (PMMA) is not a new chemical, according to Sgt. Stephen Conohan, a provincial drugs and organized crime awareness co-ordinator with the RCMP. The Telegram, A4

*** RCMP scoring higher in Yukoners' esteem**
Seventy-eight per cent of Yukoners believe RCMP officers demonstrate professionalism at work, according to a new national survey released last week. That's a 12 per cent increase over the same survey in 2010. The annual national survey polled about 500 adult Yukoners over the phone during June and July 2011. Three-quarters of Yukoners say the RCMP is an organization with integrity, compared to 63 per cent in 2010. Whitehorse Star, 2

*** Newfoundland man pleads not guilty to charges in six-day standoff with RCMP**
A Newfoundland man charged after a six-day standoff with the RCMP in December 2010 has pleaded not guilty to all charges. Leo Crockwell barricaded himself inside a Bay Bulls, N.L., home and eventually evaded police by slipping out a side window. The Guardian, A6

*** Banishment remains tool of First Nations justice**
Back in the day, if you were a First Nations citizen who killed another member of the same band or committed a serious crime, you most likely would face banishment. Banishment back then was a nasty piece of business. You had to leave the safety of the camp and take your chances in the outside world. Fast forward 150 years, and the issue of banishment has come full circle. The media recently picked up the fact that the Samson Band in Alberta was contemplating banishment to rid the community of gang members. The four bands at Hobbema, Alta., have been in the news because of runaway gang violence. In the past several years, there have been a rash of murders, drive-by shootings and other evidence of gang activity on the reserve. Saskatoon Star-Phoenix, A9

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Vancouver police should have probed Pickton, officer says
Vancouver police should have investigated serial killer Robert Pickton rather than simply leaving him to the RCMP in a neighbouring city, the public inquiry into the case has heard. Ontario's Peel Regional Police Deputy Chief Jennifer Evans, who conducted an external review for the inquiry, contradicted the Vancouver police force's contention that Mr. Pickton was the responsibility of the Mounties in Port Coquitlam because that's where women were being killed. Deputy Chief Evans said Thursday when Vancouver police received information in 1998 and 1999 that Mr. Pickton may have been picking up sex workers in the city and killing them at his farm, they should have opened a criminal investigation. Globe and Mail, S1 (Red Deer Advocate); Leader-Post (Times Colonist)

*** City police should have pressured RCMP**
Vancouver police should have pressured the Coquitlam RCMP to aggressively investigate Robert Pick-ton in relation to the murder of dozens of missing women, an Ontario policing expert said Thursday. Peel Regional Police Deputy Chief Jennifer Evans, in her fourth day of testimony at the Missing Women Com-mission of Inquiry, insisted the VPD "should have made it a priority" to pressure the Mounties. The Province, A14

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Texas fugitive caught in province
RCMP and the Canada Border Services Agency (CBSA) have announced the arrest of a Texas fugitive.The man, identified as 46-year-old Gene Paul Hooks, was taken into custody Jan. 10 by the Canadian Border Services Agency in Shaunavon. The CBSA issued a "deportation order for serious criminality" Jan. 13. Hooks appeared in court Thursday in Regina and is scheduled to return to court in Swift Current Jan. 25. CBSA spokesman Sean Best said the deportation order won't be acted on until criminal matters have concluded. Leader-Post, A4

*** Mexican journalist in B.C. fears for life if deported**
A Mexican journalist who blew the whistle on corrupt officials in her homeland is pleading with the federal government to let her stay in Canada and says she will be persecuted if sent back. Karla GarcDia RamDirez, a mother of two children, fled to B.C. as an asylum seeker in 2008 after uncovering shady dealings in a government ministry. Red Deer Advocate, A7 (Toronto Star); Chronicle-Herald

*** Campaign shines light on human trafficking**
As many as 15,000 people become victims of human trafficking every year in Canada. That's far too many, says a Tory MP who has devoted herself to the cause. "Modern-day slavery is really manipulation of the mind," said Joy Smith before speaking to a group of University of Alberta students Thursday afternoon. Her passion to com-bat human trafficking was sparked by her son, who spent two years on the RCMP's Integrated Child Exploitation Unit. Edmonton Sun, 38

*** Justice and reconciliation are at the heart of Rwanda's recovery**
An opinion piece by Edda Mukabagwiza, Rwanda's high commissioner to Canada states, "Defence lawyers are paid to do and say whatever it takes to protect the interests of their clients. This explains why Léon Mugesera's lawyers, in a last-minute scramble to prevent their client's deportation to Rwanda, resorted to raising the spectre of torture. It amounts to a baseless and cruel slur against our country, and therefore demands a response..." Montreal Gazette, A17

*** City mother's deportation has been deferred**
The Canadian Border Services Agency (CBSA) confirmed Thursday that Hamilton mother Lucene Charles is no longer scheduled to be deported. In a statement read to The Spectator, a CBSA spokesperson said Charles has asked the agency to defer her removal from Canada. Hamilton Spectator, A5

*** "Ça passe ou ça casse"**
C'est aujourd'hui que les avocats de Léon Mugesera tenteront de prolonger le séjour du Rwandais au Canada, le temps que le comité contre la torture de l'ONU étudie le dossier et se prononce. Ce matin, à 9 h, une procédure complète sera présentée devant la Cour supérieure pour faire valoir le droit de Mugesera de s'adresser au comité contre la torture et l'obligation qu'a le gouvernement canadien de respecter les mesures provisoires jusqu'à la décision du comité. Journal de Montréal, 9

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Teen to be moved to federal prison
One of the B.C. teenagers who raped and murdered Kimberly Proctor in 2010 will be transferred from Victoria's youth detention centre to a federal penitentiary on Monday, his 18th birthday. Kruse Hendrik Wellwood lost his bid Wednesday to extend his stay at the youth facility until June 30 to allow him to complete Grade 12. B.C. Supreme Court Justice Robert Johnston agreed with the Crown that Wellwood needs intensive psychiatric and psychological treatment, available only in the federal system. National Post, A5 (The Province)

*** Forum looks at aboriginal women's plight - Manitoba MP to take issue to PM**
A Manitoba MP believes a United Nations conference this week can help his government shed some light on the issue of violence against aboriginal women. Rod Bruinooge, the Conservative MP for Winnipeg South, was at the UN in New York City this week for a three-day expert group conference of the Permanent Forum on Indigenous Issues. Research by the Native Women's Association of Canada showed more than 500 aboriginal women have been murdered or gone missing in Canada in the last four decades. Aboriginal women are 3.5 times more likely to be victims of violence than non-aboriginal women and five times more likely to be slain. The research spawned recognition of the problem and some action, including better police investigations when aboriginal women are reported missing. Winnipeg Free Press, A8

*** Egadz looks to expand sex trade registry**
A Saskatoon outreach program is looking to expand its sex-trade registry, which collects detailed information from workers in case they are found dead. Egadz, a non-profit agency that provides support for atrisk youth, has more than 100 sex trade workers on its "high-risk homicide registry," which was launched 15 years ago. The goal this year is to grow the registry to include information on more than 200 women and potentially expand to include youth at risk of running away, said Don Meikle, Egadz's director of outreach services. StarPhoenix, A6

*** B.C. cops brace for killings after murder of gangster**
Police across British Columbia's Lower Mainland are bracing for possible retaliatory killings after the brazen public execution of longtime gangster Sandip (Dip) Duhre by someone he was meeting at the Sheraton Wall Centre Tuesday night. They are looking at whether the targeted hit is linked to a series of tit-fortat slayings between rival groups over the

past 15 months that has left a trail of dead and wounded from Kelowna, B.C., to downtown Vancouver. Windsor Star, A6 (Times Colonist), Calgary Sun

*** Safe-injection sites a dilemma for Tremblay**
An opinion piece states, "...But at the moment, many of the 80,000 or so residents of the downtown borough are concerned, if not downright frightened, of what may happen to their neighbourhoods if a proposal to establish a safe-injection site in their midst is approved. A coalition of citizens groups has called for a moratorium on the project and are promising to show up at next month's meetings of their borough council and local health board to air their concerns..." Gazette, A9

*** Murder suspect's dad blames the system**
The justice system failed slaying victim Otto (Bunty) Loose if the man accused of killing him is convicted of the crime, the suspect's father said Thursday. At the time of the killing, Timmy Engel, 35, of Clares-holm was under house arrest while awaiting trial on charges stemming from a domestic incident last month. The murder charge against Timmy Engel hasn't been proven, but his father said the accusation raises serious questions about why his son wasn't remanded following the domestic charges in December. Calgary Herald, B1

*** 'Mockery of the system'**
An editorial states, "Being of Haitian origin has nothing to do with aboriginal culture in Canada, which is why rapist and killer Gregory Bromby should not have been entitled to an aboriginal parole hearing on Wednesday... Global News reports that in 2010-2011, 492 offenders who were up for parole asked for aboriginal hearings and 56 of those inmates were not aboriginal. Parole board hearings should deal strictly with the offender's crime, not his spiritual bent. A hearing concerns itself with justice, and should be conducted accordingly." Calgary Herald, A20

*** End of the line for second chances**
The real-life story of a Brampton man who was given a reprieve by a judge and turned his life around could soon be fodder for fables. And that's because Bill C10, expected to pass into law in Canada by the end of March, will make second chances a thing of the past. Instead, the bill's mandatory minimum sentences will make sure that people such as Maxwell Beech go to jail. Toronto Star, GT1

*** PM's priorities out of touch**
A letter states, "Canadians face 'tough choices,' PM says, Jan. 16. I guess we're fortunate to have a tough, level-headed economist at the helm. Obviously cuts must be made but, as we all know, some things are just too important to be left behind. I'm sure we can trust the Harper government to keep its priorities in order. Tax cuts for Big Business, support for Big Oil, the purchase of F-35s, the building of new prisons - these are the things Canadians want and need..." Toronto Star

*** Ashley Smith's mother to speak at Feb. 4 event**
The mother of a Moncton teen who died under troubling circumstances in a women's prison will be a guest speaker at a Moncton event aimed at dispelling myths about mental health. Times & Transcript, A9

*** Judge blasts appeal court**
One of Alberta's top judges has come out railing against his Court of Appeal colleagues for an apparent "tough on crime" agenda. Justice Ronald Berger, in a written judgment released Thursday, was highly critical of an earlier appeal court decision, which reiterated a three-year starting point for major sexual assaults. He said the sentencing guidelines established by the court in the Jordan Arcand case in 2010, "ignores the plethora of empirical studies that cast doubt on the efficacy of incarceration as a means of suppressing criminal conduct."
Calgary Sun, 8

*** Inmate dies months before completing sentence**
A Toronto man serving time for stabbing the mother of his former common-law wife to death died in custody Wednesday -- just six months before completing his 12-year sentence for manslaughter. Corrections officials say 60-year-old Joseph Caissie, an inmate at Joyceville Institution, was found unresponsive in his cell around 1:15 p.m. by correctional officers. Kingston Whig-Standard, 2 (Ottawa Sun)

*** Leave it to the law, and leave culture out**
An opinion piece states, "Can someone please tell me why we even have "culturally sensitive" parole hearings for cons seeking early release? To be honest, before the story broke this week about the Haiti-born killer who was granted an aboriginal culturally sensitive parole hearing in Winnipeg, I'd never even heard of this before... My question is, why do we even have these types of hearings? What does a person's culture, adopted or otherwise, have to do with a hearing that's

supposed to assess the risk of an offender and determine whether he or she should be granted parole?..." Winnipeg Sun, 5

*** NDP follows Einstein's maxim on crime issues**
The government of Manitoba has been on a spending spree on adult-jail operating expenses. Since 2004, the operating budget for jails has increased 83 per cent. While federal New Democrats harshly criticize the federal Conservatives for the tough-on-crime omnibus bill, the provincial NDP government has been quietly building more jails and hiring more prison guards to the extent that it dwarfs the Harper expenditures. Winnipeg Free Press, A11

*** Un pédophile au long cours déclaré délinquant dangereux**
Après 35 ans d'arrestations, de condamnations et de peines de prison, le tribunal s'est rendu à l'évidence, hier: rien ne peut guérir Jean-Claude Séguin de sa déviance, la pédophilie. Le cuisinier d'origine montréalaise, dont les derniers délits ont été commis à Granby, est automatiquement condamné à une peine de prison indéterminée, sans possibilité de libération conditionnelle avant au moins sept ans. La Voix de l'Est, 7

*** Policière en danger**
Laurent Minier, qui a sauvagement agressé une policière de Québec, en 2002, devrait être transféré, d'ici le mois d'avril, à la maison de transition Marcel-Caron, qui se trouve à moins d'un kilomètre de la résidence de la policière. Selon elle, la Commission nationale des libérations conditionnelles (CNLC) ne devrait jamais permettre que ce type d'agresseur soit retourné près des victimes, encore moins à un kilomètre de leur résidence de la victime parce que ça devient "carrément un cauchemar éveillé". Le Journal de Montréal, 9

*** Supreme Court to rule later on sex workers' Charter fight**
A controversial case over who can mount a Charter of Rights challenge to Canada's sex trade laws made it to the Supreme Court, bringing dozens of supporters to the court's front steps Thursday. Ottawa Citizen, C6

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Bilingui$me**
Un article d'opinion déclare, « On apprenait cette semaine que la prestation de services publics bilingues au Canada coûterait plus de deux milliards de dollars par année. Comme c'est exactement le même montant qu'a coûté le registre des armes à feu, j'ai bien peur que Stephen Harper veuille faire comme avec le registre, et élimine la langue française au pays!... » Journal de Montréal, 21

*** Feds eye MP pension reform**
MPs may soon be scrambling their golden nest eggs. Treasury Board President Tony Clement says his review of government spending to find an annual savings of $4 billion will include looking at MP pensions -- pensions the Canadian Taxpayers Federation has dubbed "platinum-plated." Kingston Whig-Standard, 9

*** Federal civil servants on edge over possible pension changes**
Finance Minister Jim Flaherty wants to be clear. The commitment he made in 2010 that the Conservative government wouldn't touch federal pensions didn't mean they would never be reviewed again. The Public Service Alliance of Canada (PSAC) was banking that public servants' paying higher contribution rates for their pensions would spare them from further changes or cuts to their pension plans. Calgary Herald, A5

OTHER / AUTRE

Double-murderer Ronald Smith asks to be spared death penalty
After almost 30 years in an isolation cell at Montana State Prison, Alberta-born double-murderer Ronald Smith - the only Canadian on death row in the United States - has formally filed his request for executive clemency to the state's parole board, submitting a 19-page appeal in which his lawyers describe the 54-year-old convict as a man who has made "great strides in his rehabilitation" and exhibits "heartfelt remorse," "a changed heart and mind" and "a potential for good." Smith, a native of Red Deer, Alta., was convicted in Montana of killing two Blackfeet Indian men - Harvey Mad Man, 24, and Thomas Running Rabbit, 20 - during a drug-and alcohol-fuelled road trip to the U.S. in August 1982. Leader-Post, A9

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-21-12 11:07 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne - Last Part / Dernière partie

Daily Media Summary / Revue de presse quotidienne
Last Part / Dernière partie
January 21, 2012 / le 21 janvier 2012

MINISTER / MINISTRE

I spy - Russian diplomats were feted, not expelled
Russia's Foreign Ministry weighed into the unfolding spy scandal involving a Canadian intelligence officer on Friday by denying reports that four of its diplomats at the country's embassy in Ottawa were expelled. Multiple sources within the diplomatic community say at least of two of the staffers - defence attaché Lieutenant-Colonel Dmitry Fedorchatenko and Third Secretary Konstantin Kolpakov - left the country weeks before the arrest of Sub- Lieutenant Jeffrey Delisle on charges of violating the Security of Information Act. Although not discounting the allegation of spying, those who knew the pair among foreign missions were mystified at the suggestion they were expelled. "It was well-known last fall that they were leaving. Their time was up," said one senior European diplomat, who asked not to be named. "It's all very bizarre." **Public Safety Minister Vic Toews had little to say. *"I'm not aware of why those individuals left Canada,"* said Toews, minister for Canada's intelligence service.** Hamilton Spectator, A11 (Red Deer Advocate; Charlottetown Guardian); Toronto Star; Journal de Montréal; Le Devoir (L'Acadie Nouvelle; Le Droit; La Presse); * Winnipeg Sun (Toronto Sun; Ottawa Sun); * Moncton Times and Transcript; * Globe and Mail

Harsher measures sought by province - Swan urges action on home invasions, knife crimes
Harsher penalties for thugs convicted of home invasions, carjackings and premeditated knife crimes are on Justice Minister Andrew Swan's shopping list as he and his federal and provincial counterparts meet in Charlottetown next week. Swan said Friday he will urge Ottawa to amend the Criminal Code to make home invasions and carjackings stand-alone offences to reflect the seriousness of the crimes. The Manitoba minister is also seeking to make it a federal offence to wear body armour and to fortify buildings and vehicles. **By Friday afternoon, Public Safety Minister Vic Toews had caught wind of Swan's requests. At a news conference in Ottawa, Toews implied that he supported more mandatory sentences -- although he didn't make any promises on the issue. Provincial justice ministers realize Ottawa's crime-fighting policies are working, Toews said. *"This will result in a safer Canada."* The federal minister couldn't resist a swipe at the NDP official opposition in Ottawa, which has not supported the mandatory minimums in recent federal crime bills. *"This is an NDP attorney general who is calling for more mandatory minimums,"* Toews said of Swan. *"This is certainly not in keeping with what his federal counterparts are saying."*** Winnipeg Free Press, A10; * Moncton Times and Transcript (Calgary Herald)

Border agency nets three more on most-wanted list - Immigration: Two surrendered voluntarily this week
Three more of the Canada Border Services Agency's most-wanted fugitives have been caught, with two surrendering voluntarily. **Public Safety Minister Vic Toews announced the arrests Friday.** Delson Jules turned himself in to CBSA authorities at Montreal's Pierre Elliott Trudeau Airport on Tuesday. Originally from Haiti, he was convicted in Canada of criminal harassment, uttering threats and assault. On Wednesday, Namibian national Christa Kozonguizi turned herself in to CBSA officials at the Greater Toronto Enforcement Centre. She is considered inadmissible to Canada based on "security grounds." A tip from the public led to the apprehension Wednesday of Damien Rami Butler, originally from Jamaica. The RCMP arrested him in the Greater Toronto Area and turned him over to local authorities. Butler has been convicted of a number of charges including trafficking. Meanwhile, Haitian national Jameson Seide was deported on Tuesday, the eighth man from the CBSA's most wanted list to be sent home. So far, 18 people on the CBSA's list have been located. Over 30 people on the list remain at large. Kingston Whig-Standard, 9 (Winnipeg Sun; London Free Press); Saskatoon Star-Phoenix; * Toronto Sun

Ottawa battles over jurisdiction in Rwanda case
The Federal Court of Canada, not Quebec Superior Court, has the jurisdiction to rule on Leon Mugesera's last-ditch attempt to stop his deportation from Canada, a federal government lawyer argued Friday. Mugesera, who has been in

Canada for almost 20 years but is wanted in his native Rwanda for inciting the 1994 genocide, wants Quebec Superior Court to put his deportation on hold until the United Nations Committee Against Torture can review the case. **Lisa Maziade argued Mugesera's case has been exhaustively analyzed by the public safety minister**, the Supreme Court and the Federal Court, and all have ruled the 59-year-old should leave Canada. Besides, she said, the decision of the UN commit-tee would not be binding. Edmonton Journal, A11; * Montreal Gazette; * Journal de Montréal; * La Tribune - Sherbrooke

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Naval espionage suspect fed phoney secrets – source
Authorities fed an alleged and unwitting Canadian naval spy fabricated information as part of a classic "sour milk" counter-intelligence ploy to taint the credibility of secrets the man is suspected of passing to Russia, the Ottawa Citizen has learned. "This was done by the book - sour the milk so that you confuse the other side," Michel Juneau-Katsuya, a former spy service counter-intelligence officer with sources close to the Halifax case, revealed in an interview Friday. Once naval officials suspected there was a spy in their midst, deliberately flawed information was baited and designed to eventually be discovered by its foreign recipients, casting doubt the usefulness of any other classified data related to the case. While military and RCMP investigators are still gathering details, Juneau-Katsuya said he believes Russia may have been after North Atlantic Treaty Organization secrets. Victoria Times-Colonist, A11 (Winnipeg Free Press; Vancouver Sun; Fredericton Daily Gleaner; Edmonton Journal)

Expert: Canada wise to play down spy scandal – ESPIONAGE
Foreign Affairs Minister John Baird's refusal to comment on reported expulsions of Russian Embassy personnel over an alleged spy scandal doesn't surprise one political science expert at Royal Military College and Queen's University. Christian Leuprecht says the prime suspect in the espionage case, Sub-Lt. Jeffrey Delisle, is a low-ranking individual -- and even if allegations he leaked secrets are true -- long-term surveillance would probably have kept really damaging information from falling into the wrong hands. Leuprecht noted Canada needs its relationship with Russia, especially if it hopes to coax Moscow to take a tougher line on Iran and Syria. "If you want Russia on side, we're not going to blow this out of proportion," he said. Kingston Whig-Standard, 9 (Winnipeg Sun; Toronto Sun; London Free Press; Edmonton Sun)

Canada, Russia in 'Cold War lite' - Frosty relations between countries hamper closer ties, trade: observers
Canada and Russia are waging a "Cold War lite" two decades after the fall of the Berlin Wall, experts say, following news that a Canadian naval officer was slapped with espionage charges and accused of selling top-secret information to a foreign entity. Professor Piotr Dutkiewicz, director of the Institute of European and Russian Studies at Carleton University, said the Harper government's thinking toward Russia is outmoded. "The Canadian government is stuck in a Cold-War mentality," he said. "We now have a Cold War lite." Although official diplomatic relations have proceeded steadily under the Harper government, there is a layer of frost on the relationship that is hampering closer ties and more trade, observers say. Moncton Times and Transcript, D4 (Montreal Gazette)

The spies among us - Even if Sub-Lt. Jeffrey Paul Delisle is found guilty of passing on secrets, the most sensitive details will likely stay under wraps
The allegations against Sub-Lt. Jeffrey Paul Delisle are the stuff of great spy novels. But what we know of the naval intelligence officer thus far is maddeningly mundane. The charges are grave, though few specifics of the government's case against him are known. Delisle is accused of having passed Canadian secrets to some foreign agency - reports have said Russia - starting in July 2007 and lasting through to last Friday, Jan. 13. He was arrested that day on criminal breach of trust charges and was charged on Jan. 14 with violating the federal Security of Information Act, a law brought in after the 9/11 attacks. If true, his case could become one of the most significant espionage plots in modern Canadian history. So how did a self-described "proud parent" of a teenage girl and two preteen boys get caught up in an alleged spying plot worthy of a Hollywood film? The possible reasons, as history shows us, are endless. Toronto Star, IN1

Putin's People - The Russian PM's circle supports the use of spying as a way to increase the country's international power
Russian spies haven't been this visibly active since the height of the Cold War. "Much of this goes on sub rosa and never comes to public view," said Wesley Wark, a University of Toronto security expert. "But the general view is that the post-Soviet Russian state remains wedded to a very intensive overseas intelligence collection effort. The Putin administration in particular seems extremely keen on investing in foreign intelligence, which is perhaps not very surprising, given his KGB background." (Mr. Putin is a former KGB spy, who was stationed in Dresden, East Germany, in 1985-90.) In fact, the scale of Russian spying has never really let up, despite the collapse of the Soviet Union 20 years ago. "As far as anyone can tell it has remained unchanged or even has increased since the end of the Cold War," said Prof. Wark. National Post, A16

Harkat lawyers take aim at security law - Revised certificate legislation leaves defendants in dark, team says

Lawyers for Ottawa's Mohamed Harkat have asked the Federal Court of Appeal to strike down the country's security certificate law for a second time. The Harkat case will be the first to test whether the government's revised security certificate law can withstand a challenge under the Canadian Charter of Rights and Freedoms. The previous version of the law, used to deport foreign-born terror suspects, was ruled unconstitutional by the Supreme Court in February 2007. In that ruling, Canada's high court said the security certificate process was so secretive that it denied defendants the fundamental right to meet the case against them. The government subsequently introduced a new law, which gave terror suspects the right to be represented in secret hearings by "special advocates" - defence lawyers with security clearance. Special advocates are allowed only limited contact with the accused. Harkat's legal team contends the new law still leaves defendants too much in the dark. Ottawa Citizen, D4

It's time to list Iran's Revolutionary Guard as terrorists
An opinion piece from MP Irwin Cotler states "Iran's Supreme Court has now confirmed the death sentence of Iranian-born web programmer Saeed Malekpour, a Canadian permanent resident. Malekpour was convicted of "crimes against Islam" and "spreading corruption on Earth" - which have emerged as classic trumped-up charges in the Iranian pattern of the criminalization of innocence. This case should serve as the wake-up call that the Canadian needs to sanction the IRGC and list it as a terrorist entity. The United States has already labelled it as a terrorist group, while the UN and EU have imposed various sanctions against the IRGC and its leaders. It is regrettable that Canada continues to dither with regard to listing it as a terrorist entity here in Canada. The hope is that pressure from the international community may yet convince Iran to drop the false charges in this case and free Malekpour - allowing him to return to Canada. But however this case ends, the time has come to sanction the IRGC, and list it as a terrorist entity." National Post, A18

CYBER SECURITY / CYBERSÉCURITÉ

The day the web went dark - U.S. anti-piracy bills spark outrage online
The Issue: Many of the Internet's most-used websites went dark on Wednesday to protest the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA), anti-piracy bills currently wending their way through U.S. Congress. The protest appeared to work with impressive efficiency - many proponents withdrew support for the bills, seen as deeply flawed. While Google's dramatic blacked-out logo was visible only to U.S. users, the self-imposed disabling of major sites such as Wikipedia affected users worldwide, including Canadians. Toronto Star, IN2; Charlottetown Guardian (Red Deer Advocate; Winnipeg Free Press)

Des pirates s'en prennent au FBI
La fermeture jeudi par les États-Unis du site de téléchargement Megaupload a entraîné depuis 48 heures une série de contre-attaques de pirates informatiques. Le Federal Bureau of Investigation (FBI), le ministère de la Justice et le palais présidentiel français ont tous été touchés par le mouvement Anonymous. Hier, la police néo-zélandaise a procédé à l'arrestation de quatre personnes reliées au site de partages de fichiers Megaupload. Kim Dotcom (de son vrai nom Kim Schmitz), l'ancien président et chef de la direction de Megaupload, fait partie des suspects arrêtés. Avec 150 millions d'utilisateurs et 50 millions de téléchargements chaque jour, Megaupload trônait parmi les sites les plus achalandés. Mais son contenu - musique, films, séries télé - était jugé illégal et violait les droits d'auteur. Le Soleil, 24; Victoria Times-Colonist; Toronto Star; National Post; Montreal Gazette; Le Devoir

Megaupload et Anonymous
Megaupload était l'un des sites de partage de fichiers les plus notoires au monde avec 150 millions d'utilisateurs. Son fondateur, Kim Dotcom, avait gagné 42 millions $US l'an dernier. Pour l'industrie cinématographique, le site fonctionnait avec des fichiers piratés. Le site a été fermé jeudi et est accusé d'avoir facilité le téléchargement illégal de plusieurs millions de fichiers, violant les droits de leurs auteurs. Le groupe de pirates informatiques Anonymous se présente comme un défenseur des libertés sur Internet. Le blocage de ces sites est la dernière cyberattaque d'Anonymous, un groupe de pirates disséminés dans le monde entier et représentés par un masque blanc et noir au sourire sarcastique, qui s'en est déjà pris à l'Église de scientologie ou au ministère de la Défense syrien. Le Soleil, 25

LAW ENFORCEMENT AND POLICING BRANCH / SECTEUR DE LA POLICE ET DE L'APPLICATION DE LA LOI

Heavy-handed G20 cops may face charges - Nobody has no plans to turn his other unbroken cheek, or reconstructed nose
A man arrested by police at the turbulent G20 summit 18 months ago is calling for criminal charges against the officers in light of a new report that finds they used excessive force against him. The report by the agency that investigates complaints against police concludes Adam Nobody, who was arrested at the provincial legislature in June 2010, made

substantiated allegations. The report calls on Chief Bill Blair to lay Police Act charges against five officers. "They beat me up tremendously bad," Nobody, 28, said in an interview Friday. "I had another human being stepping on my face, grinding my face into the ground. It's appalling." The report by the Office of the Independent Police Review Director names constables Babak Andalib-Goortani, Michael Adams, Geoffrey Fardell, David Donaldson and Oliver Simpson. It concludes their behaviour hurt the reputation of the police force and was of a "serious nature." Hamilton Spectator, A10 (Red Deer Advocate; Charlottetown Guardian; Halifax Chronicle-Herald); La Voix de L'Est; * Toronto Star; * Toronto Sun; * National Post; * Globe and Mail

Dozens of female RCMP officers seek justice through class-action lawsuit
Lawyers are in the final stages of drafting documents to be filed in court as early as next week that are expected to set in motion a class-action lawsuit that threatens to further destabilize one of the most iconic institutions in the country - the Royal Canadian Mounted Police. At this point, 94 current and former female members of the force from every province have asked to join the suit that is seeking damages potentially in the tens of millions of dollars for alleged maltreatment on the job. It's expected the number of women involved in the action will eventually be well over 100. Regardless of its outcome, the lawsuit, and the vast array of ugly harassment-related charges contained within it, is likely to provoke profound changes within the walls of an organization whose reputation has been shattered in recent years. New RCMP Commissioner Bob Paulson has vowed to investigate all harassment complaints thoroughly and take a zero-tolerance attitude towards workplace abuse going forward. Globe and Mail, S1

Mafia used list to deal: source - Duchesneau recalls working with officer, describes him as one of 'safest guys'
The list of police informants stolen by a retired intelligence officer in the Montreal police force was used as a bargaining chip by mafia lawyers to get reduced sentences for their clients, according to a source close to the investigation. The source told The Gazette that retired police officer Ian Davidson, who was found dead in a Laval hotel room with his throat cut, had tried to shop the list of 2,000 informants to the mafia. He said police were able to seize the list and claimed that no informant names were compromised. Montreal Gazette, A8; Journal de Montréal; Red Deer Advocate (Charlottetown Guardian); La Presse; Toronto Sun

Des bombes artisanales découvertes - CRIME ORGANISÉ ASIATIQUE
Une dizaine de bombes de fabrication artisanale ont été découvertes par hasard, jeudi, lors d'une opération visant un réseau de stupéfiants lié au crime organisé asiatique et apparemment dirigé par un ex-associé des Hells Angels Salvatore Cazzetta. Les enquêteurs de la moralité et des stupéfiants de la région ouest de la police de Montréal s'attendaient à trouver de la drogue et au moins un locataire lorsqu'ils se sont présentés dans un duplex de la rue LaSalle, à Longueuil, jeudi soir. Mais à leur grande surprise, les limiers sont plutôt tombés sur une dizaine de bombes artisanales fabriquées avec des tuyaux, communément appelées pipebombs. Ils ont aussitôt fait évacuer l'immeuble et appelé les artificiers de la Sûreté du Québec qui ont désamorcé les engins. Journal de Montréal, 25

Defence wants to know why police weren't called
The lawyer defending a Mountie on trial in Red Deer for extortion repeatedly asked a witness on Friday, who said she was terrified of the officer, why she didn't report him to police. Jennifer Henschel, who was under cross-examination, said she didn't call the police because - he was the police. "Because he was an RCMP officer. He told me he could run people out of town," Henschel said on Friday. RCMP Const. Hoa Dong La, in a judge-alone trial before Justice David Gates in Red Deer Court of Queen's Bench, is accused of using a variety of tactics for monetary gain, involving five different properties in Innisfail and Bowden and in the rural area near Bowden Institution. La, 47, faces 15 counts altogether, including three counts of extortion, two of criminal harassment and 10 of mortgage fraud. Red Deer Advocate, A2

Judge needs more time to review material in RCMP case
Judge Nancy Orr says she needs more time to review the reams of material presented in the case of an RCMP officer here facing charges of assault and confinement. The case surrounds 37-year-old Constable Darren Doucette who was not in court. He was posted to administrative duties last year when he was charged with assaulting and confining in his police cruiser 19-year-old Donovan Fitzpatrick. Doucette was responding to a noise complaint on Main Street when four men in an apartment fled out a back door and he pursued. Fitzpatrick complained the officer used excessive force. The decision by the judge is pending Feb. 23. Charlottetown Guardian, A3

Gang war escalating, police warn - Man shot to death in Surrey Thursday was half-brother of Dhak member killed in October
One of two men gunned down in Surrey late Thursday was the half-brother of a Dhak associate shot to death there in October, The Vancouver Sun has learned. And police are bracing for more violence as the death toll rises in a bloody ongoing conflict between two rival groups of gangsters. Sgt. Bill Whelan, of the Combined Forces Special Enforcement Unit, said heads of organized crime and homicide teams met Friday to strategize about what to do in the after-math of a string of gang murders, including the execution at the Sheraton Wall Centre Tuesday of high-profile gangster Sandip (Dip) Duhre. Vancouver Sun, A13; Toronto Star; Edmonton Journal; Windsor Star

Ex-Mountie gets 3 years for child porn, sexual assault
A Vancouver man who had nearly 27,000 images of child pornography on his computer and who sexually assaulted a 14-year-old boy has been sentenced to three years, three months in jail. In December, Warren Robert Allen, 53, pleaded guilty to one count of possession of child porn for the purpose of distribution and one count of sexual assault. Allen was arrested in May 2010 during a police crackdown on child pornography that resulted in more than 200 charges being laid and 57 arrests in Canada and overseas. The mitigating factors in the case included that Allen, who served as an RCMP officer in Alberta from 1978 to 1984, has no prior criminal record and is a "very intelligent, high-functioning and high-achieving" man, said the judge. Calgary Herald, A6

RCMP issue ecstasy warning in Saskatchewan
Saskatchewan RCMP are warning residents to stay away from the street drug ecstasy following several deaths associated with the drug in neighbouring provinces. "Illegal drugs are conveyed across provincial and international borders and the public needs to be aware of the inherent dangers of ecstasy and other illegal drugs," the force says in a Friday news release. The B.C. Coroners Service has found the toxic compound paramethoxymetamphetamine (PMMA) in the victims of at least five people who died after taking ecstasy in the last six months, and other deaths are under investigation. Alberta has also seen ecstasy-related deaths in recent months. No such deaths have yet been reported in Saskatchewan, RCMP say. Saskatoon Star-Phoenix, A6

Canucks tip aussies in massive drug scheme
Four men alleged to be part of an international drug syndicate were arrested Friday in Australia after police were tipped off by Canadian border security. The Canada Border Services Agency discovered 6.1 kg of cocaine, 12.3 kg of Ecstasy and nearly two kilos of methamphetamine concealed in a shipping container full of ovens at Vancouver's port. CBSA officials alerted law enforcement in Australia, where the container was bound. Toronto Sun, 25

Dad charged
A father is facing now charges after his nine-year-old son was fatally shot by his older brother. RCMP arrested the 34-year-old Sagkeeng First Nation man on charges of unsafe storage of a firearm. His 14-year-old son got his hands on a loaded weapon and accidentally shot his nine-year-old brother Nov. 3. The boy later died in hospital. The father is scheduled to appear in court Feb. 22. Edmonton Sun, 26

Penalty killers - Police union, brass drag their feet on charges
An opinion piece states "Running out the clock. With there being no one in power who seems to care, it's a strategy that's working. It's not just the Toronto Police Association ragging the puck but the chief, the board and politicians who oversee them too. The result is police do not seem accountable. The bottom line is police, as shown by routinely not co-operating with the Special Investigations Unit, don't seem to want to be accountable. The CBC's Dave Seglins broke the story that 'Ontario's top police complaints watchdog has concluded five officers involved in the now infamous arrest of G20 protester Adam Nobody should be charged with misconduct for using unnecessary force and for discreditable conduct.' Good cops need bad cops gone quickly but the sand in this hour-glass is moving slow. Justice delayed is justice denied after all. Perhaps Premier Dalton McGuinty or Mayor Ford could take some action but neither are that stupid or brave." Toronto Sun, 6

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Pickton inquiry head frustrated by slow pace
In the past week, lawyers for more than half a dozen current and former Vancouver police and RCMP officers have joined the hearings, arguing their clients' reputations have been put at stake by a report that criticized how both forces investigated missing women and Pickton. The collection of high-profile criminal lawyers all asked to cross-examine the author of that report, Peel Regional Police Deputy Chief Jennifer Evans, who conducted an external review for the commission. Evans has already been on the stand for five days, and the officers' lawyers want another week with her. Commissioner Wally Oppal, who has until June 30 to complete his report into why Pickton wasn't caught, appeared exasperated Friday as he acceded to the request. "The courts get bogged down by lengthy submissions and lengthy arguments and lengthy trials, and we're falling into the same trap here." Oppal said. Halifax Chronicle-Herald, B2

Police foresaw Pickton inquiry - Bungled investigative efforts noted in 2000
It was April 2000, the height of Robert "Willie" Pickton's killing spree. Dozens of women were already missing, and 23 more would vanish. Pickton was by then a prime police suspect. Documents disclosed recently at the Missing Women Inquiry of Commission in Vancouver offer stunning details of what police knew - or thought they knew - and what some officers didn't seem to want to know. Perhaps most telling, on April 25, 2000, RCMP officers were already discussing the possibility that bungled police efforts would lead to a public inquiry. National Post, A1

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

"Une histoire kafkaïenne", dénonce Hassan Diab
Accusé d'avoir proféré un attentat terroriste en France, dans les années 1980, Hassan Diab a parlé publiquement pour la première fois depuis son arrestation. Une vingtaine de manifestants ont voulu présenter une pétition de 650 noms au ministre de la Justice, Rob Nicholson, pour réclamer l'annulation de l'extradition de M. Diab vers la France. Selon les partisans de l'accusé, M. Diab est victime d'une méprise de la part du gouvernement français. L'"attentat de la rue Copernic" est resté gravé dans la mémoire des Français. Le groupe de manifestants réclame au passage une réforme de la loi canadienne sur l'extradition, qui devrait inclure la notion de présomption d'innocence, le droit à un procès équitable et à la divulgation de la preuve. Le Droit, 9; * Ottawa Sun; * Edmonton Journal; * Le Devoir

Whistleblowing Mexican author fears death if forced back home
A Mexican journalist fears she and her family could be killed if they are forced to leave Canada. Karla Berenice Garcia Ramirez, who sought asylum in Canada in 2008 with her husband, says threats against her life intensified after she wrote a book alleging corruption at a Mexican government ministry where she once worked. Ramirez's refugee status application was rejected in 2010. Last November, the government conducted a pre-removal risk assessment and issued a deportation order, said Lobat Sadrehashemi, one of Ramirez's lawyers. Ramirez and her husband have filed an application to remain in Canada on humanitarian grounds and are seeking a Federal Court review of the recent risk-assessment decision. Winnipeg Free Press, A22 (Vancouver Sun)

Jamaican tot found dead in suitcase
Canadian police help has been requested following the arrests in Jamaica of a Scarborough woman and her deportee husband after the remains of a two-year-old boy was found stuffed in a suitcase. Stephanie Warren, 34, a Canadian citizen, who last lived on Tuxedo Crt., and her husband, Alfanso, 32, are being detained in a Kingston jail and charges are pending, Jamaica Constabulary Force spokesman Karl Angell said on Friday. Angell said his officials have been in touch with the High Commission of Canada in Jamaica to request help from police here in probing the background of the couple, who lived in the Ellesmere and Markham Rds. area for years before returning to Jamaica. Toronto Sun, 10

Menottés à l'arrivée
Entre leur arrivée au Canada et le traitement de leur dossier, plusieurs milliers de demandeurs d'asile passent chaque année par la «case détention». Une expérience de routine pour le gouvernement canadien. Un traumatisme pour ceux qui sont emprisonnés, révèle une étude de l'Université McGill, la première du genre menée au Canada. Au moment où le gouvernement fédéral songe à systématiser la mise en détention des demandeurs d'asile et à en allonger la durée avec la loi C-4, ces résultats en inquiètent plusieurs. L'an dernier, plus de 4000 demandeurs d'asile sont passés par un centre de prévention de l'immigration, pour un séjour qui dure en moyenne 28 jours, selon l'Agence des services frontaliers du Canada (ASFC). Ces séjours ne sont pas sans laisser de traces sur la santé mentale des demandeurs d'asile. La Presse, A16

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Care and feeding of cows and inmates
An opinion piece states "In Kingston this week, in another courtroom in another courthouse far from where I was at the notorious Shafia honour-killing case, eight people went on trial for mischief. They are the holdouts from a group of 24 who were arrested in August of 2010 in protests to save the so-called 'prison farm' at the Frontenac Institution facility in this prison-heavy part of south-eastern Ontario. The judge will deliver his verdict next month. The eight had refused the chance to walk away with a charitable donation through a diversion program and demanded a trial: Essentially, they objected to the six prison farms once located at minimum-security institutions across the country (two near Kingston, and one each in New Brunswick, Manitoba, Saskatchewan and Alberta) being shut down by the federal government. The protesters failed - the Frontenac dairy herd was eventually trucked away and sold - just as those who fought to save the other farms failed." National Post, A4

INTERNATIONAL / INTERNATIONAL

Explosions rock Nigeria's Kano, at least six killed

At least six people were killed in a string of bomb blasts on Friday in Nigeria's second city Kano and the authorities imposed a curfew across the city, which has been plagued by an insurgency led by the Islamist sect Boko Haram. Kano, like other northern cities in Nigeria, has been plagued by an insurgency led by Islamist sect Boko Haram, blamed for scores of bombings and shootings against mostly government targets that are growing in scale and sophistication. Kingston Whig-Standard, 12

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Pages 1729 to / à 1736

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Klassen, Nathan

From: Bendelier, Kenneth
Sent: January-23-12 1:26 PM
To: Dincoy, Rana; Klassen, Nathan
Subject: RE: New write-up for a new event - My comments underlined

THIS WEEK AT CCIRC

NEW EVENTS REPORTED IN CANADIAN CRITICAL INFRASTRUCTURE

STRATFOR hacking. CCIRC learned from a trusted (type of authority (law enforcement?)authority that personal and credit card information of Strategic Forecasting Inc (brief description of STRATFOR) (STRATFOR)'s (delete "website", otherwise the sentence is hard to read) website report clients were posted on the Internet by a hacker group. Over [redacted] 'in this case, the type of client is important – law enforcement, etc,) were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident. (and will.....)

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure (both personal and corporate..) passwords and credit card information is secure. (Delete this line about free privacy protection) STRATFOR also offers a one-year privacy protection to clients. STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons. (In my opinion, less comments above, this is very good)*

STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack. (note sure this latter line is required)

From: Dincoy, Rana
Sent: January-23-12 1:12 PM
To: Bendelier, Kenneth; Klassen, Nathan
Subject: New write-up for a new event
Importance: High

What do you think of this:

THIS WEEK AT CCIRC

NEW EVENTS IN CANADIAN CRITICAL INFRASTRUCTURE

STRATFOR hacking. CCIRC learned from a trusted authority that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s website report clients were posted on the Internet by a hacker group. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident.

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure passwords and credit card information is secure. STRATFOR also offers a one-year privacy protection to clients. STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons.*

STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack.

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

s.16(2)(c)

Klassen, Nathan

From: Klassen, Nathan
Sent: January-23-12 1:26 PM
To: Dincoy, Rana
Cc: Bendelier, Kenneth
Subject: RE: New write-up for a new event
Attachments: THIS WEEK AT CCIRC -- Nate's comments.docx

s.16(2)(c)

Hi Rana,

Txs for the opportunity to comment. My quick thoughts are in the attached document. Sry – I did not have time to read through for editing / grammar. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

From: Dincoy, Rana
Sent: January-23-12 1:12 PM
To: Bendelier, Kenneth; Klassen, Nathan
Subject: New write-up for a new event
Importance: High

What do you think of this:

THIS WEEK AT CCIRC

NEW EVENTS IN CANADIAN CRITICAL INFRASTRUCTURE

STRATFOR hacking. CCIRC learned from a trusted authority that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s website report clients were posted on the Internet by a hacker group. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident.

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure passwords and credit card information is secure. STRATFOR also offers a one-year privacy protection to clients. STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons.*

STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack.

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

THIS WEEK AT CCIRC

New Events

1. **STRATFOR hacking.** CCIRC learned from a trusted authority that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s website report clients were posted on the Internet by a hacker group. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks. CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident.

   - ***Comment:*** *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure passwords and credit card information is secure.* ***STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons.***

Formatted: Font: +Headings (Cambria), 18 pt, Underline

Deleted: IN CANADIAN CRITICAL INFRASTRUCTURE

Formatted: Font: +Headings (Cambria), 14 pt, Italic

Deleted: *NEW EVENTS*

Formatted: Font: (Default) Times New Roman, 12 pt

Deleted: ¶
<#>¶
¶
¶

Formatted: Font: Not Bold

Formatted: Font: Italic

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.27 cm + Indent at: 1.9 cm

Deleted: *STRATFOR also offers a one-year privacy protection to clients.*

Comment [KN1]: Something on corporate emails

Formatted: Font: Italic

Deleted: ¶
STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack.¶

Dincoy, Rana

From: Dincoy, Rana
Sent: January-23-12 1:12 PM
To: Bendelier, Kenneth; Klassen, Nathan
Subject: New write-up for a new event s.16(2)(c)

Importance: High

What do you think of this:

THIS WEEK AT CCIRC

NEW EVENTS IN CANADIAN CRITICAL INFRASTRUCTURE

STRATFOR hacking. CCIRC learned from a trusted authority that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s website report clients were posted on the Internet by a hacker group. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident.

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure passwords and credit card information is secure. STRATFOR also offers a one-year privacy protection to clients. STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons.*

STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack.

Rana Dincoy
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773

s.16(2)(c)

Bendelier, Kenneth

From: Beaudoin, Luc S
Sent: January-23-12 12:42 PM
To: [redacted]
Cc: Danaitis, Algis; 'Tiago Dejesus' (Tiago.Dejesus@rcmp-grc.gc.ca); Maurizio Rosa (Maurizio.Rosa@rcmp-grc.gc.ca); CYBERDO; Darren Sabourin (Darren.Sabourin@rcmp-grc.gc.ca); * [redacted]
Subject: Anonymous anti-ACTA threat

Ref: CE12-2590

[redacted]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-23-12 8:22 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; CYBERDO; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 23, 2012/ le 23 janvier 2012

Print Media

Beware of "anti-virus" scams
The Canadian Anti-Fraud Centre, formerly Project Phonebusters, issued an alert last year about socalled "anti-virus scams." It notes the scam has been proliferating since March 2010, and police in Manitoba and Ontario dealt with an increasing number of such complaints in 2011. Leader-Post

Woman victimized by Spanish email scam
Dorothy Pilarski started getting calls from friends who thought she was stranded in Spain. Hackers had gotten into her email account and written to all her contacts, pretending to be Dorothy. Toronto Star

The gang that hijacked your computer - Meet the Koobface group, who are living comfortably in Russia - allegedly several million dollars richer
Five men believed to be responsible for spreading a notorious computer worm - and to have pocketed several million dollars from online schemes - are hiding in plain sight in St. Petersburg, Russia, investigators say. The group is known as

the Koobface gang. Beginning in July 2008, the Koobface gang targeted web users with invitations to watch a funny or sexy video. Those curious enough to click the link got a message to update their computer's Flash software, which begins the download of the Koobface malware. Victims' computers are drafted into a "botnet," or network of infected PCs, and are sent official-looking advertisements of fake anti-virus software. Their web searches are also hijacked and the clicks delivered to unscrupulous marketers. The security software firm Kaspersky Labs has estimated the network included 400,000 to 800,000 PCs worldwide at its height in 2010. Hamilton Spectator

The day the web went dark - U.S. anti-piracy bills spark outrage online
The Issue: Many of the Internet's most-used websites went dark on Wednesday to protest the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA), anti-piracy bills currently wending their way through U.S. Congress. The protest appeared to work with impressive efficiency - many proponents withdrew support for the bills, seen as deeply flawed. While Google's dramatic blacked-out logo was visible only to U.S. users, the self-imposed disabling of major sites such as Wikipedia affected users worldwide, including Canadians. Toronto Star; Charlottetown Guardian

Des pirates s'en prennent au FBI
La fermeture jeudi par les États-Unis du site de téléchargement Megaupload a entraîné depuis 48 heures une série de contre-attaques de pirates informatiques. Le Federal Bureau of Investigation (FBI), le ministère de la Justice et le palais présidentiel français ont tous été touchés par le mouvement Anonymous. Hier, la police néo-zélandaise a procédé à l'arrestation de quatre personnes reliées au site de partages de fichiers Megaupload. Kim Dotcom (de son vrai nom Kim Schmitz), l'ancien président et chef de la direction de Megaupload, fait partie des suspects arrêtés. Le Soleil; Victoria Times-Colonist; Toronto Star; National Post; Montreal Gazette; Le Devoir

Online Media

Contractors vie for edge in cybersecurity race
The cybersecurity arms race is ramping up. In this case, it's contractors that are eager to show off an increasingly expansive set of capabilities ready for government use. Many contractors have erected cyber-focused centers near Fort Meade — home to both the National Security Agency and the U.S. Cyber Command — but some are now going a step farther. Washington Post

Government to form new body to oversee telecom and cyber security
India plans to set up a new body that will oversee telecom and cyber security to avoid overlap between various ministries and intelligence agencies that are currently handling this issue. The Economic Times

Israel's hobbyist hackers cause a stir, but not much else
Israel's news cycle has been dominated for the past two weeks by increasingly panicky reports of an escalating cyber war between it and the Arab world. For all the media hullabaloo, Israeli specialists in the field of cyber security reject the term "cyber war" altogether when it comes to the recent high jinx. The danger, Weimann said, is of "an actual terrorist attack perpetuated by computers. Real cyber terror involves hitting control systems of airports or other infrastructure, nuclear facilities, transportation systems, hospitals, everything that is controlled by computers. The damage and the risk are huge." GlobalPost

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From:
Sent: January-23-12 1:48 PM
To:
Cc:
Subject: RE: CE12-2590 [Operation SACTA Posted on Pastebin]

s.15(1) - Def
s.16(2)(c)

Hi

It appears that the recent DDoS attacks (OpMegaUploader)

The following links may assist in developing an efficient IDS / IPS signature:

http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html
http://isc.incidents.org/diary/Javascript+DDoS+Tool+Analysis/12442
http://nakedsecurity.sophos.com/2012/01/20/anonymous-opmegaupload-ddos-attack/

Thanks,
Gregg

-----Original Message-----
From: @CSE-CST.GC.CA]
Sent: January-23-12 11:44 AM
To:
Subject: RE: CE12-2590 [Operation SACTA Posted on Pastebin]

Classification: UNCLASSIFIED

Thanks, we will look into it.

ctec@cse-cst.gc.ca

-----Original Message-----
From: @ps-sp.gc.ca]
Sent: January 23, 2012 11:09 AM
To:
Cc:
Subject: CE12-2590 [Operation SACTA Posted on Pastebin]

s.16(2)(c)

Regards,

Gregg Murphy
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-3579 Facsimile | Télécopieur +1 613-991-3574 gregg.murphy@ps-sp.gc.ca www.publicsafety.gc.ca Government of Canada | Gouvernement du Canada

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-23-12 12:36 PM
To: [redacted] Moore, Bruce; Williston, Sandra; Murphy, Gregg
Cc: Phlek, Vireak
Subject: RE: CE12-2590 [Operation SACTA Posted on Pastebin]

s.15(1) - Def
s.16(1)(b)
s.16(2)(c)

We could also pass to CTEC the links to the use by anonymous [redacted]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

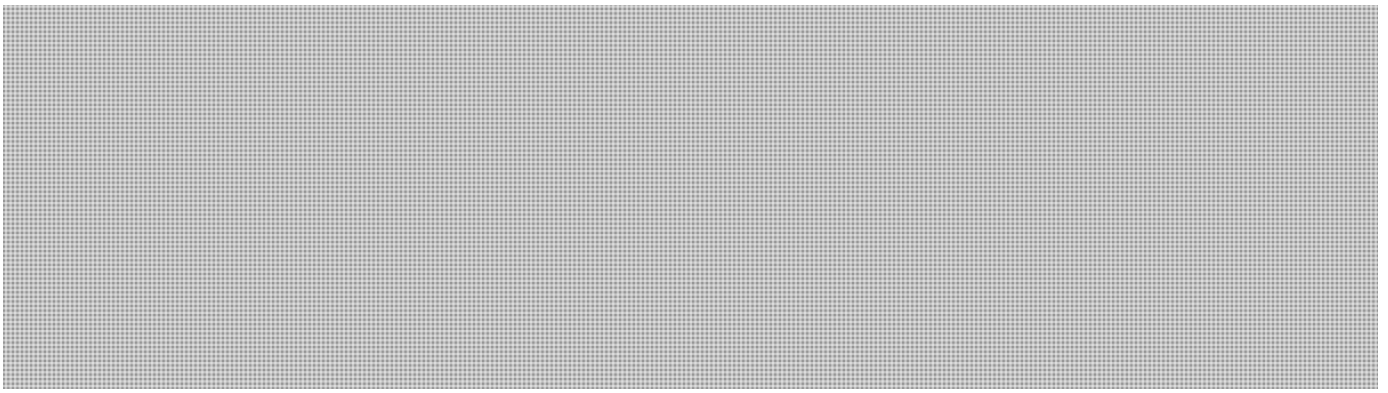
-----Original Message-----
From: [redacted]
Sent: January-23-12 11:10 AM
To: Moore, Bruce; Williston, Sandra; Beaudoin, Luc S
Cc: Phlek, Vireak
Subject: FW: CE12-2590 [Operation SACTA Posted on Pastebin]

FYI, Virak found the following on Pastebin.

-----Original Message-----
From: Gregg.Murphy@ps-sp.gc.ca
Sent: January-23-12 11:09 AM
To [redacted] CSE-CST.GC.CA> [redacted] CSE-CST.GC.CA)'
Cc: [redacted]
Subject: CE12-2590 [Operation SACTA Posted on Pastebin]

* PGP Signed: 23/01/2012 at 11:08:54 AM

[redacted]



Regards,

s.16(2)(c)

Gregg Murphy
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-3579 Facsimile | Télécopieur +1 613-991-3574 gregg.murphy@ps-sp.gc.ca www.publicsafety.gc.ca Government of Canada | Gouvernement du Canada

* Gregg.Murphy@ps-sp.gc.ca <gregg.murphy@ps-sp.gc.ca>
* 0x0077ACD7

St-Louis, Danielle

From: Beaudoin, Luc S
Sent: January-23-12 12:42 PM
To: [redacted]
Cc: Danaitis, Algis; 'Tiago Dejesus' (Tiago.Dejesus@rcmp-grc.gc.ca); Maurizio Rosa (Maurizio.Rosa@rcmp-grc.gc.ca); [redacted]; Darren Sabourin (Darren.Sabourin@rcmp-grc.gc.ca); [redacted]
Subject: Anonymous anti-ACTA threat

Ref: CE12-2590

s.16(2)(c)

[redacted]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

s.16(2)(c)

Williston, Sandra

From: Clow, Patrick
Sent: January-23-12 7:42 AM
To: Turbide, Frank; Melanson, Daryl
Subject: CyberNews

Something to consider including in Cyber News this morning.....

"After Wednesday's unprecedented unified online yelp against SOPA and PIPA, Thursday saw a new milestone: the first direct and public activist malware from Anonymous. A version of Anonymous' voluntary botnet software, known as LOIC (Low Orbit Ion Canon), was modified to make it not so voluntary, drafting unwary bystanders, journalists and even anons who don't support DDoS tactics into attacks on the U.S. Justice Department. Thursday's trickery seems not to have been central to the successful takedown of sites like justice.gov, RIAA.com and MPAA.com, but not all anons are pleased with forcing unwitting bystanders to join in a potentially illegal action.

The trick snagged those who happened to click on a shortened link on social-media services, expecting information on the ongoing #opmegaupload retaliation for the U.S. Justice Department's takedown of popular file sharing site Megaupload. Instead they were greeted by a ***Javascript version of LOIC*** *— already firing packets at targeted websites by the time their page was loaded."*

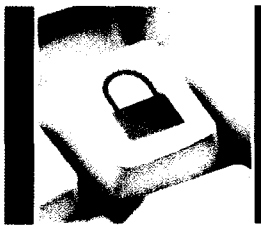
http://www.wired.com/threatlevel/2012/01/anons-rickroll-botnet/

Dincoy, Rana

From: Dincoy, Rana
Sent: January-23-12 3:47 PM
To: Bendelier, Kenneth; Klassen, Nathan
Subject: For your review - PS-SP-#543735-v11A-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_JAN_3__2012
Attachments: PS-SP-#543735-v11A-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_JAN_3__2012.DOC.doc

Your comments have been incorporated. The only thing missing is the blurb in the back on who CCIRC is, our mandate, and reporting cyber incidents to CCIRC...

Public Safety Canada | Sécurité publique Canada



Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CYBER SECURITY SUMMARY FOR CIOs

Reporting Period: JANUARY 14-28, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-002

Purpose

This product is intended to provide Chief Information Officers in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations.

This product also provides contextual background information for the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Overview

Domestically, there were no significant cyber incidents reported over the last two weeks. There were reports of Canadian computers being used for malicious purposes, including attacking a US State Police website. A Canadian federal department linked to the signing of the international Anti-Counterfeiting Agreement (ACTA) was targeted through a malicious e-mail. There was also a message on the Internet by hackers to e-mail or launch a cyber attack against this Department. Internationally, hackers attacked government websites in US, Poland, Ireland and the EU to protest signing of ACTA. There are also continued reports of infected computers in Canada and around the world due to the Ghostclick fraud.

Highlights

New Events:

- A Canadian federal department with links to ACTA targeted by hackers
- File server log in credentials of a federal department posted on the Internet
- Incidents of Canadian computers hosting malicious software
- US State Police website attack traced to Canada
- Some Canadian Industrial Control Systems (ICS) reported as being exposed to potential cyber attack".
- Phishing: Fraud attempts in the Financial sector; Cyber criminals impersonating federal organizations
- Website compromises and publicized vulnerabilities in following sectors: Canadian health, non-critical infrastructure sector and a foreign Defence Department

CCIRC Products Released during the reporting period:

- Cyber Flash on cyber attacks by Anonymous related to copyrights and intellectual property (CF12-001)

Noteworthy News in the Media:

- Israeli and Palestinian hackers exchange website attacks
- Hackers around the world protest current and intended anti-piracy measures:
    - MegaUpload's shutdown prompts hacker attacks on US government and music industry websites
    - Proposed US copyright law SOPA being protested: Certain websites elect to go dark for one day in protest; Anonymous attacks US government websites such as DOJ & FBI
    - Signing of the international Anti-Counterfeiting Agreement (ACTA) prompting hacker attacks on US, Poland, Ireland and European government websites.

NEW EVENTS REPORTED IN GOVERNMENT AND OTHER CANADIAN CRITICAL INFRASTRUCTURE SECTORS

Federal Government Sector

Operation SACTA (Stop Anti-Counterfeiting Trade Agreement): An online message signed by Anonymous posted a link to a Canadian federal department website, encouraging users to join the anti-ACTA movement, and attack if necessary. This message was posted on a popular text-file sharing website often used by hackers and is presumably encouraging cyber attacks on websites.

CCIRC provided available technical details to CTEC, the federal Government's CERT, for their further investigation.

> ***Comment:*** *There are provisions in the international Anti-Counterfeiting Trade Agreement that have important implications for content sharing on the Internet. This is a multi-lateral trade agreement which Canada has signed. Canada's new proposed copy-right law, Bill C-11 (former Bill C-32), is currently in Parliament at the second reading stage. There is a great deal of opposition to this agreement around the world by the on-line community and websites of other government have recently been attacked by hackers in protest.*

File Server (FTP) Login Credentials of a Federal Department posted on the Internet. CCIRC learned that the FTP login credentials of a federal department were posted on the Internet. CCIRC advised CTEC and provided known technical details.

> ***Comment:*** *FTP login credentials are used to gain access to a file sharing server where users may upload or download files. If a threat actor used these credentials, the result could be information compromise or the use of the server as a launch point for cyber attacks.*

Non-Federal Government Sector

Canadian computers being used in cyber attacks. CCIRC has learned that a cyber attack on a US State Police website was traced to a Canadian university's computer. In addition, another Canadian university's website was found to host malicious software that could infect website visitors. There were also reports of malicious software being hosted at a website hosting service provider's server and at two other unidentified Canadian entities.

CCIRC contacted the known Canadian organizations, with mitigation advice. The RCMP was informed of items of interest. CCIRC warned the website hosting service provider that the website in question was added to various block lists, possibly resulting in reduced legitimate traffic to this website. The malicious software from the university's website has been removed and is no longer being served.

> ***Comment:*** *It is possible that cyber criminals compromised these Canadian computers to use them remotely for malicious purposes, without their owners' knowledge. Organizations that offer computers for public use, such as universities, can be particularly susceptible to such compromises.*

Some Canadian Industrial Control Systems exposed to potential cyber attacks. A trusted international partner alerted CCIRC that information that could allow remote access to certain Canadian houses and apartment buildings' heating and air conditioning systems, was posted on the Internet. CCIRC alerted those responsible for the buildings and houses, offering mitigation advice. There is no report of any cyber attack in these cases at this time.

> ***Comment:*** *Many Industrial Control Systems (ICS), such as the ones used for heating and cooling buildings, are monitored or even maintained remotely through the use of certain software. It is likely that the technicians responsible for the set-up and maintenance of the heating systems for these buildings did not take cyber security into consideration or did not know the standard practices for protecting against such exposure.*
>
> *Since the Stuxnet virus attack on an Iranian nuclear facility, there has been a heightened awareness, both domestically and internationally, of cyber security for ICS. The trusted international partner who alerted CCIRC is focussed primarily on securing ICS. CCIRC recently moderated discussion at a ICS conference in Montreal.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonating Canadian financial institutions, tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in United States and Taiwan.

Cyber criminals also attempted to solicit personal information by impersonating Service Canada and Canada Revenue Agency.

CCIRC notified the impersonated financial institutions of these fraud attempts and the Government CTEC for the federal government cases. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website compromises and publicized vulnerabilities. CCIRC discovered a small health organization's website was defaced and offered mitigation advice. CCIRC also discovered a foreign Defence Department's website was compromised and contacted the organization, as well as CCIRC's equivalent organization. There was also a list of vulnerable websites posted on the Internet, which includes a Canadian university.

There were additional website compromises in the health and non-critical infrastructure sectors. Website usernames and passwords were posted on the Internet by hackers.

> ***Comment:*** *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

Ghostclick Fraud. There were new and continued reports of infected computers in three provincial governments, three provincial health organizations, an airport authority, an energy organization, two banks, 19 Canadian universities, a national media organization and 13 telecommunications companies.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012. There are currently websites around the world for computer users to check whether their machine is infected by the malicious software used in this fraud. These sites can be found by searching with the keywords "dns-ok".

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in. CCIRC is also working with the Canadian Internet Registration Authority (CIRA) to provide notifications to affected users.

Operation Ghostclick was worldwide fraud campaign, exposed in late 2011 by the FBI. Cyber criminals hijacked users' Internet web searches and diverted them to websites that generated advertising and sales revenues. Computers across multiple sectors, in organizations large and small, and those belonging to the general public have been affected.

> ***Comment:*** *Organizations should ensure they have taken the mitigation measures outlined in CCIRC's Information Note. CCIRC noted that the type and size of affected organizations varied, and were spread across Canada. The number of affected telecommunications companies more than likely indicates number of infected client computers of Internet via Service Providers. These Internet Service Providers receive information from CCIRC.*
>
> *Organizations that offer Internet access, including those that provide publically accessible wireless networks, may be particularly vulnerable. In addition to the cooperative effort underway between CCIRC and CIRA, the Canadian government has launched a website for cyber security public education..*

CCIRC PRODUCTS RELEASED:

Hacktivist attacks related to proposed anti-piracy legislation. There have been coordinated distributed denial-of-service (DDoS) attacks on websites by hacktivists, claiming to be associated with Anonymous. There were multiple international targets, which included governments (Canada, US, Poland, Ireland and EU) and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA).

not a redaction

In response, CCIRC issued Cyber Flash CF12-001, titled *"Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property"*. This Cyber Flash, was sent to technical and security contacts within stakeholder organizations in government and other critical infrastructure

sectors . Government and industry organizations involved with the Copyright legislation and copyrighted material were encouraged to assess their risk exposure to coordinated DDoS attacks on their networks.

NOTEWORTHY NEWS IN THE MEDIA:

Israeli and pro-Palestinian hackers exchange website attacks. Open sources reported that the websites of Israel's main stock exchange, several banks and the national airline were attacked. Pro-Palestinian hackers claimed responsibility and even claimed to have posted the login credentials for several industrial control systems in Israel on the Internet. Shortly thereafter, there were reports of suspected Israeli hackers bringing down the Saudi Stock Exchange, interfering with the Abu Dhabi Security Exchange, and publishing e-mail addresses & passwords of 30,000 Arab Facebook users.

> ***Comment:*** *It is now becoming commonplace to carry real-world grievances into the cyber world. There could be an adverse impact from these attacks for Canadians and Canadian businesses that do business with the stock exchanges or banks involved. There were some media reports that some of the Israeli banks could block international access to their sites.*

Hackers around the world attack government websites to protest anti-piracy measures.

- **Retaliation for file-sharing service Mega Upload's shutdown:** Hackers, claiming to be with Anonymous, attacked the websites of the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music.

- **Signing of the international Anti-Counterfeiting Agreement (ACTA) and proposed US copyright laws:** Wikipedia shut down for one day to protest the proposed SOPA and PIPA bills. SOPA and PIPA were also cited by Anonymous as a reason for their attacks on the DOJ and FBI websites. Operation STOP ACTA by Anonymous also prompted hacker attacks on websites for US, Poland, Ireland governments as well as for the European Parliament.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

OUR ORGANIZATION

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest.

CCIRC operates in conjunction with the Government Operations Centre within Public Safety Canada, and is a key component of the government's all-hazards approach to emergency management and national security.

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-24-12 8:21 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; CYBERDO; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; ; Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; Houston, Laura; Jones, Scott; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 24, 2012/ le 24 janvier 2012

Print Media

Scammer most foul
As it turns out, the computer virus scam is so widespread that the RCMP and Canadian Anti Fraud Centre (CFAC) issued a warning about it last fall. The RCMP says the increase in calls from frustrated Canadians indicates that the scam is actually working. Times & Transcript

Meeting a precursor to planned exercises
Top government and military leaders met at CFB Kingston last week to discuss the future of Canadian military and humanitarian missions. Hosted by 1 Canadian Division Headquarters, the discussion included representatives from Canada's army, navy, air force and special forces, as well as civilian officials from the Department of Foreign Affairs and International Trade, the Canadian International Development Agency and the **Ministry of Public Safety**. The seminar covered topics including the headquarters unit's principle responsibilities -- deployment of the Disaster Assistance Response Team (DART) , the evacuation of Canadian civilians from crisis areas and the deployment of Canadian military units -- as well as offshore piracy and cyber attack. Kingston Whig-Standard

Online Media

Microsoft fingers alleged Kelihos botnet culprit
Four months after taking down the Kelihos botnet, Microsoft on Monday identified the man it believes was behind the massive infection designed to deliver spam and steal data. ZDNet UK; CNET

Anonymous to attack Facebook on January 28 (video)
A new video allegedly from the hacktivist group Anonymous claims the next target is Facebook. Anonymous wants to take down Facebook with a Distributed Denial of Service (DDoS) attack. ZDNet

China-based Cyber Attack Targets DoD Access Cards
Cyber security firms have discovered a computer virus that uses servicemembers' network security cards to hack into government networks. Blasco said he suspects the cyber attack originates from China because of the Chinese characters found within the virus' coding. Military.com

Researcher traces 'Gameover' malware to maker of Zeus
The "Gameover" malware that the FBI warned users about earlier this month is a preview of the next version of the even-more-notorious Zeus money-stealing Trojan, a security researcher said today. Computerworld

Cyber defence managed service
Cyber attacks are on the increase. It seems that almost every day the media report on yet another serious security breach and that no one is immune. The consequences of a cyber attack are far reaching. Apart from the obvious damage that hacking causes to systems and networks; negative press, loss of credibility, loss of customers (and revenue) and long-term damage to brands can set an organisation back decades. The Guardian (UK)

Researchers demonstrate tragic state of SCADA security
Since the discovery of Stuxnet, we've been hearing from a variety of researchers about security vulnerabilities in SCADA computer systems. While some researchers such as Luigi Auriemma occasionally share with the public entire batches of SCADA flaws and PoC attacks for exploiting them, others get pressured by authorities and manufacturers into canceling their lectures about their discoveries. Help Net Security

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From: CCIRC Internal Portal - CDO Watch and Operations [redacted]
Sent: January-24-12 2:00 PM
To: Beaudoin, Luc
Subject: Cyber Events

s.16(2)(c)

CCIRC Internal Portal - CDO Watch and Operations

Cyber Events - Daily Summary

Modify my alert settings View Cyber Events

Title	Modified	Modified by	
CRA Phishing	1/23/2012 2:02 PM	Murphy, Gregg	Edited

Status Closed

Summary CCIRC received a [redacted] phishing email.

Email prompts user to click on [redacted] in order to obtain refund.

Updates Link was found to be no longer active. No action required.

[redacted] Deleted

s.16(2)(c)
s.20(1)(c)

[redacted]

1/23/2012 2:46 PM Moore, Bruce Edited

CE-Number CE12-2592

Status Closed

Summary [redacted] Drone Report: 2012-01-22
notifications to multiple organizations. Hosts within these organizations were infected with DNS Changer malware.

Updates

Mon 23/01/2012 2:07 PM
Notifications sent to IT security or technical contacts in the following organizations:
Provincial: 2 Provinces [redacted]
Energy: 1 Company [redacted]
Telecom: 15 Companies [redacted]

Transportation: 1 Company [redacted]
Academia: 10 Universities [redacted]

s.16(2)(c)
s.20(1)(b)

CI Sector Affected	[redacted] 01B Provincial; 02A Telecoms; 02C Energy; 02D Transportation; 05 Academia
Date Closed	1/23/2012 2:45 PM
REF_COL_LOOKUP	[redacted] CE12-2592 [redacted] Notifications - Multiple Organizations]

Targeted Email/Trojan .xls Attac... 1/23/2012 3:28 PM Murphy, Gregg New!

CE-Number	CEYY-nnnn
Status	Active
Title	Targeted Email/Trojan .xls Attachment Report
CCIRC Handler	Murphy, Gregg
Take-down	No
Notification	No
Reporting Organization	Other
Summary	CCIRC received a report that an infected .xls file contained [redacted] File is picked up as: http://www.naked-security.com/malware/Downloader.Sarhus/
Updates	
Incident Type	Cat 3 - MALICIOUS CODE / COMPROMISE
CI Sector Affected	01A Federal
Severity	Normal
Impact	Unknown
Primary Contact	
Related Incidents	
CCIRC/GOC Related Product Number	
Date Closed	
_NOT_USED_Secondary Contact	
_NOT_USED_IATFF Category	Event
_NOT_USED_Primary Event	No
_NOT_USED_Related Event(s)	
_NOT_USED_Assigned To	
_NOT_USED_Priority	(2) Normal
_NOT_USED_Category	(2) Category2
_NOT_USED_Due Date	1/23/2012 4:00 PM
REF_COL_LOOKUP	CEYY-nnnn [Targeted Email/Trojan .xls Attachment Report]

Targeted Email/Trojan .xls Attac... 1/23/2012 3:29 PM Murphy, Gregg Edited

CE-Number	[redacted] CE12-2593
Summary	[redacted]

http://www.naked-security.com/malware/Downloader.Sarhus/
CCIRC received a report that an infected .xls file contained [redacted]

s.16(1)(b)
s.16(2)(c)
s.20(1)(c)

File is picked up as:
http://www.naked-security.com/malware/Downloader.Sarhus/

Updates Sent encrypted notifications to [redacted]

REF_COL_LOOKUP [redacted] CE12-2593 [Targeted Email/Trojan .xls Attachment Report]

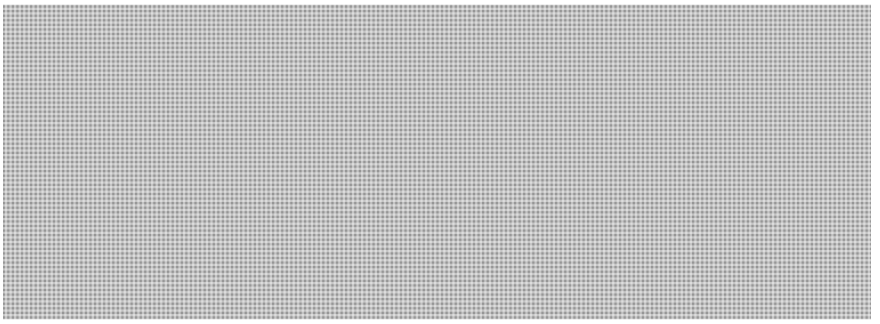
ftp credentials post on the Inte... 1/23/2012 4:51 PM Phlek, Vireak **New!**

CE-Number	CEYY-nnnn
Status	Active
Title	ftp credentials post on the Internet
CCIRC Handler	Phlek, Vireak
Take-down	No
Notification	No
Reporting Organization	
Summary	[redacted]
Updates	
Incident Type	Cat 1 - UNAUTHORIZED ACCESS / CREDENTIAL THEFT
CI Sector Affected	01A Federal; 07 Other Institutions
Severity	Normal
Impact	Unknown
Primary Contact	
Related Incidents	
CCIRC/GOC Related Product Number	
Date Closed	
_NOT_USED_Secondary Contact	
_NOT_USED_IATFF Category	Event
_NOT_USED_Primary Event	No
_NOT_USED_Related Event(s)	
_NOT_USED_Assigned To	
_NOT_USED_Priority	(2) Normal
_NOT_USED_Category	(2) Category2
_NOT_USED_Due Date	1/23/2012 5:00 PM
REF_COL_LOOKUP	CEYY-nnnn [ftp credentials post on the Internet]

ftp credentials post on the Inte... 1/23/2012 4:52 PM Phlek, Vireak Edited

CE-Number [redacted] CE12-2594

Summary



s.16(2)(c)
s.20(1)(c)

Updates

REF_COL_LOOKUP CE12-2594 [ftp credentials post on the Internet]

hxxp://4ca.ca/ CLONE site with a... 1/24/2012 12:09 PM Williston, Sandra Edited

Updates

1. CCIRC asked PS lawyer for his opinion.
2. CCIRC asked CIRA to review the Registrant's compliance with our policies, rules and procedures.
3. CCIRC advised CTEC

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-24-12 12:59 PM
To: Boily, Mario **s.16(2)(c)**
Subject: FW: Anonymous anti-ACTA threat

C est ca que j ai envoyé hier matin....

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Beaudoin, Luc S
Sent: January-23-12 12:42 PM
To: GOC-COG
Cc: Danaitis, Algis; 'Tiago Dejesus' (Tiago.Dejesus@rcmp-grc.gc.ca); Maurizio Rosa (Maurizio.Rosa@rcmp-grc.gc.ca); [redacted] Darren Sabourin (Darren.Sabourin@rcmp-grc.gc.ca); * [redacted]
Subject: Anonymous anti-ACTA threat

Ref: CE12-2590

FY Awareness.

SITUATION:

[redacted]

[redacted]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-24-12 10:20 PM
To: Beaudoin, Luc
Subject: OpsIreland

Irish Government's moves to introduce copyright legislation has gotten the attention of Anonymous as they announced this evening they plan to attack Irish websites.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

Klassen, Nathan

From: Bendelier, Kenneth
Sent: January-24-12 7:54 AM
To: Klassen, Nathan
Subject: RE: Third BN you did

Right, thanks

-----Original Message-----
From: Klassen, Nathan
Sent: January-24-12 7:53 AM
To: Bendelier, Kenneth
Subject: Re: Third BN you did

Not sure what your questions is -- I have done far more than 3 briefing notes :). Last week I did the Israeli and Anonymous ones (stat report and Rana's weekly made up our 4 SA products that week).

I was going to also do one on the Internet blackout - but we ran out of time. Cheers,

Nate

----- Original Message -----
From: Bendelier, Kenneth
Sent: Tuesday, January 24, 2012 07:42 AM
To: Klassen, Nathan
Subject: Third BN you did

Brain fart.

Got the one on Israel and the attacks in the States. What was the third one?

Thanks

Klassen, Nathan

From: Klassen, Nathan
Sent: January-24-12 7:53 AM
To: Bendelier, Kenneth
Subject: Re: Third BN you did

Not sure what your questions is -- I have done far more than 3 briefing notes :). Last week I did the Israeli and Anonymous ones (stat report and Rana's weekly made up our 4 SA products that week).

I was going to also do one on the Internet blackout - but we ran out of time. Cheers,

Nate

----- Original Message -----
From: Bendelier, Kenneth
Sent: Tuesday, January 24, 2012 07:42 AM
To: Klassen, Nathan
Subject: Third BN you did

Brain fart.

Got the one on Israel and the attacks in the States. What was the third one?

Thanks

January 23, 2012

UNCLASSIFIED

DATE:

File No.: 385262
RDIMS No.: 550276

MEMORANDUM FOR THE DEPUTY MINISTER

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEBSITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) websites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, 2012, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of Friday, January 20, 2012, most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these websites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Gregg Murphy

UNCLASSIFIED

DATE:

File No.:
RDIMS No.: 550276

MEMORANDUM FOR THE DEPUTY MINISTER

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Gregg Murphy

"Anonymous" DDoS Activity

Original release date: January 24, 2012
Last revised: --
Source: US-CERT

Overview

US-CERT has received information from multiple sources about coordinated distributed denial-of-service (DDoS) attacks with targets that included U.S. government agency and entertainment industry websites. The loosely affiliated collective "Anonymous" allegedly promoted the attacks in response to the shutdown of the file hosting site MegaUpload and in protest of proposed U.S. legislation concerning online trafficking in copyrighted intellectual property and counterfeit goods (Stop Online Piracy Act, or SOPA, and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, or PIPA).

I. Description

US-CERT has evidence of two types of DDoS attacks: One using HTTP GET requests and another using a simple UDP flood.

The Low Orbit Ion Cannon (LOIC) is a denial-of-service attack tool associated with previous Anonymous activity. US-CERT has reviewed at least two implementations of LOIC. One variant is written in JavaScript and is designed to be used from a web browser. An attacker can access this variant of LOIC on a website and select targets, specify an optional message, throttle attack traffic, and monitor attack progress. A binary variant of LOIC includes the ability to join a botnet to allow nodes to be controlled via IRC or RSS command channels (the "HiveMind" feature).

The following is a sample of LOIC traffic recorded in a web server log:

"GET /?id=1327014400570&msg=We%20Are%20Legion! HTTP/1.1" 200 99406 "hxxp://pastehtml.com/view/blafp1ly1.html" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1) Gecko/20100101 Firefox/9.0.1"

The following sites have been identified in HTTP referrer headers of suspected LOIC traffic. This list may not be complete. Please do not visit any of the links as they may still host functioning LOIC or other malicious code.

"hxxp://3g.bamatea.com/loic.html"
"hxxp://anonymouse.org/cgi-bin/anon-www.cgi/"
"hxxp://chatimpacto.org/Loic/"
"hxxp://cybercrime.hostzi.com/Ym90bmV0/loic/"

"hxxp://event.seeho.co.kr/loic.html"
"hxxp://pastehtml.com/view/bl3weewxq.html"
"hxxp://pastehtml.com/view/bl7qhhp5c.html"
"hxxp://pastehtml.com/view/blafp1ly1.html"
"hxxp://pastehtml.com/view/blakyjwbi.html"
"hxxp://pastehtml.com/view/blal5t64j.html"
"hxxp://pastehtml.com/view/blaoyp0qs.html"
"hxxp://www.lcnongjipeijian.com/loic.html"
"hxxp://www.rotterproxy.info/browse.php/704521df/ccc21Oi8/
vY3liZXJ/jcmltZS5/ob3N0emk/uY29tL1l/tOTBibVY/wL2xvaWM/v/b5/
fnorefer"
"hxxp://www.tandycollection.co.kr/loic.html"
"hxxp://www.zgon.cn/loic.html"
"hxxp://zgon.cn/loic.html"
"hxxp://www.turbytoy.com.ar/admin/archivos/hive.html"

The following are the A records for the referrer sites as of January, 20, 2012:

3g[.]bamatea[.]com A 218[.]5[.]113[.]218
cybercrime[.]hostzi[.]com A 31[.]170[.]161[.]36
event[.]seeho[.]co[.]kr A 210[.]207[.]87[.]195
chatimpacto[.]org A 66[.]96[.]160[.]151
anonymouse[.]org A 193[.]200[.]150[.]125
pastehtml[.]com A 88[.]90[.]29[.]58
lcnongjipeijian[.]com A 49[.]247[.]252[.]105
www[.]rotterproxy[.]info A 208[.]94[.]245[.]131
www[.]tandycollection[.]co[.]kr A 121[.]254[.]168[.]87
www[.]zgon[.]cn A 59[.]54[.]54[.]204
www[.]turbytoy[.]com[.]ar A 190[.]228[.]29[.]84

The HTTP requests contained an "id" value based on UNIX time and user-defined "msg" value, for example:

GET /?id=1327014189930&msg=%C2%A1%C2%A1NO%20NOS%20GUSTA%20LA%20

Other "msg" examples:

msg=%C2%A1%C2%A1NO%20NOS%20GUSTA%20LA%20
msg=:)
msg=:D
msg=Somos%20Legion!!!
msg=Somos%20legi%C3%B3n!
msg=Stop%20S.O.P.A%20:)%20%E2%99%AB%E2%99%AB HTTP/1.1" 200 99406
"http://pastehtml.com/view/bl7qhhp5c.html"
msg=We%20Are%20Legion!
msg=gh
msg=open%20megaupload
msg=que%20sepan%20los%20nacidos%20y%20los%20que%20van%20a%20nacer
%20que%20nacimos%20para%20vencer%20y%20no%20para%20ser%20vencidos
msg=stop%20SOPA!!
msg=We%20are%20Anonymous.%20We%20are%20Legion.%20We%20do%20not%20

forgive.%20We%20do%20not%20forget.%20Expect%20us!

The "msg" field can be arbitrarily set by the attacker.

As of January 20, 20012, US-CERT has observed another attack that consists of UDP packets on ports 25 and 80. The packets contained a message followed by variable amounts of padding, for example:

66:6c:6f:6f:64:00:00:00:00:00:00:00:00:00 | flood.....

Target selection, timing, and other attack activity is often coordinated through social media sites or online forums.

US-CERT is continuing research efforts and will provide additional data as it becomes available.

II. Solution

There are a number of mitigation strategies available for dealing with DDoS attacks, depending on the type of attack as well as the target network infrastructure. In general, the best practice defense for mitigating DDoS attacks involves advanced preparation.

* Develop a checklist or Standard Operating Procedure (SOP) to follow in the event of a DDoS attack. One critical point in a checklist or SOP is to have contact information for your ISP and hosting providers. Identify who should be contacted during a DDoS, what processes should be followed, what information is needed, and what actions will be taken during the attack with each entity.

* The ISP or hosting provider may provide DDoS mitigation services. Ensure your staff is aware of the provisions of your service level agreement (SLA).

* Maintain contact information for firewall teams, IDS teams, network teams and ensure that it is current and readily available.

* Identify critical services that must be maintained during an attack as well as their priority. Services should be prioritized beforehand to identify what resources can be turned off or blocked as needed to limit the effects of the attack. Also, ensure that critical systems have sufficient capacity to withstand a DDoS attack.

* Have current network diagrams, IT infrastructure details, and asset inventories. This will assist in determining actions and priorities as the attack progresses.

* Understand your current environment and have a baseline of daily network traffic volume, type, and performance. This will allow

staff to better identify the type of attack, the point of attack, and the attack vector used. Also, identify any existing bottlenecks and remediation actions if required.

* Harden the configuration settings of your network, operating systems, and applications by disabling services and applications not required for a system to perform its intended function.

* Implement a bogon block list at the network boundary.

* Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls.

* Separate or compartmentalize critical services:

  * Separate public and private services
  * Separate intranet, extranet, and internet services
  * Create single purpose servers for each service such as HTTP, FTP, and DNS
  * Review the US-CERT Cyber Security Tip Understanding Denial-of-Service Attacks.

III. References

* Cyber Security Tip ST04-015 - <http://www.us-cert.gov/cas/tips/ST04-015.html>

* Anonymous's response to the seizure of MegaUpload according to CNN - <http://money.cnn.com/2012/01/19/technology/megaupload_shutdown/index.htm>

* The Internet Strikes Back #OpMegaupload - <http://anonops.blogspot.com/2012/01/internet-strikes-back-opmegaupload.html>

* Twitter Post from the author of the JavaScript based LOIC code - <http://www.twitter.com/#!/mendes_rs>

* Anonymous Operations tweets on Twitter - <http://twitter.com/#!/anonops>

* @Megaupload Tweets on Twitter - <http://twitter.com/#!/search?q=%2523Megaupload>

* LOIC DDoS Analysis and Detection - <http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html>

* Impact of Operation Payback according to CNN - <http://money.cnn.com/2010/12/08/news/companies/mastercard_wiki/index.htm>

* OperationPayback messages on YouTube -

<http://www.youtube.com/results?search_query=operationpayback>

* The Bogon Reference - Team Cymru -
<http://www.team-cymru.org/Services/Bogons/>

The most recent version of this document can be found at:

<http://www.us-cert.gov/cas/techalerts/TA12-024A.html>

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@cert.org> with "TA12-024A Feedback INFO#919868" in the subject.

For instructions on subscribing to or unsubscribing from this mailing list, visit <http://www.us-cert.gov/cas/signup.html>.

Revision History

January 24, 2012: Initial release

* Unknown Key
* 0x5713B18C(L)

---

first-teams mailing list
first-teams@lists.first.org

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-25-12 8:17 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 25, 2012/ le 25 janvier 2012

Print Media

Hackers target Coach website
Some visitors to Coach Inc.'s website Tuesday were directed to a hacker group's site that featured a drawing of Adolf Hitler, and the retailer said it has corrected most of the issues in the U.S. The hacker site said it targeted Coach, the largest U.S. luxury handbag maker, because it supports the Stop Online Piracy Act. Calgary Herald

Online Media

Anonymous: We Will Not Attack Facebook
Hackers' collective Anonymous clarified on Monday that it has no plans whatsoever to target Facebook on Jan 28 as reported by a section of the media. ITProPortal.com

Targeted attacks will change the economics of security
Today, European Justice Commissioner, Viviane Reding, will unveil the new European Privacy Directive, designed to safeguard personal, identifiable information that is stored by private and public sector organizations. "With the

increasingly stealthy tactics employed by cybercriminals and hacktivists, companies are going to be increasingly wary of untoward activity on servers, email and Web channels. We predict that the European directive will drive a new wave of awareness and innovation in information protection and cyber security," he added. Help Net Security

ISF launches guide to help businesses prepare for cyber attacks
The Information Security Forum (ISF), an independent information security body, has launched a report giving advice to businesses on how they can prepare their organisations for cyber threats. Cybercrime is now the third biggest crime problem experienced by UK businesses according to the 2011 PricewaterhouseCoopers (PwC) Global Economic Crime Survey. ComputerworldUK

Privacy commissioner offers parents tips for online privacy
Privacy commissioner Jennifer Stoddart has produced a video, a tip sheet for parents and a kit for teachers to help kids deal with online privacy threats. She says young people often don't think about privacy problems as they surf the net. The material is aimed at children in Grade 7 and Grade 8. The online video looks at some of the privacy pitfalls associated with the web. The tip sheet offers parents a dozen points to use when discussing the issue with their children. Stoddart produced a similar package for high school students last fall, but says she wants to lower the bar as younger and younger children jump online. Canadian Press; Ottawa Citizen; CBC News; 580 CFRA News; Toronto Star

US launched cyber attacks on other nations
The assumption that the US has the technological know-how to cripple a competing nation has always been just that: as assumption. In a recent sit-down interview, however, a former spy chief confirmed that America has already waged cyber attacks. Mike McConnell, the former director of national intelligence at the National Security Agency under George W Bush, tells Reuters this week that cyber war is more than a distant possibility. According to the current vice chairman at Booz Allen Hamilton, the US has already launched attacks on the computer networks of other nations. RT

The not-so-advanced persistent threat
Stuxnet, DuQu and the advanced persistent threat (APT) are currently dominating the headlines. Sophisticated zero-day exploits, carefully researchered and planned attacks that appear to be almost impossible to defend against, have many security professionals wondering if this is a game they can possibly win. The part that is often overlooked: These attacks target only a small number of organizations. SC Magazine

Hackers hijack US trains
Foreign hackers apparently took control of the US Northwest rail company's computers and played trains with the railway signals twice in December. Apparently the train service on the unnamed railroad "was slowed for a short while" and rail schedules were delayed about 15 minutes after the interference. Having caught a US train from New York to Florida and arrived a day and a half late we are surprised that any one noticed a 15 minute delay. The next day before rush hour, a "second event occurred" that did not affect schedules, TSA officials added. The report into the train hack seems to be its first major brush with cyber crime. The Homeland Security Department, which oversees TSA, is not sure if the rail infiltration was a targeted attack. However, it seems that the events were enough to start the TSA on a programme to educate the train companies on the perils of hacking. TechEye.net; Nextgov

Microsoft fingers alleged Kelihos botnet kingpin
Microsoft has filed a lawsuit against a Russian national who allegedly created and operated the Kelihos botnet, prior to a takedown operation in September 2011. The Register

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From: Bergeron, Dominic
Sent: January-25-12 1:48 PM
To: Bakri, Kareem
Subject: RE: The US "getcybersafe" equivalent Hacked

I'm pretty sure our internet provider has a mechanism in place too but unsure how efficient it is.
A bunch of sites were taken down last week including the fbi.

From: Bakri, Kareem
Sent: January-25-12 1:47 PM
To: Bergeron, Dominic
Subject: Re: The US "getcybersafe" equivalent Hacked

There are mechanisms built into both the [redacted]

Kareem Bakri
991-2945

From: Bergeron, Dominic
Sent: Wednesday, January 25, 2012 01:45 PM
To: Bakri, Kareem
Subject: RE: The US "getcybersafe" equivalent Hacked

Real question: How can we effectively protect ourselves against distributed denial of service (thousands of nodes)

From: Bakri, Kareem
Sent: January-25-12 1:27 PM
To: Bergeron, Dominic
Subject: FW: The US "getcybersafe" equivalent Hacked

Did you hear anything about this yet?

From: McCorkell, Shawn
Sent: January-25-12 12:31 PM
To: Bakri, Kareem
Subject: Fw: The US "getcybersafe" equivalent Hacked

From: Szauksztun-Zvinis, Robert
Sent: Wednesday, January 25, 2012 12:28 PM
To: Hunter, Linda; Robertson, Steve; Charette, Yves
Cc: McCorkell, Shawn; Ecker, Neil
Subject: FW: The US "getcybersafe" equivalent Hacked

FYI

Robert Szauksztun-Zvinis

Manager | Gestionnaire
Applications and Server Platforms Division | Division des applications et plates-formes du serveur
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West Ottawa ON K1A 0P8 | 269 avenue Laurier ouest Ottawa ON K1A 0P8
robert.szauksztun-zvinis@ps-sp.gc.ca
Telephone | Téléphone 613-991-7048
Facsimile | Télécopieur 613-948-8877
Government of Canada | Gouvernement du Canada

From: MacKenzie, Sara
Sent: Wednesday, January 25, 2012 10:38 AM
To: Eke, Darren; Stanfield, Charles; Hannan, Andrew; Jarrette, Amy; Charette, Yves; Szauksztun-Zvinis, Robert; Crépeault, David
Subject: Fw: The US "getcybersafe" equivalent Hacked

FYI

Yves, Robert: please forward to others as required.

From: Champoux, Martin
Sent: Wednesday, January 25, 2012 10:34 AM
To: Beaudoin, Luc S; Hatfield, Adam
Cc: Swift, Andrew; MacKenzie, Sara
Subject: RE: The US "getcybersafe" equivalent Hacked

I have already passed it on.

From: Beaudoin, Luc S
Sent: Wednesday, January 25, 2012 10:22 AM
To: Champoux, Martin; Hatfield, Adam
Subject: The US "getcybersafe" equivalent Hacked

This is to draw you attention to the CCIRC daily entry from yesterday. Could you please forward to the GetCyberSafe site team ?

5. Title : US govt security website hacked
Portal offering Internet security advice taken offline by hacktivist group Anonymous in protest of piracy crackdown
Hacktivist group Anonymous has claimed responsibility for taking down a website operated by US Federal Trade Commission (FTC) that offers Internet security advice to consumers.
The hit on OnGuardOnline.gov appears to go beyond the usual denial of service attack. The Pastebin post claiming responsibility for attack purports to show a log of the intrusion in progress, with the hacker gaining complete access to the site's back-end MySQL database and posting links to a full copy of its copied structure.
Reference: http://www.information-age.com/channels/security-and-continuity/news/1687113/us-govt-security-website-hacked.thtml

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca

Williston, Sandra

From: [redacted]
Sent: January-25-12 4:01 PM
To: Beaudoin, Luc
Subject: Activity Log

CCIRC Internal Portal - CDO Watch and Operations

Activity Log - Daily Summary

Modify my alert settings View Activity Log

Title	Modified	Modified by	
Weekly technical report	1/24/2012 4:27 PM	Beaudoin, Luc S	New!

Date/Time 1/24/2012 5:00 PM

Short Description Weekly technical report

Issue Status Closed

Detail Description Vireak put together.

Indicator research:

Indicators

SQL injections attempts initiated from [redacted]

s.16(2)(c)
s.19(1)

s.16(2)(c)

Handler Beaudoin, Luc S

Updates

CI Sector / Client Group 01A Federal; 01B Provincial; 01C Municipal

Context

Projects

N&T 25 Jan 2012 1/25/2012 8:04 AM Williston, Sandra New!

Date/Time 1/25/2012 9:00 AM

Short Description N&T 25 Jan 2012

Issue Status Closed

Detail Description N&T 25 Jan 2012

Handler Phlek, Vireak

Updates

CI Sector / Client Group

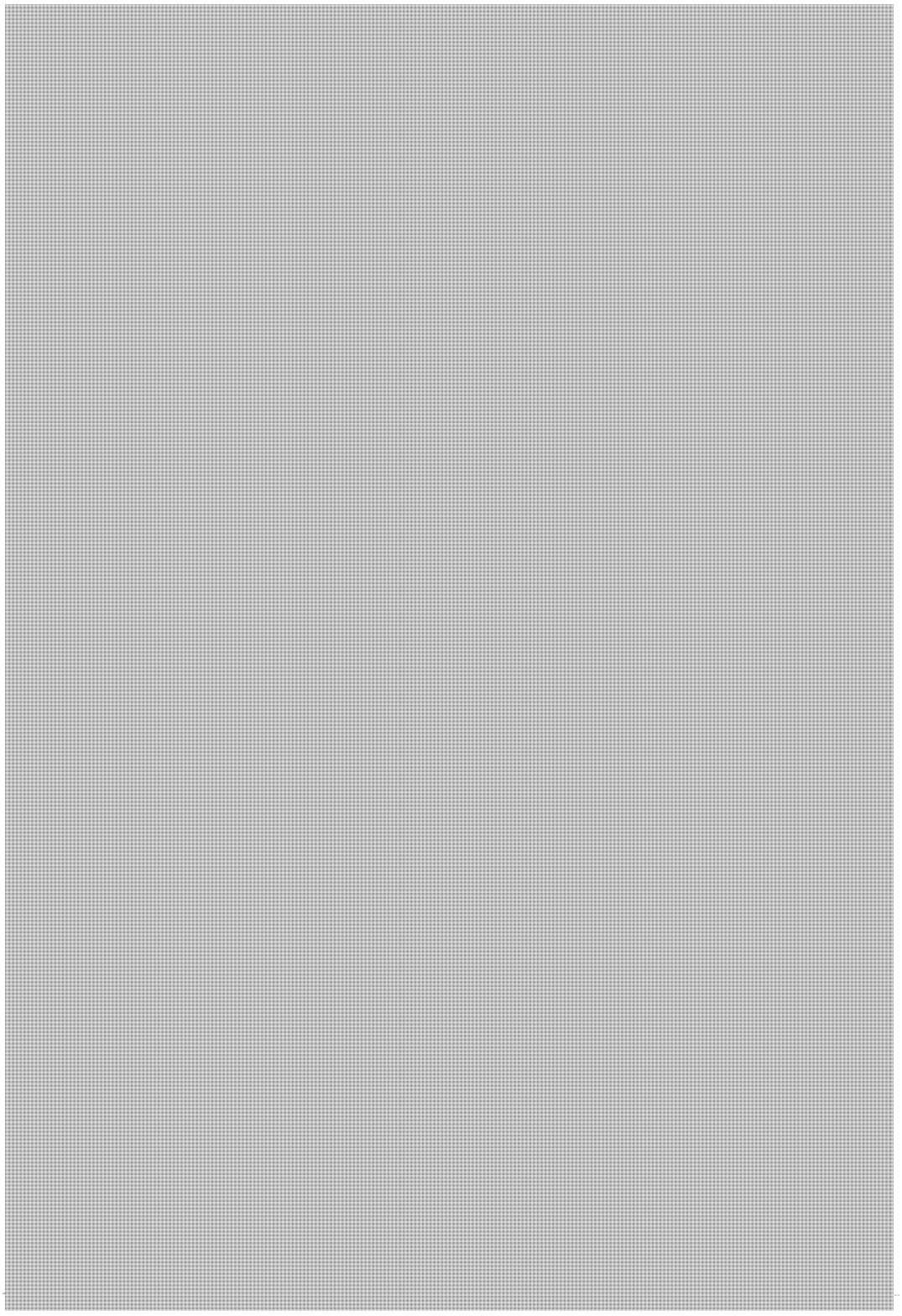
Context

Projects

Weekly technical report

1/25/2012 8:27 AM Beaudoin, Luc S Edite

Detail
Description



s.16(2)(c)

Page 1790

is withheld pursuant to section

est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Updates

PKI public key for CFNOC - Daily... 1/25/2012 9:20 AM Williston, Sandra **New!**

Date/Time 1/25/2012 10:00 AM

Short Description PKI public key for CFNOC - Daily Reports

Issue Status Closed

Detail Description CCIRC produces a daily report which covers the past 24 hours Events, Activities, International reporting, publications released, vulnerability and threat watch reporting, and current Cyber News.

This report is released, to a limited distribution list, using PKI

If CFNOC is able to provide a PKI key, either for the Group account [redacted] (or other group address) or an individual who holds a PKI key. CCIRC would like to add you to our distribution list for this daily product.

Handler Williston, Sandra

Updates Good Morning MCpl Ennover;

Thank you for your response.

The email address you provided below is an internal DWAN address and will not work on our systems external to DND. However, I assumed you meant to send me the SMTP address, [redacted] which I attempted to test using PKI and was unsuccessful. No address match found.

Is it possible to EXPORT the public key and send to us? Once received, I would like to do a test.

Please advise. Thanks!

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca
"Patience isn't a skill — it's a decision"
From: TERRY.ENNOVER@forces.gc.ca [mailto:TERRY.ENNOVER@forces.gc.ca]
Sent: January-25-12 8:12 AM
To: [redacted]
Cc: GRAHAM.BELL@forces.gc.ca
Subject: FW: CCIRC Daily Situation Reports

Good day Sandra

s.16(2)(c)

CFNOC Incident Handling [redacted]

[redacted]

Cheers

CI Sector / Client Group

Context

Projects

Anonymous response to MegaUpload 1/25/2012 9:27 AM Williston, Sandra New!

Date/Time 1/25/2012 10:00 AM

Short Description Anonymous response to MegaUpload

Issue Status Closed

Detail Description Information pertaining to Anonymous response to MegaUpload

Handler Williston, Sandra

Updates

CI Sector / Client Group

Context

Projects

CF12-XXX ["Anonymous" DDoS Activ... 1/25/2012 10:11 AM CYBERDO New!

Date/Time 1/25/2012 11:00 AM

Short Description CF12-XXX ["Anonymous" DDoS Activity]

Issue Status Closed

Detail Description Processing for CF12-XXX

Handler Williston, Sandra

Updates

CI Sector / Client Group

Context

Projects

CF12-XXX ["Anonymous" DDoS Activ... 1/25/2012 10:11 AM CYBERDO Edite

Short Description [redacted] CF12-XXX ["Anonymous" DDoS Activity] - Processing

Updates

Shodan - account CyberDo 1/25/2012 11:06 AM Phlek, Vireak New!

Date/Time 1/25/2012 12:00 PM

Short Description Shodan - account CyberDo

Issue Status Closed

Detail Description Create an account for CyberDo in the shodan search engin.

Handler Phlek, Vireak

Updates

CI Sector / Client Group

Context Account creation

Projects

s.13(1)(a)
s.16(1)(b)
s.19(1)
s.20(1)(c)

Contact - [redacted] 1/25/2012 1:27 PM Williston, Sandra New!

Date/Time 1/25/2012 2:00 PM

Short Description Contact - [redacted]

Issue Status Closed

Detail Description GOC got a request for CDO to call [redacted]

Handler Phlek, Vireak

Updates I recommended that they send their question to communications@ps-sp.gc.ca with the attention to NCSD and that they clearly indentify the scope of their definition of smartGrid.

CI Sector / Client Group

Context

Projects

[redacted] 1/25/2012 3:04 PM Beaudoin, Luc S New!

Date/Time 1/25/2012 3:00 PM

Short Description [redacted]

Issue Status Closed

Detail Description [redacted]
- Tool fixing DNS setting: AVIRA, exe for windows.
- Talk to identifying the source of the data publically, and raising awareness.
- Proposed a single eye-chart with multi-language.

Updates

CI Sector / Client Group 04 Trusted Security Partners

Context

Shodan - account CyberDo 1/25/2012 3:37 PM Phlek, Vireak Edite

Updates

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-25-12 12:36 PM
To: [redacted]
Subject: CF related
Attachments: [redacted]

Could you have a look to see if additional info here would be relevant to CF ? I am reviewing CF....

s.13(1)(a)
s.16(2)(c)

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Beaudoin, Luc S
Sent: January-24-12 1:08 PM
To: Beaudoin, Luc S
Subject: JS LOIC

[redacted]

Distribution is GREEN (ie: OK to share with need-to-know partners but not to post publicly)

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Anderson, Windy

From: Bendelier, Kenneth
Sent: January-25-12 9:01 AM
To: Dick, Robert
Cc: Hatfield, Adam; Cameron, Bud; Beaudoin, Luc S; Anderson, Windy
Subject: Deck For CCIRC <-> DHS Brief
Attachments: CCIRC Overview Presented to DHS.ppt

Importance: High

Good morning,

Please find attached the proposed CCIRC – DHS Brief for tomorrow. It is, essentially, relevant plagiarism of the Brief to the DM, Adam's Brief to the DND IA Symposium with additional input from CCIRC's Operations Section.

For your review.

Thanks

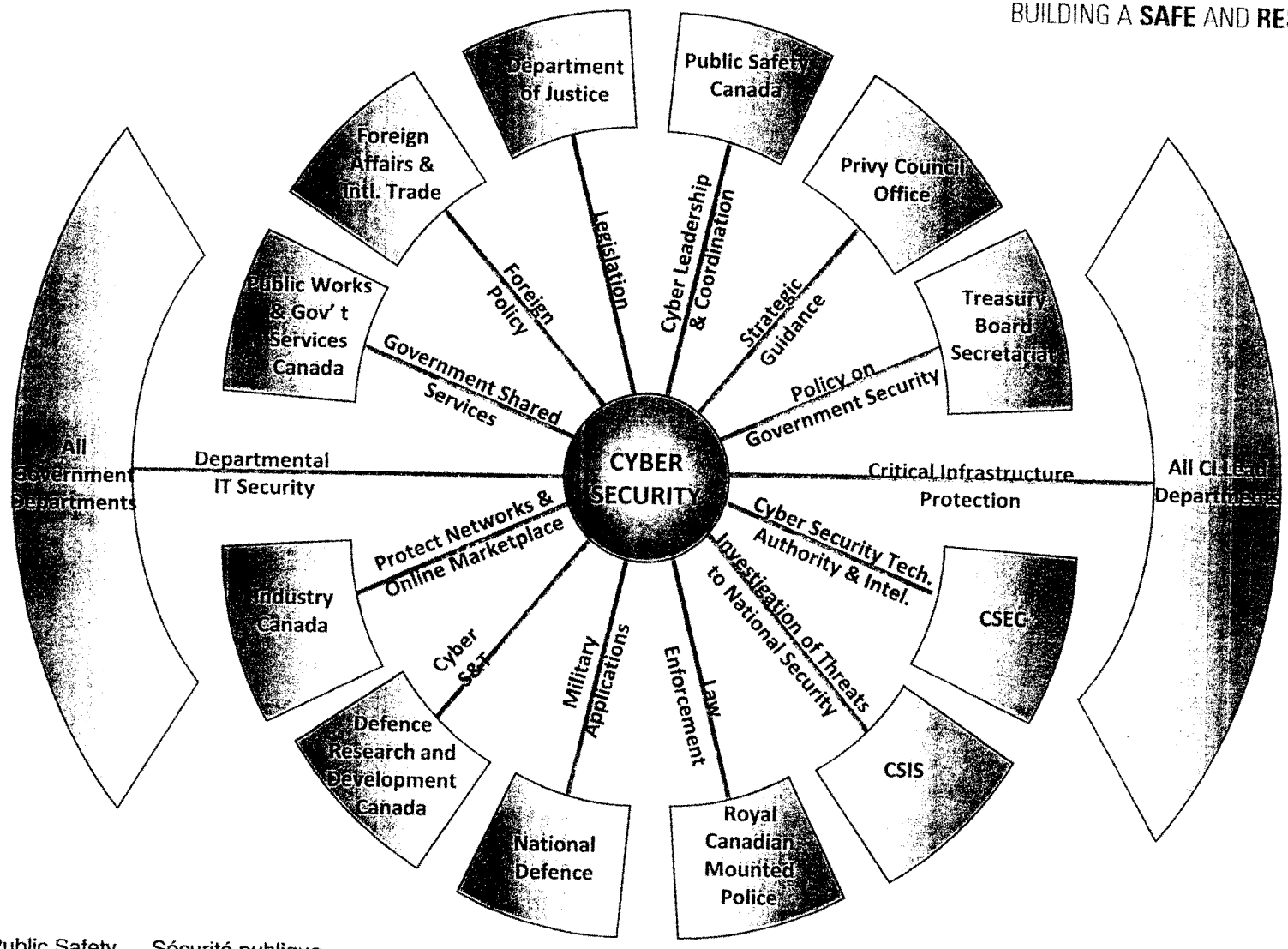
Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-993-5042
Facsimile | Télécopieur +1 613-954-3097
Kenneth.Bendelier@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

UNCLASSIFIED

...curity Roles and Responsibilities ...m the Government of Canada

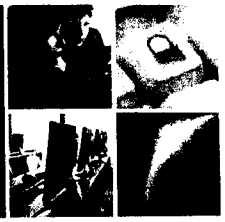
BUILDING A **SAFE** AND **RESILIENT CANADA**



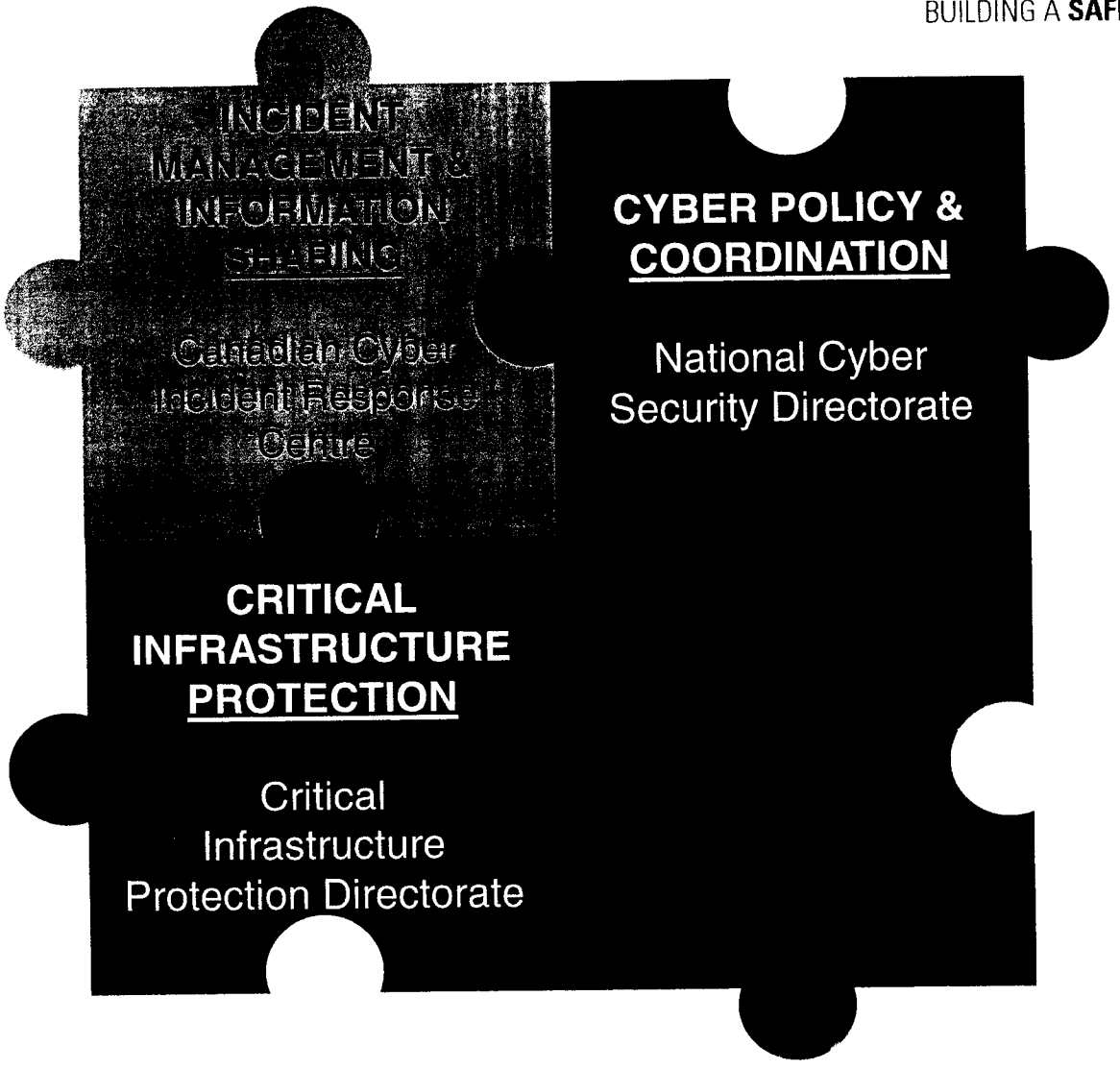
Public Safety Canada | Sécurité publique Canada

001796

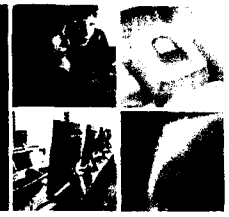
Cyber Security Roles and Responsibilities within Public Safety Canada



BUILDING A **SAFE** AND **RESILIENT CANADA**



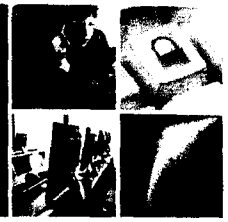
Division of Cyber Security Roles in Canada



BUILDING A **SAFE** AND **RESILIENT CANADA**

- On June 20, 2011, the responsibilities between Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) and Communications Security Establishment Canada (CSEC) were modified in terms of cyber incident management:
  - CSEC has created the Cyber Threat Evaluation Centre, which is the computer emergency response team for federal departments and agencies.
  - CCIRC is now the national computer emergency response team for provinces, territories and critical infrastructure sectors.

Proposed Mandate



-FOR DISCUSSION ONLY

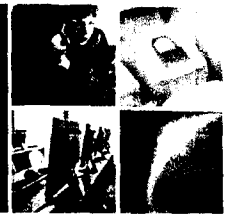
Proposed mandate

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

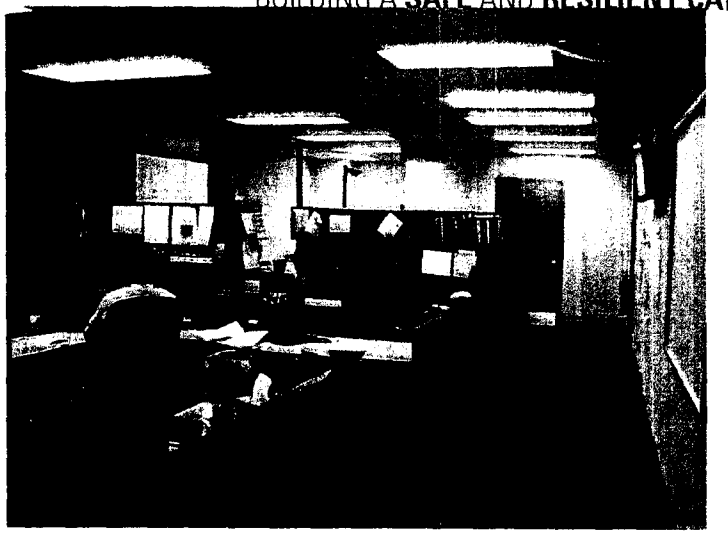
As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention, mitigation, and response to cyber events.

CCIRC provides authoritative advice to, and coordinates information sharing and event response among, all levels of government, international counterparts, critical infrastructure operators and information technology vendors.

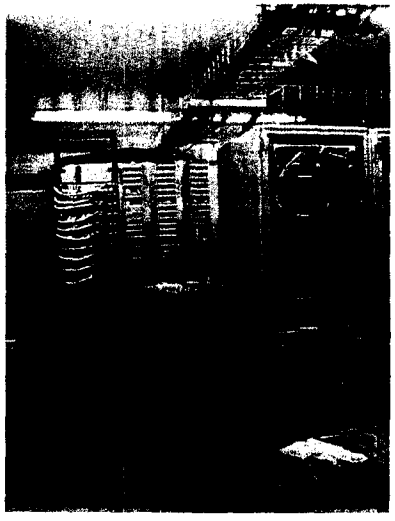
CCIRC – what it is



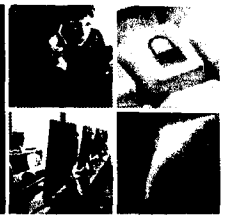
- Incident response centre
  - primary contact point into Government for domestic and international partners
  - CCIRC subject matter experts respond 9-5, 5 days a week
  - after hours coverage by Government Operations Centre



- Computer lab
  - isolated from corporate network for analyzing malicious software and testing solutions
  - industrial control system equipment for security testing and analysis in support of CI sectors



CCIRC – who it is



- 22 FTEs, 14 staffed
  - mainly highly specialized computer specialists (CS) with knowledge of IT security, computer forensics, and incident handling
  - 4 positions to be staffed for analysis of multi-source intelligence and technical data and writing strategic assessments
- Organized into three functions:
  - Incident Handling – assists partners in identifying, mitigating, and managing incidents
  - Technical Support – operates CCIRC lab infrastructure and provides technical analysis support to incident handling and analysis
  - Strategic Initiatives and Situational Awareness – builds and maintains operational relationships with partners, and produces strategic analysis products for decision makers

CCIRC – what it does

-These partners…

-Government S&I community

-Critical Infrastructure

-Provinces and territories

-Five Eyes and International CERTs

-Trusted vendors

-Academia

-Cyber security -expert community

-Open source

provide information to…

-CCIRC

which provides these services:

~~Incident Handling and National Event~~ Coordination and Assistance

-- Direct technical assistance to partners and coordination of Government response to cyber events of national significance

-- Audience: technical staff in partner organizations responding to cyber incidents

-- Metric: 749 incidents responded to in 2011; 197 notifications to partners of compromised systems, 9 requests issued to shut down ~~malicious systems in Nov/Dec 2011~~

-Provision of Mitigation Advice

-- Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice

-- Audience: technical staff in partner organizations

-- Metric: 27 Cyber Flashes, 6 Alerts, 49 Advisories, and 13 Technical Notes in 2011

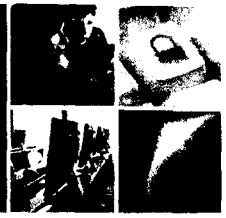
~~-Reporting and Analysis~~

-- Daily, weekly, monthly and annual reports providing summary, trend, and strategic analysis

-- Audience: technical staff, decision makers (~~under development~~)

UNCLASSIFIED

CCAP: CCIRC Cyber Awareness Products



BUILDING A **SAFE** AND **RESILIENT CANADA**

-Currently Produced

-In Development

Product	CyberFlash	Daily Report	Weekly Technical Report	Information Notes	Technical Report	Advisory	Monthly Statistical Report	Weekly SA Report	Monthly SA Rollup	Issue of the Month	Annual Report	Ad hoc
Description	Time sensitive reports for immediate security issues ➢ Security fix unavailable	Daily situation report	Summary of daily reports, CCIRC products / events / activities / indicators / and cyber reporting	Report on significant cyber events ➢for general awareness	Detailed report WRT a cyber security issue ➢Ad hoc	Cyber security advisory on threat and vulnerability ➢ Security fix available	All CCAP products + (1) incidents handled ; (2) take down requests; and (3) victim notifications	Notable cyber events / CCIRC products / open source reports	Summary of weekly SA reports for ADM	Single strategic cyber issue analysis	Yearly status report WRT Canadian cyber security	Strategic cyber issue 1 pagers
Clients	P/T/CI operational contacts	CCIRC / trusted GoC partners	P/T/CI/GoC operational contacts	P/T/CI/GoC ➢Posted on website	P/T/CI operational contacts	P/T/CI operational contacts ➢Posted on website	Public Safety /other Federal departments	GoC managers / executives P/T/CI partners	Public Safety / Senior GoC executives	P/T/CI partners	Public	Public Safety

-Operational / Technical

-Strategic

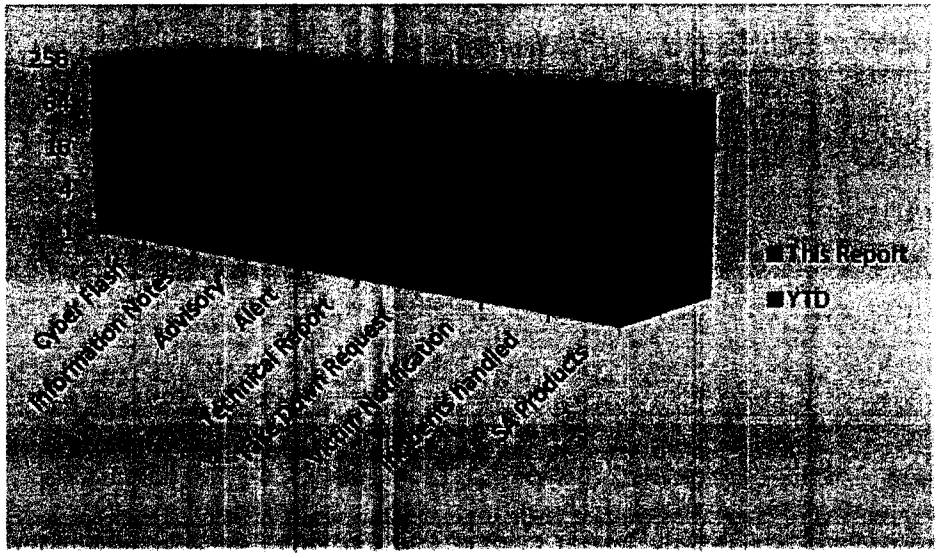
Public Safety Canada | Sécurité publique Canada

001803

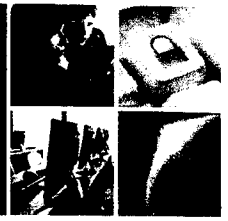
CCIRC Activity Summary

BUILDING A **SAFE** AND **RESILIENT CANADA**

CCIRC Activities -- January 16 - 22									
	Cyber Flash	Information Notes	Advisory	Alert	Technical Report	Take Down Request	Victim Notification	Incidents handled	SA Products
This Report	0	0	1	0	0	3	110	20	4
YTD	0	0	3	0	0	5	176	60	9

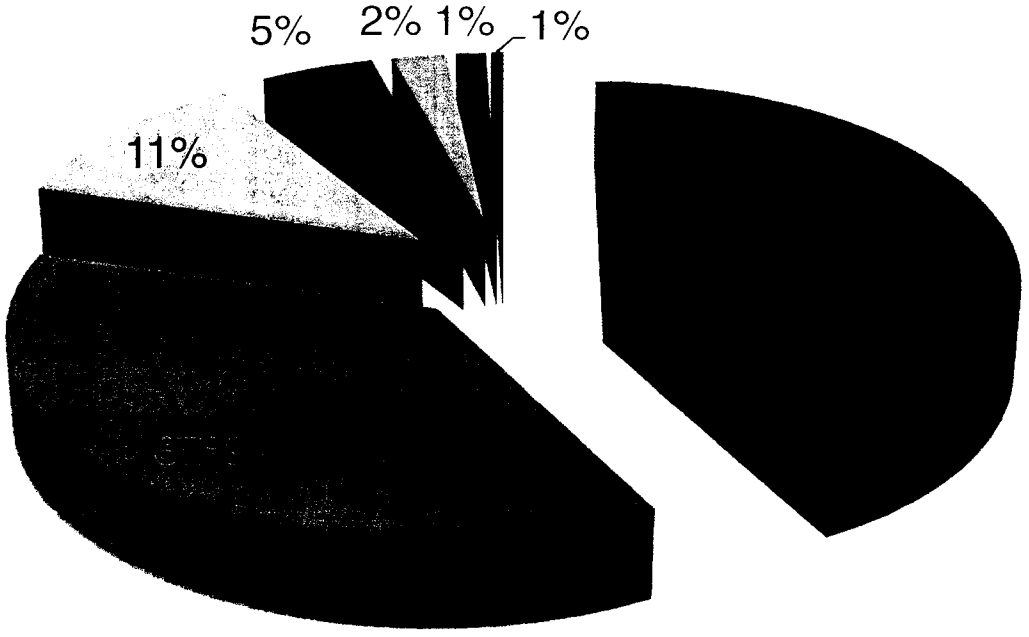


Stats



BUILDING A **SAFE** AND **RESILIENT CANADA**

Events



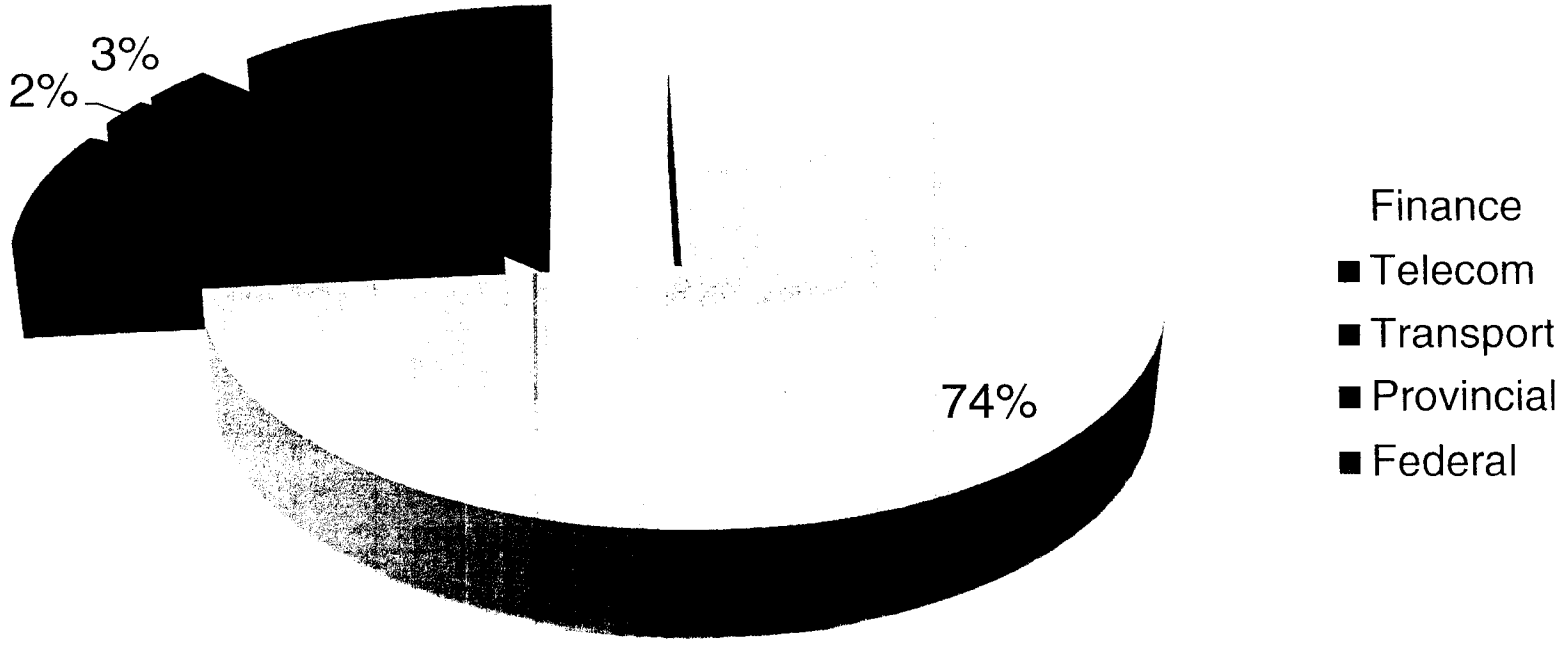
- Cat 3 - MALICIOUS CODE / COMPROMISE
- Cat 7 - PHISHING / TARGETED EMAILS
- Cat 6 - INVESTIGATION / RESEARCH
- Cat 4 - IMPROPER USAGE / MISCONFIG
- Cat 1 - UNAUTHORIZED ACCESS / CREDENTIAL THEFT
- Cat 5 - SCANS/PROBES/ATTEMPTED ACCESS
- GridEx

Public Safety Canada | Sécurité publique Canada

Phishing Reports

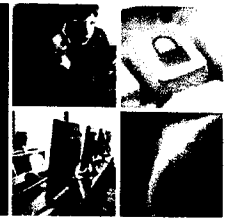
BUILDING A **SAFE** AND **RESILIENT CANADA**

Phishing Reports to CCIRC
Jul 2011 - Jan 2012



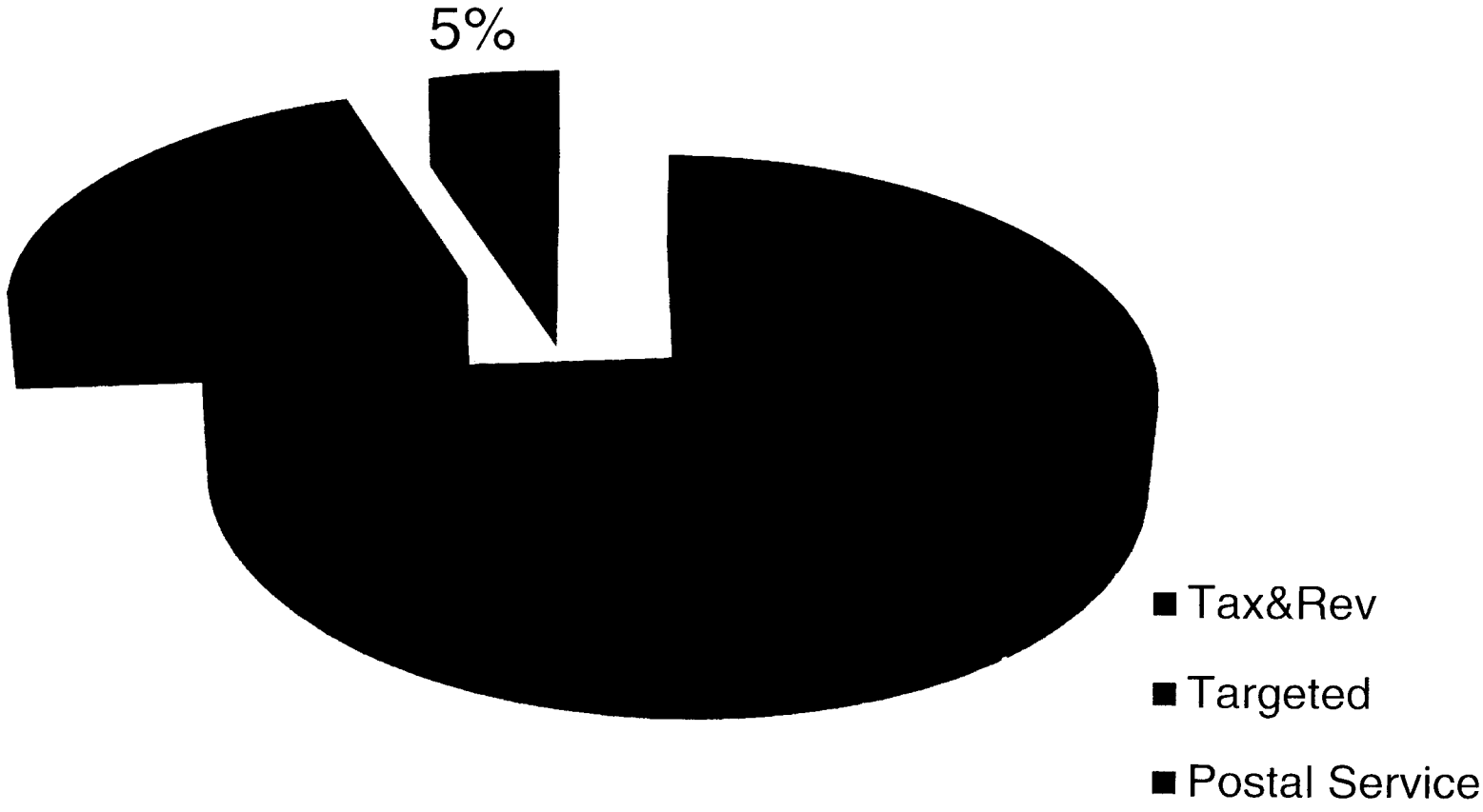
Public Safety Canada | Sécurité publique Canada

Phishing Reports



BUILDING A **SAFE** AND **RESILIENT CANADA**

Federal



Public Safety Canada / Sécurité publique Canada

Where CCIRC fits in *Canada's Cyber Security Strategy*

BUILDING A **SAFE** AND **RESILIENT CANADA**

-Securing Federal Government Systems

-Key actors:

- CSEC
- Shared Services
- TBS CIOB
- CF

-Partnering to Secure Vital Systems Outside the Federal Government

-Key actors:

- PS CCIRC, NCSD, CISCD
- CI Sector lead departments

-Existing effort:

- PT, select CI (telecom, energy, finance)
- U5 CERTs

-Future effort:

- trusted vendors
- international CERTs
- remaining CI sectors
- economic interests
- academia

-Helping Canadians to be Secure Online

-Key actors:

- PS Communications
- law enforcement
- Industry Canada
- CRTC
- Privacy Commissioner
- Competition Bureau

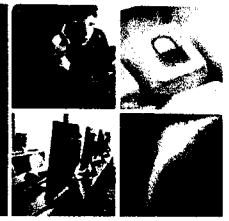
-Audiences:

- Home users
- Academia
- Small business

-State-sponsored cyber espionage ← ***-Risk*** → **-Crime**

Public Safety Canada | Sécurité publique Canada

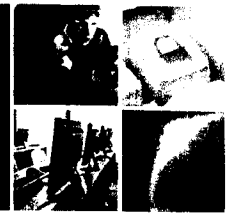
Partnership Focal Areas



BUILDING A **SAFE** AND **RESILIENT CANADA**

- Federal Government Partners
  - Security and Intelligence Leads
  - Industry Canada / Competition Bureau / Privacy Commissioner
- Provinces and Territories
- Critical Infrastructure
  - Canadian Electrical Association
  - Canadian Association of Petroleum Producers
  - Finance Sector
  - Telecommunications Sector
- International Partners
  - U5
  - International Watch and Warning Network (IWWN)
  - Forum for Incident Response and Security Teams (FIRST)

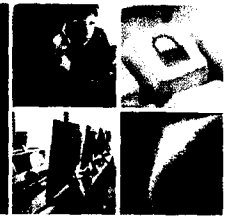
Current Initiatives



- [redacted] tools being reviewed
- [redacted] implementation in the next quarter
- Notification tool for email and CI sector IP range, domain and ASN matching implemented operationally
- SCADA/ICS simulation and VA tools being deployed
- Significant overhaul of lab infrastructure
- Partner Portal

s.16(2)(c)

CCIRC – US-CERT Cooperation



BUILDING A **SAFE** AND **RESILIENT CANADA**

- **Assistance with malicious site Take-down in the US:**
  - Canada Revenue Agency Phishing
  - Targeted Email and associated infrastructure (hop host, etc)

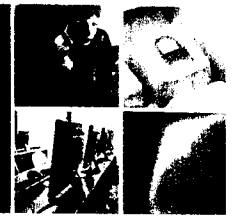
- **Sharing of threats and vulnerabilities:**

s.13(1)(a)
s.16(2)(c)

  - [redacted]
  - APT related indicators (ex: IP, URL, phishing email samples)
  - Hacktivist (ex: Anonymous during Tarmageddon)
  - Crimeware (ZeuS, BlackHole)
  - Pastebin information related to CAN/US : vulnerable systems, SCADA, accounts…

- **Industrial Control Systems**
  - Web exposed ICS devices notifications
  - Vulnerability coordination with SCADA Canadian companies

Contacting CCIRC



BUILDING A **SAFE** AND **RESILIENT CANADA**

Government Operations Centre

s.16(2)(c)

[redacted]

(request CYBERDO)

PGP: http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx

www.publicsafety.gc.ca/cyber

www.publicsafety.gc.ca/ci

s.16(2)(c)

Williston, Sandra

From:
Sent: January-26-12 9:03 PM
To:
Subject: CCRIC CF12-001 Collectif d'hacktivistes Anonymous – Attaques par déni de service distribué (DSD) en rapport avec le droit d'auteur et la propriété intellectuelle

(English version previously sent)

==========
CCRIC – Bulletin cybernétique CF12-001
Date : 26 janvier 2012
==========

PUBLIC CIBLE
==========
Ce bulletin cybernétique est destiné aux professionnels et aux gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales, ainsi que des industries à infrastructure critique et autres industries connexes.

Titre
====
Collectif d'hacktivistes Anonymous – Attaques par déni de service distribué (DSD) en rapport avec le droit d'auteur et la propriété intellectuelle.

Détails
=====
On a porté à l'attention du CCRIC une série d'attaques coordonnées par déni de service distribué (DSD) contre des cibles internationales, y compris des organisations gouvernementales et des entreprises du divertissement dont les efforts sont axés sur l'adoption de lois protégeant le droit d'auteur aux États-Unis, comme la Stop Online Piracy Act (SOPA) et la Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA), ainsi que de l'Accord commercial relatif à la contrefaçon (ACRC).

Il appert qu'Anonymous, un collectif hétéroclite d'« hacktivistes », a annoncé que des attaques seraient portées en réponse à la fermeture de MegaUpload, un site d'hébergement et de partage de fichiers, et aux projets de loi sur le trafic de matériel protégé par le droit d'auteur et de marchandises contrefaites que s'apprêtent à adopter les États-Unis. Des attaques qu'ont signalé par la suite les médias visaient diverses organisations gouvernementales déjà engagées dans le processus de ratification de l'ACRC, à savoir les gouvernements d'Irlande et de Pologne.

Deux formes d'attaques DSD sont connues :

De l'information diffusée récemment laisse entendre que des hacktivistes surveillent de près la position du Canada. Le gouvernement fédéral souhaite en effet amender la Loi sur le droit d'auteur avec son projet de loi C-11, la Loi sur la modernisation du droit d'auteur, encore à l'étude au Parlement.

Page 1814

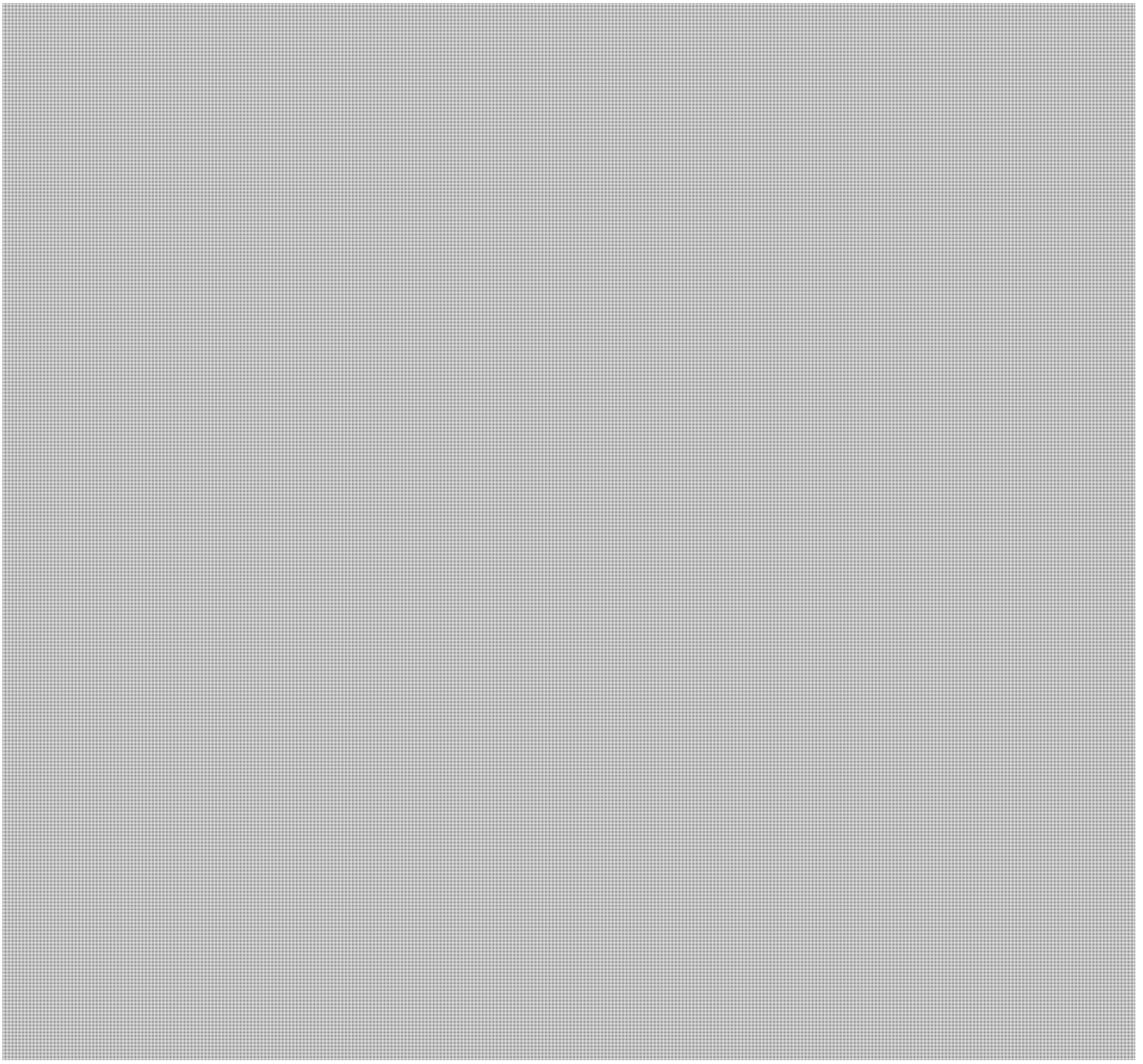
is withheld pursuant to section

est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information



Atténuation
==========
Le CCRIC presse les organisations gouvernementales et les entreprises, qui participent de près à la modification de la Loi sur le droit d'auteur et dont les principales activités sont axées sur le matériel qu'elle protège, d'évaluer les risques d'être exposées à des attaques DSD, telles que les décrit le présent document, et de mettre en place les statégies d'atténuation nécessaires pour y faire face.

Différentes stratégies d'atténuation permettent de contrer ces attaques en fonction de leur type et de l'infrastructure de réseau ciblée. En règle générale, la meilleure défense consiste à s'y préparer à l'avance, ce que permet de faire la liste de contrôle suivante :

Préparation
****

1. Identifier les ressources matérielles les plus cruciales et les services dont elles assurent la prestation.
    - Les derniers correctifs ont-ils été installés?
    - Exécutent-elles des services inutiles comme Telnet, FTP, etc.?

2. De concert avec le fournisseur d'accès Internet (FAI), établir des procédures pour connaître l'étendue du soutien qu'il peut apporter à l'organisation lorsqu'elle fait l'objet d'une attaque DSD. Savoir s'il existe un accord sur les niveaux de services (ANS) et connaître les coûts à assumer.

3. Dresser la liste des personnes-ressources du FAI que l'on peut joindre en tout temps, ainsi que des autres moyens de communiquer avec elles.

4. Bloquer tout trafic qui présente des signes évidents d'usurpation d'identité (p. ex., les adresses IP à l'intérieur du réseau de l'organisation qui ne devraient pas être associées à du trafic entrant ou sortant). Instaurer une liste de filtrage Bogon (plage d'adresses non allouées) au périmètre du réseau.

5. Établir des procédures sur la façon de cloisonner les réseaux de l'organisation en cas d'attaque DSD. Se servir des appareils existants, comme les routeurs et les commutateurs gérés, pour s'en protéger. Dans la mesure du possible, configurer les routeurs du périmètre pour filtrer les services afin de réduire la chargeimposée aux dispositifs de sécurité, tels les pare-feu, qui analysent le trafic.

6. Désactiver tout service inutile et bloquer tout accès non autorisé vers et depuis les hôtes critiques identifiés précédemment.

7. Créer une liste blanche des adresses IP source s'il est nécessaire d'établir un trafic proritaire durant une attaque.

8. Documenter la topologie de réseau, y compris toutes les adresses IP. Tenir cette information à jour.

9. Passer en revue plan de continuité des opérations (PCO) de l'organisation et s'assurer que la haute direction et le service du contentieux comprennent bien ce qu'est une attaque DSD et les rôles et responsabilités qui leur sont dévolus.

10. Comprendre ce que constituent des conditions normales. Établir le niveau de référence du trafic sur le réseau, de la charge de travail imposée aux processeurs, de l'utilsiation des connexions et de la mémoire des hôtes essentiels en situation normale afin que les outils de surveillance du réseau entrent en œuvre lorsqu'une variation anormale se produit.

11. Reconnaître que l'organisation peut être attaquée. Solliciter la direction afin d'obtenir son approbation en vue d'élaborer et de mettre en œuvre des politiques, plans et procédures pour se défendre contre les attaques DSD. Identifier et obtenir les ressources nécessaires pour mettre en œuvre ces politiques, plans et procédures.

12. Attribuer les rôles et responsabilités. Connaître les intervenants dans la défense contre les attaques DSD et s'assurer qu'ils sont au fait de cette responsabilité. Ces personnes devraient appartenir au personnel affecté aux fonctions opérationnelles essentielles, aux opérations de TI, à la sécurité des réseaux et des TI, au service du contentieux et aux relations publiques. Tenir à jour la liste des points de contacts primaires et secondaires. Le réseau étant susceptible d'être en panne, y compris les appareils mobiles, mettre également en place d'autres mécanismes de communication.

13. Effectuer des exercices. Ce n'et plus le temps de faire l'essai des plans et des procédures lorsqu'une attaque se produit.

Identification
****

1. Savoir si l'orgaisation est une victime ciblée ou accidentelle.

2. Comprendre le déroulement logique de l'attaque.

3. Déterminer le trafic dont se sert l'attaquant en identifiant les adresses IP, les ports et les protocoles qu'il exploite.

4. Envisager de recourir à des outils d'analyse du réseau pour déterminer le type de trafic qu'exploite l'attaquant (p. ex., TcpDump, Wireshark, Snort)

5. Consulter les journaux disponibles du serveur pour comprendre la fonctionnement de l'attaque et les cibles visées.

6. Aviser le personnel concerné, notamment celui de la haute direction et du service du contentieux.

Confinement
****
1. Communiquer avec le FAI pour mettre en place un mécanisme de filtrage du trafic.

2. Bloquer le trafic le plus près possible du réseau en nuage (p. ex., avec un routeur, un pare-feu, un équilibreur de charges).

3. Changer l'adresse IP de l'hôte ciblé par l'attaque. Il s'agit là d'une solution provisoire.

4. Si l'attaque vise une application en particulier, envisager sa désactivation.

5. Identifier et corriger la vulnérabilité ou la faiblesse du système qui est exploitée. Il peut s'agir par exemple d'un service inutilisé maintenu involontairement en activité sur un dispositif destiné au public ou d'un système d'exploitation dont les correctifs n'ont pas été installés.

6. Mettre en place un mécanisme de filtrage en fonction des caractéritiques de l'attaque, par exemple le bocage des paquets IMCP Echo.

7. Limiter le trafic de certains protocoles à un nombre quelconque de paquets par seconde ou en n'autorisant l'accès des paquets qu'à certains hôtes.

Reprise des services
****
1. Confirmer que l'attaque DSD a pris fin et que les services sont de nouveau disponibles.

2. Confirmer que le niveau de performance de référence des réseaux est rétabli.

3. Au besoin, installer les correctifs et les mises à jour sur les machines touchées.

4. Dansla mesure du possible, identifier l'origine de l'attaque. Solliciter l'aide du FAI.

5. Passer en revue les registres de journalisation pour y repérer la trace des tentatives de reconnaissance. Conserver ces registres en vue d'éventuelles poursuites judiciaires.

Leçons retenues
****
Rédiger ou mettre à jour les documents suivants :

- Procédures d'opération normalisées
- Procédures d'opération d'urgence
- Plans de continuité des opérations

Consultez les références ci-dessous pour en apprendre davantage sur les activités du collectif Anonymous, l'outil LOIC servant aux attaques DSD, le projet de loi C-11 et le déni de service distribué.

Références :
http://www.us-cert.gov/current/index.html#anonymous_activities (en anglais) http://www.us-cert.gov/cas/tips/ST04-015.html (en anglais) http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html (en anglais) http://isc.incidents.org/diary/Javascript+DDoS+Tool+Analysis/12442 (en anglais) http://nakedsecurity.sophos.com/2012/01/20/anonymous-opmegaupload-ddos-attack/ (en anglais) http://www.channelregister.co.uk/2012/01/24/anon_attacks_poland_over_acta/ (en anglais) http://www.reuters.com/article/2012/01/25/ireland-web-attack-idUSL5E8CP1VU20120125 (en anglais) http://www.reuters.com/article/2012/01/23/idUS426379616120120123 (en anglais) http://www.michaelgeist.ca/ (en anglais) http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/acta-acrc.aspx?lang=fra&view=d (en français) http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5144516&file=4 (contenu bilingue)

Note cruciale :

Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à avertir le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique, notamment l'exploration, le téléchargement, le balayage, ou même une recherche Web selon tout texte du présent rapport.

Signalement
=========
AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Le présent message et toutes les pièces jointes qui l'accompagnent contiennent des renseignements qui peuvent avoir été recueillis de diverses sources externes dont le CCRIC ne peut vérifier ni la fiabilité ni l'intégrité. Le CCRIC n'assume aucune responsabilité pour des conséquences négatives résultant de l'utilisation des renseignements fournis dans la présente.

Les liens vers d'autres sites Web ne relevant pas du gouvernement du Canada sont fournis aux utilisateurs uniquement pour des raisons de commodité. Le gouvernement du Canada n'assume donc pas la responsabilité de l'exactitude, du caractère actuel ni de la fiabilité de leur contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites et leur contenu.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Centre des opérations du gouvernement/
Government Operations Centre
Courriel/email:

s.16(2)(c)

Williston, Sandra

From:
Sent: January-26-12 2:17 PM
To:
Subject: CCIRC CYBER FLASH CF12-001: Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property

(La version française suivra)

==========
CCIRC - Cyber Flash CF12-001
Date: 26 January 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property

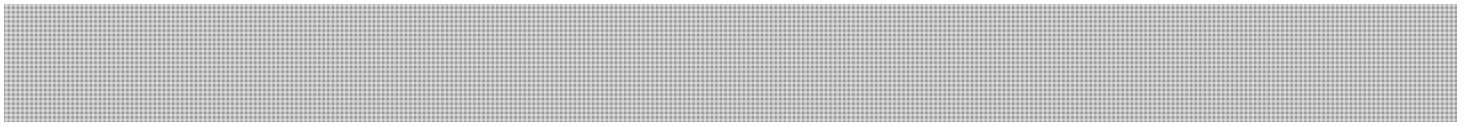
Detail
======
CCIRC has received information about coordinated distributed denial-of-service (DDoS) attacks with multiple international targets including government and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA).

The loosely affiliated collective hacktivist group "Anonymous" allegedly promoted attacks in response to the shutdown of the file hosting site MegaUpload and in protest of proposed U.S. legislation concerning online trafficking of copyrighted intellectual property and counterfeit goods. Follow-on attacks reported in the media targeted various governments organizations involved in the ratification of ACTA, namely the governments of Ireland and Poland.

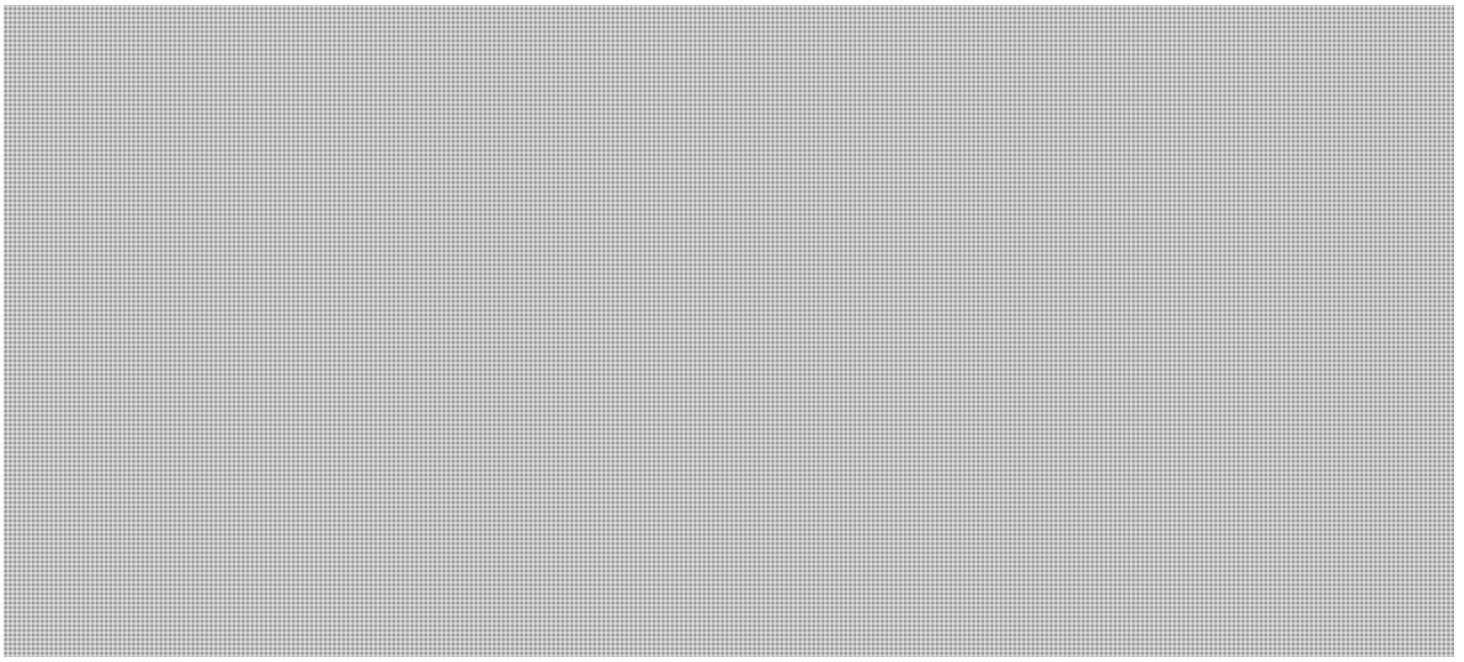
Two types of DDoS attacks were reported:

suggests active monitoring of the Canadian position by the hacktivists. The update to Canada's Copyright Act is currently bill C-11 - Copyright Modernization Act, which is still in parliament.

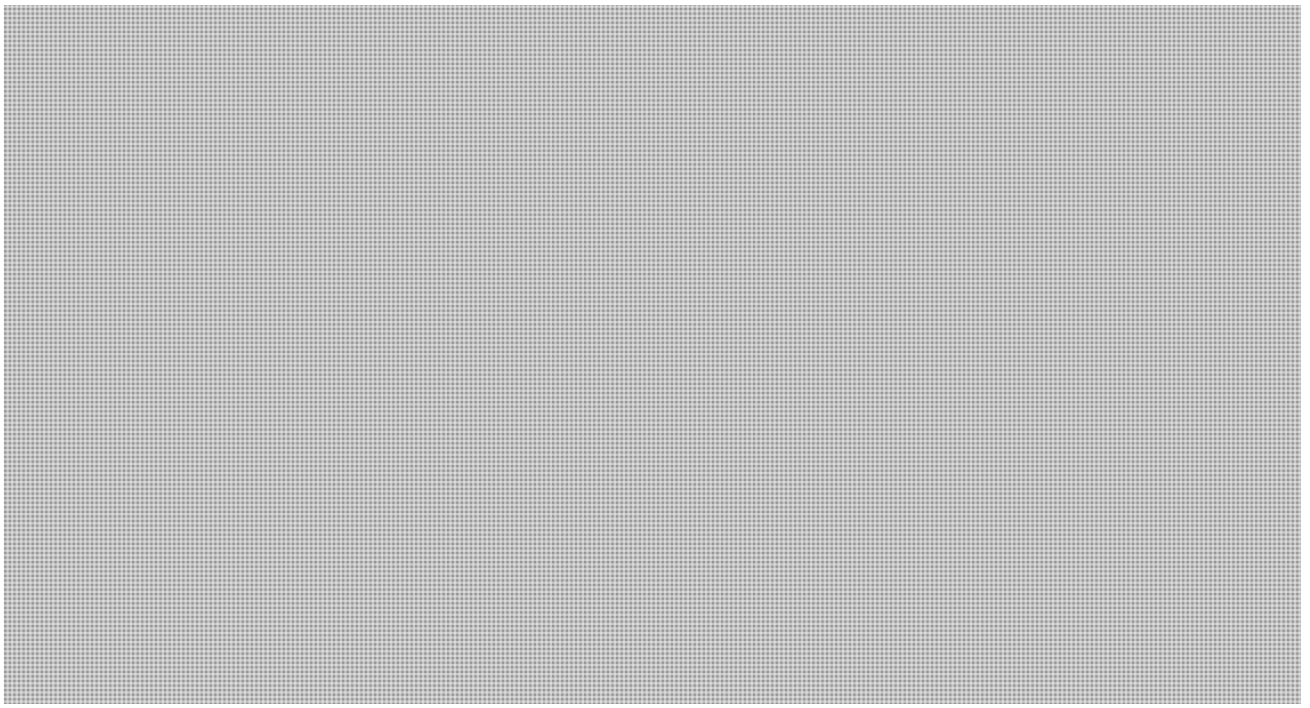
The following is a reported sample of LOIC traffic recorded in a web server log:



The following sites have been identified in HTTP referrer headers of suspected LOIC traffic. This list may not be complete. Please do not visit any of the links as they may still host functioning LOIC or other malicious code.



The following are the A records for the referrer sites as of January, 20, 2012:



Mitigation
==========

s.16(2)(c)

CCIRC encourages government and industry organizations closely involved with the Copyright Law and copy-righted material to assess risk exposure to DDoS attack as described herein and implement mitigation strategies accordingly.

There are a number of mitigation strategies available for dealing with DDoS attacks, depending on the type of attack and the target network infrastructure. In general, the best practice defence for mitigating DDoS attacks involves advanced preparation. The following checklist may be used for this purpose:

Preparation
****

1. Identify your most critical assets and the services they provide.
    - Are they up to date with the latest patches?
    - Do they run any unnecessary services such as Telnet, FTP, etc.?

2. Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.

3. Establish 24/7 contact information for your ISP and alternate methods for communications.

4. Deny all obviously spoofed traffic (e.g., internal IP addresses that should not be coming in or going out of your network). Implement a bogon block list (unallocated address space) at the network boundary.

5. Establish procedures on how to segregate your networks in the event of a DDoS attack. Use existing network devices, such as routers and managed switches, to defend against DDoS attacks. Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls.

6. Disable all unnecessary services and restrict all unauthorized access to and from all previously identified critical hosts.

7. Create a whitelist of the source IPs you must allow if you need to prioritize traffic during an attack.

8. Document your network topology including all IP addresses. Keep it up to date.

9. Review your Business Continuity Plan (BCP) and ensure senior management and legal team understand the significance of a DDoS attack, including their roles.

10. Understand "normal." Establish a baseline of network traffic, CPU usage, connection and memory utilization of critical hosts under normal conditions so that network monitoring tools will trigger on abnormal changes.

11. Acknowledge that your organization may be attacked. Seek and obtain management's approval for the development and implementation of policies, plans and procedures to defend against DDoS attacks. Identify and obtain resources to implement these plans.

12. Assign responsibility. Identify who plays a role in defending against a DDoS attack and ensure they are aware of this responsibility. This should include personnel from critical business functions, IT operations, network and IT security teams, legal advisors, and media relations staff. Ensure an up-to-date point-of-contact list with primary and alternate personnel is maintained. As the network may be unavailable, including mobile devices, ensure alternate communications mechanisms are in place.

13. Conduct exercises. The worst time to test plans and procedures is during an attack.

Identification
****

1. Determine if you are the target or a collateral victim.

2. Understand the logical flow of the attack.

3. Determine what type of traffic is being used, such as IP addresses, ports and protocols.

4. Consider using network analysis tools to determine the type of traffic being used in the attack (e.g., TcpDump, Wireshark, Snort)

5. Review any available logs to understand the attack and what is being targeted.

6. Notify appropriate personnel. This may include senior management and the legal team.

Containment
****

1. Contact your ISP provider to implement filtering.

2. Block the traffic as close to the network cloud as possible (e.g., router, firewall, load balancer)

3. Relocate the target to another IP address if a particular host is being targeted. This is a temporary solution.

4. If a particular application is being targeted, consider disabling it temporarily.

5. Identify and correct the vulnerability or weakness that is being exploited. An example of this may be an unused service that is accidently left enabled on a public-facing device or unpatched operating system.

6. Implement filtering based on the characteristics of the attack. An example may be blocking IMCP echo packets.

7. Implement rate limiting for certain protocols, allowing a certain number of packets per second for a specific protocol or to access a certain host.

Recovery
****
1. Confirm that the DDoS attack has finished and services are reachable again.

2. Confirm that your networks are back to your baseline performance.

3. If necessary, patch and update all affected machines.

4. If possible, identify the source of the attack. Enlist the help of your ISP.

5. Review logs for signs of reconnaissance. Maintain logs for possible future law enforcement requirements.

Lessons Learned
****
Create or update the following documents:

- Standard Operating Procedures
- Emergency Operating Procedures
- Business Continuity Plans

Please consult the references below for additional information on Anonymous activities, the DDoS tool LOIC, Bill C-11 and DDoS in general.

References:
http://www.us-cert.gov/current/index.html#anonymous_activities
http://www.us-cert.gov/cas/tips/ST04-015.html
http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html
http://isc.incidents.org/diary/Javascript+DDoS+Tool+Analysis/12442
http://nakedsecurity.sophos.com/2012/01/20/anonymous-opmegaupload-ddos-attack/
http://www.channelregister.co.uk/2012/01/24/anon_attacks_poland_over_acta/
http://www.reuters.com/article/2012/01/25/ireland-web-attack-idUSL5E8CP1VU20120125
http://www.reuters.com/article/2012/01/23/idUS426379616120120123
http://www.michaelgeist.ca/
http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/acta-acrc.aspx?lang=eng&view=d
http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5144516&file=4

Critical Note:

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities

outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

Reporting

NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel:

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-26-12 8:31 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 26, 2012/ le 26 janvier 2012

Print Media

Software phone scam hooking Canadians
A scam where callers pretend to be Microsoft employees offering to solve computer problems now accounts for 70 per cent of all fraud complaints in Canada, reports the Canadian Anti-Fraud Centre. The fraud artists claim they are with Microsoft and offer to help people rid their computers of malicious software. Daily Gleaner, D1

Online Media

DHS disputes memo on purported railway computer breach
The Department of Homeland Security is disputing a government memo obtained by Nextgov.com that said a targeted attack on the computer network of a railway company in the Northwest disrupted train service in early December. CNET

Senators back Obama's call for cybersecurity reform
Senate Homeland Security Committee Chairman Joe Lieberman (I-Conn.) echoed President Obama's call in the State of the Union for Congress to pass comprehensive cybersecurity legislation on Tuesday evening. "The President's call for Congress to pass cybersecurity legislation underscores the pressing nature of securing the government's cyber systems

and networks — and a limited number of private sector networks that touch the lives of all Americans," Lieberman said. The Hill

Hackers attack Irish govt over new web law
Hackers attacked the websites of Ireland's departments of finance and justice on Wednesday in a protest against government plans to block websites that violate copyright laws. Officials said both websites were taken offline for a short time in the early hours of Wednesday in a denial of service attack, in which the sites were bombarded with a huge number of requests. Reuters

Understanding the threat
Many companies today make the mistake of viewing the advanced persistent threat (APT) type of attack as a single incident consisting of exploit, infection and remediation stages. However, APT attacks are now co-ordinated efforts to establish a foothold for the purposes of cyber crime, cyber espionage or emerging cyber warfare scenarios. CRN

56% of Brits don't check if public Wi-Fi is encrypted before logging on
More than half (56 percent) of Brits that use public Wi-Fi rarely check if it is encrypted before logging on, says UK2. Research conducted by the web hosting firm in conjunction with YouGov revealed more than two thirds (67 percent) did not know what VPN or Virtual Private Network means. However, 86 percent said they ensure their home Wi-Fi network is secure, indicating there is a discrepancy between ensuring safety when surfing the web from home and when on-the-go. PC Advisor

Sourcefire Uses Big Data Analytics To Stop Malware
Cyber security vendor Sourcefire's latest product uses big data analytics methods to search data to discover patterns in malware attacks and intervene to stop them. The release of FireAMP comes the same week that Cisco Systems released its 4Q11 Global Threat Report detailing how pervasive the malware threat is to organizations. Network Computing

Feds Issue Comprehensive Cloud Security Guidance
There's no silver bullet to ensuring security in the public cloud, but organizations need to take the reins and not leave security up to service providers and service arrangements, the National Institute of Standards and Technology (NIST) said in comprehensive new cloud security guidance. Information Week

ISF: consider a cyber resiliency response to protect against 'unknown unknowns'
Cyber resilience is a matter for the whole business to be involved with and not just the security team. At a presentation this week, Michael de Crespigny, CEO of the Information Security Forum (ISF), said that cyber security is not an information security issue, but a business issue. SC Magazine UK

Davos 2012: Alarming growth in cyber-attacks
Ian Powell, UK chairman and senior partner of PwC, said that the danger of cyber-attacks was little understood by many people at the top of business. "The alarming growth in cyber crime highlights the challenge that all global business leaders face. Although they might be aware of the threat they are not necessarily equipped to respond effectively," he told delegates at Davos. "After all, cyber [crime] is a global risk that knows no boundaries." The Telegraph

Microsoft researchers find new type of stealth malware
Security researchers have uncovered a new type of malware that appears to be benign as it is downloaded, potentially fooling security software, but which morphs into malicious software once it is on a user's computer. Researchers at Microsoft's Malware Protection Centre wrote about their findings this week, explaining that the code is surprising in that unlike most other similar types of malware, it doesn't attempt to download or inject an executable file into a host machine. Computing UK

Build Up Your Phone's Defenses Against Hackers
Chuck Bokath would be terrifying if he were not such a nice guy. A jovial senior engineer at the Georgia Tech Research Institute in Atlanta, Mr. Bokath can hack into your cellphone just by dialing the number. He can remotely listen to your calls, read your text messages, snap pictures with your phone's camera and track your movements around town — not to mention access the password to your online bank account. New York Times

Accused Kelihos botmaster's former employer 'angered' at revelation
A security-related company that until late December employed the Russian developer who allegedly created the Kelihos botnet said today it was "extremely disappointed and angered" at the revelation. Returnil, which sells the Virtual System Pro program, confirmed Wednesday that Andrey Sabelnikov had worked in its St. Petersburg office until Dec. 21, 2011. Network World

Apple malware became more sophisticated in 2011
Malware aimed at Macs is still insignificant compared to Windows but Apple users should to pay careful attention to the growing threat from social engineering attacks, a report has found. The Year in Mac Security by Apple security company Intego divides 2011 into two halves before and after the day, 2 May, when the fake antivirus scam Mac Defender was discovered. Tech World

Gingrich on international cyber espionage
Newt Gingrich, the current leader in the race for the Republican Party's nomination for US presidential candidate, has shared his thoughts on the matter of international cyber-espionage. In a December 9th interview with Coffee and Markets, Gingrich expressed his concern about hacking attacks, suggesting that "state-based covert activities" be treated with the same level of severity as acts of war and, further, that "we have to respond to that and create a level of pain which teaches people not to do it." Washington Post

Chinese Hackers Blamed For US Satellite Attack
A forthcoming report from a US Congressional commission reportedly blames cyber attackers for interfering with two government satellites several times over a two-year period. The intrusions on the satellite occurred four times in 2007 and 2008, according to a draft of a report from the US-China Economic and Security Review Commission obtained by Bloomberg BusinessWeek on 27 October. Tech Week Europe

Threatened by Anonymous, Symantec tells users to pull pcAnywhere's plug
Symantec this week took the highly unusual step of telling users of its pcAnywhere remote access software to disable or uninstall the software while it fixes an unknown number of bugs. Security experts said the move was unprecedented for a company of Symantec's size. Computerworld

Hackers launch fresh attacks on Israeli websites
Arab hackers claimed responsibility Wednesday for a series of attacks on prominent Israeli websites, including that of daily newspaper Haaretz. Cyber attacks against Israeli sites have been increasing since the start of the month, many of them claimed by Arab hackers. AFP

Israeli Hacker Steals 85,000 Arabs' Facebook Logins
An Israeli hacker calling himself Hannibal stole and exposed the Facebook login credentials of 85,000 Arabs earlier this week. It's the latest retaliatory strike in a politically motivated battle between Israeli and Arab hackers that's been going strong since the beginning of the month. MSNBC

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From: [redacted] **s.16(2)(c)**
Sent: January-26-12 9:59 AM
To: Alain.Labossiere@ic.gc.ca
Cc: CYBERDO
Subject: RE: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

Hi Alain,

CCIRC will be releasing the Cyber Flash today.

Thanks,

Gregg Murphy
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-3579 Facsimile | Télécopieur +1 613-991-3574 gregg.murphy@ps-sp.gc.ca www.publicsafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Alain.Labossiere@ic.gc.ca [mailto:Alain.Labossiere@ic.gc.ca]
Sent: January-25-12 11:21 AM
To: [redacted]
Subject: RE: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

I cans end it to the CTCP folks, now or wait for your cyberflash?
(I want to follow protocol of course)

al

-----Original Message-----
From: [redacted] mailto: [redacted]
Sent: Wednesday, January 25, 2012 9:32 AM
To: Labossière, Alain: [redacted]
Subject: FW: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

---

From: Beaudoin, Luc S
Sent: Wednesday, January 25, 2012 9:31:51 AM (UTC-05:00) Eastern Time (US & Canada)
To: [redacted]
Subject: RE: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

OK.....could you do a cut-paste into a Cyber Flash ? (first this year) I think we need to do this.... Thoughts ? ETC ?

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----
From: [redacted]
Sent: January-25-12 9:17 AM
To: Beaudoin, Luc S; Bendelier, Kenneth; Cameron, Bud; Clow, Patrick; Melanson, Daryl; Moore, Bruce; Murphy, Gregg; Phlek, Vireak; Turbide, Frank; Williston, Sandra
Subject: FW: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

FYI

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill - it's a decision"

[redacted]

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-28-12 9:09 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne - First Part / Première partie

Daily Media Summary / Revue de presse quotidienne
First Part / Première partie
January 28, 2012 / le 28 janvier 2012

MINISTER / MINISTRE

Fredricton's gun registry extends to Nerf toys
The looming end to the federal long-gun registry will soon leave Fredericton in a unique position: the only major Canadian city with a municipal gun registry. Except that its registry covers anything that shoots a projectile by means of compressed air, spring or mechanical means. That covers pellet and paintball guns and, in theory, even such toys as Nerf guns. Since 2005, Fredericton has maintained Canada's only mandatory registry regime for such items, complete with fees, fines, databases and, in one instance, a SWAT team raid on a home. But it could also represent the wave of the future, as **Public Safety Minister Vic Toews** says municipalities have full freedom to implement registries of their own - whether for real guns or fake ones. The Guardian, A7 (Vancouver Sun, Calgary Herald, Edmonton Journal, Telegraph-Journal, Times & Transcript, Montreal Gazette, Leader-Post, Ottawa Citizen)

Province ranks highest for fear of crime
Canadians are more likely to believe crime is going down now than they were a year ago, a new poll reveals. Except if they live in Manitoba. While fewer than half of Canadians believe crime is getting worse, more than two-thirds of Manitobans believe it is. That is by far the highest number of any province. Manitoba is also the only province to show a significant increase in the number of people who think crime is getting worse. Almost every other province showed a decrease in that number . . . **Public Safety Minister Vic Toews** said the Environics survey results are consistent with the Harper government's crime strategy. ***"I'm glad that people are beginning to feel safer. That's exactly what we want to see. But that doesn't mean that we should in any way take our foot off the gas. It's a lot like saying to a patient who's been taking a course of medicine that, 'Gee, you're feeling better now. Get off the medicine.' You keep on with the medicine until the problem is in fact cured."*** Winnipeg Free Press, A4

'Scourge' takes its toll
RCMP are trying to tackle what they call a "disturbing trend" surrounding elaborate marijuana grow operations in Manitoba, after last year seizing enough pot plants to almost cover a football field . . . Federal Public Safety Minister Vic Toews said the ***"scourge of drugs"*** takes a ***"huge toll ... on our families."*** Winnipeg Sun, 4; Winnipeg Free Press

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Seniors may be prone to new swine flu virus
There may be a lot more vulnerability in the population to a new swine influenza virus than was first thought, new Canadian research suggests. It has been believed that while children and teens are probably vulnerable to the new H3N2 variant, people over the age of 20 or so would have antibodies that would either block infection or protect against severe disease caused by the viruses. Hamilton Spectator, G8; Toronto Star

1663: séismes terrifiants
Un article d'opinion déclare, «...On se souvient par ailleurs de la catastrophe nucléaire survenue l'an dernier au Japon à la suite du tremblement de terre. Tous les pays civilisés ont remis en cause l'utilisation de l'énergie nucléaire suite à cette catastrophe. Enfin presque tous. Il reste au Québec et au Canada quelques irréductibles promoteurs de dangers publics... » Le Nouvelliste, 19

Green groups warn of deepwater drilling risks

Environmental groups are sounding the alarm that a new round of deepwater drilling off the coast of Nova Scotia could end in another natural disaster such as the Gulf Coast spill of 2010. The Ecology Action Centre and the Sierra Club are urging regulatory bodies to proceed with extreme caution and toughen up regulations before allowing drilling to go ahead. Chronicle-Herald, A1

Flood is not over, nor is the fight
An opinion piece states, "One senses that a general malaise has set in about the Lake Manitoba flood, that it is over and that the construction of the emergency channel has solved the problem. But it is far from over and the construction of the emergency channel has not solved the problem. It is only the beginning of a solution to the problem..." Winnipeg Free Press, J11

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Tories to Hamas: Stay home
Two federal ministers have put up a "not welcome" sign for members of Hamas, a banned terrorist group in Canada, who might attend an International Parliamentary Union (IPU) meeting in Quebec City. QMI Agency has obtained a letter that Foreign Affairs Minister John Baird and Immigration Minister Jason Kenney have sent to the speakers of the House of Commons and the Senate. Toronto Sun, 12

Spying on our own : secret files revealed
Canadian security forces kept close tabs on renowned constitutional scholar Eugene Forsey from his early days as a left-wing academic to his stint as a senator, according to newly declassified documents . . . The secret files kept on Forsey by the RCMP Security Service - the predecessor to the Canadian Security Intelligence Service (CSIS) - are public for the first time after the Star obtained them through an access-to-information request to Library and Archives Canada. Toronto Star, IN5

Naval centre one of 'Five Eyes' on the world
As you approach the Royal Canadian Navy's secretive Trinity intelligence centre near the Halifax Harbour, at least nine surveillance cameras track your movement. Protected behind two chain-link fences, both topped with barbed wire, the main Trinity facility is really a building within a building. A separate interior structure, with metal-clad walls, safeguards its secrets. Globe and Mail, A8

CYBER SECURITY / CYBERSÉCURITÉ

Beaucoup de profit à vous espionner
Tout ce que vous écrivez sur les sites de réseautage social et même en utilisant vos courriels gratuits est utilisé. Big Brother enregistre tout. Demain ou l'un de ces jours, vous risquez de recevoir de la publicité parce que vous aimez les chaussures anglaises ou le chocolat. Ou encore parce que vos amis et vos relations les aiment. Comment estce possible? Le Journal de Montreal, 50

What to do when hackers strike
If you do any shopping, banking or other business online and it hasn't happened to you yet, it probably will. In the U.S., the online retailer Zappos (which is owned by Amazon), recently sent an email to 24 million of its customers telling them that their personal information might have been compromised in a data breach. Though credit card and payment data were unaffected, the company said names, email addresses, billing and shipping information, phone numbers and other information were at risk. Edmonton Journal, C6

Hacker group targets new websites
The activist hacker group Anonymous attacked three Mexican government websites on Friday in protest at a proposed bill that seeks to toughen local laws about online file-sharing. The affected sites belong to the Interior Ministry, the Senate and the Chamber of Deputies. The homepage of the Interior Ministry remained offline by mid-afternoon. Kingston Whig-Standard, 14

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Victims of crime supported

The federal government announced more than $1.6 million in funding to support victims of crime in New Brunswick yesterday. The announcement was made by Robert Goguen, MP for Moncton-Riverview-Dieppe and Parliamentary secretary to Justice Minister Rob Nicholson, and Marie-Claude Blais, minister of justice and attorney general of New Brunswick, on behalf of Robert B. Trevors, minister of public safety and solicitor general of New Brunswick. Times & Transcript, A12

WCB hostage-taker on hunger strike, friend says
Patrick Clayton, the man convicted of taking nine hostages at the Workers' Compensation Board building in Edmonton in October 2009, is apparently on a hunger strike at the Drumheller Institution. Clayton, 40, has been held at the prison since late November, after he was sentenced to 11 years. Edmonton Journal, A4

La mort de Moïse Thériault vécue comme une «délivrance»
A travers douleur et déchirement, Gabrielle Lavallée a accueilli l'assassinat de Roch Moïse Thériault comme une «délivrance». Reste qu'elle s'interroge sur les circonstances de la mort de celui qui lui a infligé un calvaire, mettant de l'avant la thèse de la préméditation . . . «Moïse» Thériault, qui avait fait de Gabrielle Lavallée une de ses femmes au sein de sa secte, a été assassiné par un voisin de cellule à la prison de Dorchester, au Nouveau-Brunswick, le 26 février dernier. Le Soleil, 26

INTERNATIONAL / INTERNATIONAL

Londres se prépare au pire
A six mois des Jeux, une médaille devrait déjà être décernée aux organisateurs des XXXes Olympiades qui s'ouvriront à Londres le 27 juillet prochain. Les enceintes sportives sont pratiquement terminées et le budget, révisé à 14,6 milliards de dollars en 2007 (le triple de l'estimation initiale), a été respecté. Toutefois deux grands impondérables demeurent : le transport et, surtout, la sécurité des Jeux. A en croire le branle-bas de combat dans la capitale, les Londoniens se préparent au pire. La Presse, A26

The tale of an American militant
MOEED ABDUL Salam didn't descend into radical Islam for lack of other options. He grew up in a well-off Texas household, attended a pricey boarding school and graduated from one of the state's most respected universities. But the most unlikely thing about his recruitment was his family: Two generations had spent years promoting interfaith harmony and combating Muslim stereotypes in their hometown and even on national television. Chronicle-Herald, F4

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-30-12 8:10 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted]; Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 30, 2012 / le 30 janvier 2012

Online Media

Dutch DigiD vulnerable to DDoS attacks – NCSC
The Dutch National Cyber Security Center (NCSC) has warned that the ICT servers of the minister of interior could be vulnerable, with DigiD open to DdoS attacks. Logius is set to upgrade their server environment on 6 February. The Dutch Govcert (Government Computer Emergency Response Team) merged on 1 January with the National Cyber Security Center (NCSC). Telecom Paper

Anonymous : les cyberactivistes vont-ils faire leur coming-out en France ?
Comment qualifier Anonymous ? Exercice difficile. Les contours sont flous. « Ce n'est pas un mouvement de pirates. Pas non plus du hacking d'amateurs (terme qu'ils refusent) », considère Jean-Philippe Bichard, journaliste, expert en sécurité IT (ex-Kaspersky) et animateur du blogAttypique.com. « Anonymous appartient au 5% de cyber-attaquants que l'on peut qualifier « d'idéologique » par opposition au 95% de cyber hacker qui recherchent l'appât du gain. » Globalement, la communauté Anonymous considère qu'il ne faut pas attaquer les sites médias et les réseaux sociaux (Facebook, Twitter…). Mais vaut mieux se méfier de ses amis… IT Espresso

A new initiative to tackle cyber threats launched at WEF

Davos: A new initiative on cyber security has been launched at the World Economic Forum to strengthen efforts to combat rising cyber risks. The initiative 'Partnering for Cyber Resilience' is a set of shared principles, endorsed by chief executives of firms that recognise interdependence of organisations in tackling cyber risks, according to a statement from the WEF. The new programme would engage the corporate firms into working towards a safer digital environment. IBN Live (India)

La Freebox victime d'un cheval de Troie
Les utilisateurs de Freebox sont la cible d'un virus malveillant dont on ignore pour l'instant comment il réussit à pénétrer les systèmes de protection. Prudence ! La firme Trusteer, spécialisée en sécurité informatique a prévenu les utilisateurs de Freebox contre le cheval de Troie (trojan) Carberp, capable de subtiliser des coordonnées bancaires. Le malware a recours à la méthode via la méthode transparente du "man in the browser". MaxiSciences

Cybersecurity efforts trigger privacy concerns
The federal government's plan to expand computer security protections into critical parts of private industry is raising concerns that the move will threaten Americans' civil liberties. In a report for release Friday, The Constitution Project warns that as the Obama administration partners more with the energy, financial, communications and health care industries to monitor and protect networks, sensitive personal information of people who work for or communicate with those companies could be improperly or inadvertently disclosed. While the government may have good intentions, it "runs the risk of establishing a program akin to wiretapping all network users' communications," the nonpartisan legal think tank says. The Associated Press obtained a copy of the report in advance. Associated Press (link to KVAL)

Call for cyberwar 'peacekeepers' force
The US Army's Cyber Command is recruiting. Its mission? To create "a world class cyberwarrior force", and to develop cyberspace as an "active domain". That's according to Lieutenant General Rhett Hernandez, Arcyber commander, speaking at a London conference on cyber defence this week. He spoke of the explosive complexity of living in a digital age, and a cyber threat that was "growing, evolving and sophisticated". BBC News

Des mises à jour dangereuses sur Androïd...
Un virus de type cheval de Troie identifié par Bitdefender sous le nom d'Android.Trojan.FakeUpdates.A s'attaque aux systèmes Android via des versions alternatives de la plate-forme de téléchargement Android Market... Ce virus, caché dans une application validée comme saine, s'installe sur le système du GSM de la personne qui a téléchargé ce programme. Lors de l'installation, une dizaines d'autorisations sont demandées et les utilisateurs les moins attentifs ouvrent la sécurité de leurs appareils sans se rendre compte du danger. Cette méthode de piratage n'est pas nouvelle mais semble être de plus en plus fréquente. Next51.net

Android.Counterclank Found in Official Android Market
Symantec has identified multiple publisher IDs on the Android Market that are being used to push out Android.Counterclank. This is a minor modification of Android.Tonclank, a bot-like threat that can receive commands to carry out certain actions, as well as steal information from the device. For each of these malicious applications, the malicious code has been grafted on to the main application in a package called “apperhand”. When the package is executed, a service with the same name may be seen running on a compromised device. Another sign of an infection is the presence of the Search icon above on the home screen. The combined download figures of all the malicious apps indicate that Android.Counterclank has the highest distribution of any malware identified so far this year. Symantec.com

Chinese Hackers Led Western Attacks, Symantec Charges
Researchers with Symantec have uncovered additional clues that point to Chinese hacker involvement in attacks against a large number of Western companies, including major U.S. defense contractors. The attacks use malicious PDF documents that exploit an Adobe Reader bug patched last month to infect Windows PCs with "Sykipot," a general-purpose backdoor Trojan horse. According to findings published Thursday by Symantec's research team, a "staging server" used by the attackers is based in the Beijing area, and is hosted by one of the country's largest Internet service providers, or ISPs. Symantec did not identify the ISP. PC World

Accused Kelihos botnet controller protests his innocence
A Russian programmer accused by Microsoft of being behind the Kelihos botnet has protested his innocence. Last week, Microsoft accused Andrey Sabelnikov of being responsible for the operations of the Kelihos botnet, saying that he had written the code for, and either created or participated in creating, the malware; it also claimed that he registered more than 3,700 'cz.cc' sub-domains, which were used to control and operate the botnet. It was also revealed that Sabelnikov had worked as a software engineer and project manager at Russian anti-virus firm Agnitum, a provider of firewalls, anti-virus and security software. Sabelnikov said that upon arriving in the US on 21 January, he learned from the press that he was accused of a felony in connection with the activities of a botnet. In a statement, Sabelnikov said: “I am a programmer with nine years' experience, graduated from St. Petersburg State University of Aerospace Instrumentation in 2003, [and

have worked] in the highly respected Russian and international IT companies. "I did not commit this crime, have never participated in the management of botnets or any other similar programs, and especially not extracted from it any benefit." SC Magazine

Android malware makes use of steganography

Security firm F-Secure have released details on how Android malware makes use of steganography to hide the control parameters for rogue code. First, what is steganography? It's the technique of hiding messages within something else, in this case, an icon file. F-Secure first suspected that Android malware was making use of steganography when researchers came across this line of code:

```
localObject2 = ((ByteArrayOutputStream)localObject2).toByteArray();
int k = paramInt + (-4 + new String(localObject2).indexOf("tEXt"));
if (k < 0)
  throw new IOException("Chank tEXt not found in png");
```

ZDNet

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
16 Jan 2012	Educational	2573	XSSed Notification – cross-site scripting vulnerability at a university website	one	University website	
26 Jan	Govt	2595	Websites vulnerable to exploits listed in Pastebin	Unknown	[redacted] notified CTEC, CERT Australia & DoD Australia	
23 Jan 2012	Other	2588	Website defacement	1	Ottawa dentist Sent notification to domain technical contact & hosting provider	
17 Jan	Various, includes health and maybe govt	2577	Website compromises – username, password posted online (pastebin)	5	[redacted] (A forum for public-private sector discussions on how to manage the environmentally in an ethically, scientifically and financially sound way); [redacted] co (sells wholesale vitamins and food supplements); soccer league and 2 AA level hockey leagues CCIRC notified the orgs	s.16(2)(c) s.20(1)(c)
27 Jan	Security – Intl	2597	Cdn University IP attacking Virginia Police website	1	[redacted] IP belongs to a library computer open to all – it's possible that machine was compromised. Workstation is rebuilt at least once a day	
16 Jan	Educational	2574	Malware hosted on a Cdn university website	one	• CCIRC observed that malware was hosted on a [redacted] website • The file "photographer.exe" is detected by McAfee as Adware (Gabpath). This file will in-turn drop a 2nd binary (postalito.jpg.exe) on victim computers (Trojan Dropper). Mon 16/01/2012 10:40 AM A follow-up check confirmed that the malware was removed from the university website and is no longer being served. Moore, Bruce (1/13/2012 1:07 PM): Fri 13/01/2012 11:49 AM Deactivation request sent to the university (RCMP cc'd). The university was advised that their domain was added to the malc0de	

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					blocklist, possibly resulting in decreased legitimate traffic to their website.	
20 Jan	Unsure	2587	Malware hosted on a Cdn IP	Unknown	Files are of the password stealing and backdoor Trojan variety (linked to botnets and stealing banking info) Sent takedown request to network's owner, cc'd LE & CTEC	
23 Jan	Other	2589	Malware hosted on a Cdn IP	1	[redacted] Script redirects user to domain hosted in US – domain registered to clickartists website services from CA but IP address belongs to [redacted]	
17 Jan 2012	Telecom	2576	Malware hosted on a Cdn IP (website hosting service server)	1	[redacted] Sent deactivation request to iweb, cc'd RCMP [redacted] was warned that this domain was added to various block lists, possibly resulting in reduced legitimate traffic to this website.	
20 Jan	Provincial, Energy, Bank, Telecom, Health, Transport, education	2586	DNS Changer malware		The telcos are probably ISPs who have their customers' computer infections showing up on the Shadowserver Drone report	Check for repetition for orgs with other events – maybe ask Luc
16 Jan	Provincial, financial, energy, health and transportation	2575	DNS Changer Malware (Ghostclick) Shadowserver Drone Report	3 provinces, 1 bank, 1 energy co, two health orgs, one transportation	[redacted] again	Check to see if they're the same ones from previous weeks or if they're new cases
18 Jan 2012	Federal, Provincial, Energy, Finance,	2580	DNS Changer Malware	24	[redacted] == sent notification	

s.16(2)(c)
s.20(1)(c)

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
	Health, Transportation, 12 universities					
24 Jan	Multiple	2592	DNS Changer malware	2 provinces, 1 energy co; 15 telecom cos' 1 Transportation; 10 universities	[redacted]	Ask someone in Ops re the eye-chart and the CCIRC-CRTC-CIRA initiative
19 Jan 2012	Financial	2581	Phishing	1	Came in through Phonebusters/anti-fraud centre Hosted in US Report sent to [redacted] Google Phishing Filter Service and APWG	
20 Jan	Financial	2584	Phishing	1	[redacted] Hosted in US Different origin and link than in event #2581 Came from phonebusters/anti-fraud centre	
20 Jan	Financial	2585	Phishing	1	[redacted] Hosted in US	
24 Jan	Govt	None	CRA Phishing		Email offering tax refund prompts user to click on link – site is no longer active as of this writing	Ask editorial board: Is this worth putting in the Weekly? I think so
26 Jan	Financial	2596	Phishing	1	[redacted] hosted in Culver City, California	
27 Jan	Financial	2598	Phishing	1	[redacted] Website hosted in Taiwan Report sent to [redacted] Google Phishing Filter service and APWG	
27 Jan	Financial	2599	Phishing	1	[redacted] Website hosted in Paris, France	

s.16(2)(c)
s.20(1)(c)

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
27 Jan	Financial	2600	Phishing	1	[redacted] Hosted on a server in Case Western Reserve University in Cleveland, Ohio	
27 Jan	Public	12-3440	Phishing e-mail		Spoofing Service Canada, asking people to complete an information form. Domain registration appears dubious. Notified CTEC and recommended notifying SC	
[redacted]					[redacted] **pinfi malware is spyware	Ask Luc or Bruce for more details – not much in the portal
24 Jan	Govt	2593	APT	1?	Targeted e-mail with trojan attachment [redacted] Told CTEC & CSIS	
24 Jan	Govt	2594	FTP credentials of a federal dept posted on the Internet		Got it through the Yahoo phishing campaign? Potential impact: credential theft /unauthorized access	Ask Gregg to explain it a bit more – is this really serious?
27 Jan	Multiple (potential)	2601	Canadian SCADA Ips posted on Pastebin		ICS-CERT alerted CCIRC The Cdn SCADA IPs are public facing Most of the IPs were previously posted on pastebin (CE12-2583). Two new IPs on this event The IPs belong to a health org & a building/property owner --	Confirm with Gregg that these IPs are likely for HVAC systems in buildings
20 Jan 2012	Energy (SCADA)	2583	SCADA IPs were posted on Pastebin –		[redacted]	

s.16(2)(c)
s.20(1)(c)

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
			Pastebin entry suggests they are vulnerable		Rich mansions in the neighbourhood The posting on Pastebin will draw attention to the log-in panel CCIRC Ops mgr thinks it's a poor practice to expose the log-in screen CCIRC Notified the maintainers that operate these sites: [redacted] and [redacted]	
24 Jan 2012	Govt	2590	Operation SACTA (stop anti-counterfeiting Trade Agreement)	1	Encouraging users to email or attack govt sites Sent info to fed govt CERT	

Noteworthy News from the CCIRC Daily Reports or Ops Meeting during the week of 16 Jan 2012: s.16(2)(c) s.20(1)(c)

Tel Aviv Stock exchanged website DDoS'd; not a sophisticated attack (17 Jan 2012) – some info also under Activity 12-3417
Israeli-Palestinian websites were attacked
Bot blackmails Facebook users (Threatwatch 20 Jan 2012)
Some websites going black (on 18 Jan 2012) to protest SOPA
Anonymous downs govt, music industry sites in largest attacks ever – in response to the federal raid on Megaupload (20 Jan 2012) (Note: this includes the US equivalent of getcybersafe.ca)
Click on an Anonymous link, and you could be DDoS'ing the US govt (20 Jan 2012)

Noteworthy News from the CCIRC Daily Reports or Ops Meeting during the week of 23 Jan 2012:

Tax season opens, tax spam follows (Threat Watch from 23 Jan 2012)
CBS is offline and its servers are wiped – by Anonymous (Note: It was actually a DNS poisoning attack; CBS servers were not wiped, but users were directed to another imposter site – CBS managed to regain control)
Cameras may open up the Board Room to Hackers (videoconferencing systems, widely used, if set up outside the firewall of the org can pick up the audio)
Hackers, reportedly associated with Anonymous have been attacking Polish govt websites to protest scheduled signing of ACTA
----Reports suggest Anonymous will attack Facebook on Feb 28
----- Hackers also attacked Irish Govt websites (Op ACTA)
-----European Parliament website taken offline in retaliation of ACTA (website down for almost a day) (27 Jan 2012)
Microsoft researchers find new type of stealth malware that appears to be benign, bypasses AV filters, but morphs into malicious software once it is on a user's computer.
(Note: the point is that you can't keep every malware out – better have a data recovery plan after a cyber attack) (26 Jan 2012)

Symantec warns customers of hacker risk *(advised customers to stop using its pc Anywhere software for accessing remote PCs, saying they're at increased risk of getting hacked. This seems to be the company's most direct acknowledgement to date that a 2006 theft of its source code put customers at risk) (26 Jan 2012: Reuters)*

Products/Alerts Released

- **CCIRC Product:** AV12-003 Oracle Critical Patch Updates – Jan 2012 released to all cyber clients and posted on PS website
- **CCIRC Product:** CF12-001 Hacktivist Group Anonymous – DdoS Activity Related to Coyrights and Intellectual Property – Released to ALL cyber clients (but not posted on departmental website) **ACTION:** *ASK WHY WE DID THIS – THE INTENDED VICTIMS WOULD BE MOSTLY IN GOVT – IS IT BECAUSE CTEC WAS NOT IN A POSITION TO DO THIS?*

- Multiple (7) **ICS-ALERTs** released by the US subsequent to the S4 SCADA conference (researchers sent/gave findings to US CERT)

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
16 Jan 2012	Educational	2573	XSSed Notification – cross-site scripting vulnerability at a university website	one	University website	
	Educational	2574	Malware hosted on university website	one	• CCIRC observed that malware was hosted on a [redacted] website • The file "photographer.exe" is detected by McAfee as Adware (Gabpath). This file will in-turn drop a 2nd binary (postalito.jpg.exe) on victim computers (Trojan Dropper). Mon 16/01/2012 10:40 AM A follow-up check confirmed that the malware was removed from the university website and is no longer being served. Moore, Bruce (1/13/2012 1:07 PM): Fri 13/01/2012 11:49 AM Deactivation request sent to the university (RCMP cc'd). The university was advised that their domain was added to the malc0de blocklist, possibly resulting in decreased legitimate traffic to their website.	
		2575	DNS Changer Malware (Ghostclick) Shadowserver Drone Report	3 provinces, 1 bank, 1 energy co, two health orgs, one transportation	[redacted] again	Check to see if they're the same ones from previous weeks or if they're new cases
17 Jan 2012	Telecom	2576	Malware hosted on website hosting service server	1	[redacted] n Mtl Sent deactivation request to iweb, cc'd RCMP [redacted] was warned that this domain was added to various block lists, possibly resulting in reduced legitimate traffic to this website.	
	Various, includes	2577	Website compromises – username,	5	[redacted] (A forum for	

s.16(2)(c)
s.20(1)(c)

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
	health and maybe govt		password posted online (pastebin)		public-private sector discussions on how to manage the environmentally in an ethically, scientifically and financially sound way); [redacted] co (sells wholesale vitamins and food supplements); soccer league and 2 AA level hockey leagues CCIRC notified the orgs	
18 Jan 2012	Federal, Provincial, Energy, Finance, Health, Transportation, 12 universities	2580	DNS Changer Malware	24	[redacted] == sent notification	s.16(2)(c) s.20(1)(c)
19 Jan 2012	Financial	2581	Phishing	1	Came in through Phonebusters/anti-fraud centre Hosted in US Report sent to [redacted] Google Phishing Filter Service and APWG	
20 Jan 2012	Energy (SCADA)	2583	SCADA IPs were posted on Pastebin – Pastebin entry suggests they are vulnerable		[redacted] Rich mansions in the neighbourhood The posting on Pastebin will draw attention to the log-in panel CCIRC Ops mgr thinks it's a poor practice to expose the log-in screen CCIRC Notified the maintainers that operate these sites: [redacted]	
	Financial	2584	Phishing	1	[redacted] Hosted in US Different origin and link than in event #2581 Came from phonebusters/anti-fraud centre	
	Financial	2585	Phishing	1	[redacted] Hosted in US	

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
	Provincial, Energy, Bank, Telecom, Health, Transport, education	2586	DNS Changer malware		The telcos are probably ISPs who have their customers' computer infections showing up on the Shadowserver Drone report	Check for repetition for orgs with other events – maybe ask Luc
	Unsure	2587	Malware hosted on a Cdn IP	Unknown	Files are of the password stealing and backdoor Trojan variety (linked to botnets and stealing banking info) Sent takedown request to network's owner, cc'd LE & CTEC	

Noteworthy News from the CCIRC Daily Reports or Ops Meeting during the week:
Tel Aviv Stock exchanged website DDoS'd; not a sophisticated attack (17 Jan 2012) – some info also under Activity 12-3417
Some websites going black (on 18 Jan 2012) to protest SOPA
Israeli-Palestinian websites were attacked
Bot blackmails Facebook users (Threatwatch 20 Jan 2012)
Anonymous downs govt, music industry sites in largest attacks ever – in response to the federal raid on Megaupload (20 Jan 2012)
Click on an Anonymous link, and you could be DDoS'ing the US govt (20 Jan 2012)

CCIRC Product: AV12-003 Oracle Critical Patch Updates – Jan 2012 released to all cyber clients and posted on PS website

Williston, Sandra

From: CCIRC Internal Portal - CDO Watch and Operations [redacted]
Sent: January-31-12 4:00 PM
To: Beaudoin, Luc
Subject: Activity Log

CCIRC Internal Portal - CDO Watch and Operations

Activity Log - Daily Summary

Modify my alert settings View Activity Log

Title	Modified	Modified by	
N&T 31 Jan 2012	1/31/2012 7:57 AM	Moore, Bruce	New!

Date/Time: 1/31/2012 8:00 AM

Short Description: N&T 31 Jan 2012

Issue Status: Closed

Detail Description: **s.16(2)(c)** **s.20(1)(b)**

Handler: Moore, Bruce

Updates

CI Sector / Client Group

Context [redacted]

Projects

CF12-XXX Hackivist Group Anonymo...	1/31/2012 8:47 AM	Williston, Sandra	Edited

Short Description [redacted] CF12-001 Hackivist Group Anonymous - DDoS Activty Related to Copyrights and Intellectual Property] - Processing

Detail Description [redacted] Processing for CF12-001

Updates

Williston, Sandra

From: CCIRC Internal Portal - CDO Watch and Operations [redacted]
Sent: January-26-12 4:00 PM
To: Beaudoin, Luc
Subject: Activity Log

s.16(2)(c)

CCIRC Internal Portal - CDO Watch and Operations

Activity Log - Daily Summary

Modify my alert settings View Activity Log

Title	Modified	Modified by	
Research - Scada Leverett report	1/25/2012 6:05 PM	Phlek, Vireak	New!

Date/Time	1/25/2012 6:00 PM
Short Description	Research - Scada Leverett report
Issue Status	Closed
Detail Description	Read the report and try to find some of the mentioned Canadian IP Scada machine facing directly in the internet. Using SHODAN search engine. What is missing is the ability do display more than 50 results and export the data into a file. Those are a paying option. More research to come. I have include the report and the partial result from my queries.
Handler	Phlek, Vireak
Updates	
CI Sector / Client Group	02F SCADA
Context	
Projects	

Research - Scada Leverett report	1/25/2012 6:08 PM	Phlek, Vireak	Edited

Detail Description

Read the report and try to find some of the mentioned Canadian IP(365) Scada machine facing directly in the internet.

Using SHODAN search engine. What is missing is the ability do display more than 50 results and export the data into a file. Those are a paying option.

More research to come. I have include the report and the partial result from my queries.

Updates

Research - Scada Leverett report 1/25/2012 6:10 PM Phlek, Vireak Edited

Updates

Research - Scada Leverett report 1/25/2012 6:15 PM Phlek, Vireak Edited

Updates Niagara Web server receiced the most hits : 725 out of 1211.
Obtain document on Niagara security from the web.

Research - Scada Leverett report 1/25/2012 6:20 PM Phlek, Vireak Edited

Updates

TAC/ Xenta511 is another popular one result in 106 hits for canadian SCADA.
Obtain doc from the cie as well.

N&T 26 Jan 2012 1/26/2012 8:02 AM Moore, Bruce New!

Date/Time 1/26/2012 9:00 AM

Short Description N&T 26 Jan 2012

Issue Status Closed

Detail Description **s.20(1)(b)**

Handler Moore, Bruce

Updates

CI Sector / Client Group

Context

Projects

CF12-XXX ["Anonymous" DDoS Activ... 1/26/2012 9:27 AM Williston, Sandra Edited

Short Description CF12-XXX Hackivist Group Anonymous - DDoS Activty Related to Copyrights and Intellectual Property] - Processing

Updates

DDoS Mitigation Information Repo... 1/26/2012 10:16 AM Murphy, Gregg New!

Date/Time 1/26/2012 11:00 AM

Short Description DDoS Mitigation Information Report

Issue Status Active

Detail Description Publish a DDoS Mitigation Information Report.

Handler Williston, Sandra

Updates

CI Sector / Client Group

s.16(2)(c)

Context

Projects

[redacted] 1/26/2012 12:42 PM Moore, Bruce New!

Date/Time 1/26/2012 1:00 PM

Short Description [redacted]

Issue Status Closed

Detail Description

Handler Moore, Bruce

Updates

CI Sector / Client Group 01A Federal

Context

Projects

Possible copied and/or stolen pe... 1/26/2012 12:56 PM Murphy, Gregg New!

Date/Time 1/26/2012 1:00 PM

Short Description Possible copied and/or stolen personal information and credit card numbers

Issue Status Closed

Detail Description [redacted] requesting our assistance in having credit card numbers removed from pastebin.com [redacted] and [redacted]

Handler Murphy, Gregg

Updates Pastebin appears to be hosted by a Canadian ISP: WMD-GAME-SERVERS in Saint John, NB.

The sites are no longer active. Notified INTERPOL that no action was required on our part.

CI Sector / Client Group 07 Other Institutions

Context

Projects

Research into APT reported activ... 1/26/2012 1:07 PM Beaudoin, Luc S New!

Date/Time 1/26/2012 2:00 PM

Short Description Research into APT reported activity

Pages 1850 to / à 1851
are withheld pursuant to sections
sont retenues en vertu des articles

13(1)(a), 16(1)(b)

of the Access to Information
de la Loi sur l'accès à l'information

Anderson, Windy

From: Gordon, Robert
Sent: January-31-12 8:07 AM
To: Matz, Mark
Cc: Dvorkin, Corey; Dick, Robert; Hatfield, Adam; Anderson, Windy
Subject: FW: Cyber: Cyber Security, Global Trends and Defences (SDA Report)
Attachments: Cyber-Security - Global Rules, SDA 2012.pdf

FYI

Robert W. (Bob) Gordon
Special Advisor, Cyber Security / Conseiller spécial, cybersécurité
Public Safety Canada / Sécurité publique Canada
340 Laurier Avenue West / 340 avenue Laurier Quest
Ottawa, Ontario K1A 0P9 / Ottawa (Ontario) K1A 0P8
613 949-7380 Fax/Téléc.: 613 990-3287
E-Mail / Courriel: Robert.Gordon@ps-sp.gc.ca

Report: *Cyber Security: The Vexed Question of Global Rules*, is attached

http://www.darkreading.com/security/news/232500700/mcafee-and-security-defence-agenda-release-global-cyber-defense-report.html

McAfee and Security & Defence Agenda Release Global Cyber Defense Report

Fifty-seven percent of global experts believe that an arms race is taking place in cyberspace

Jan 30, 2012 | 12:11 PM |

Brussels, Washington DC - JANUARY 30, 2012 - McAfee and the Security & Defence Agenda (SDA) today revealed the findings from a report; Cyber-security: The Vexed Question of Global Rules that paints, for the first time, a global snapshot of current thinking about the cyber-threat and the measures that should be taken to defend against them, and assesses the way ahead. The SDA, the leading defense and security think-tank in Brussels, interviewed leading global security experts to ensure that findings would offer usable recommendations and actions. The report was created to identify key debate areas and trends and to help to governments and organizations understand how their cyber defense posture compares to those of other countries and organizations.

Here are some noted findings:

57% of global experts believe that an arms race is taking place in cyber space. 36% believe cybersecurity is more important than missile defense. 43% identified damage or disruption to critical infrastructure as the greatest single threat posed by cyber-attacks with wide economic consequences (up from 37% in McAfee's

2010 Critical Infrastructure Report). 45% of respondents believe that cybersecurity is as important as border security. The state of cyber-readiness of the United States, Australia, UK, China and Germany all ranked behind smaller countries such as Israel, Sweden and Finland (23 countries ranked in report).

McAfee asked the SDA, as an independent think-tank, to produce the most informed report on global cyber defense available. The SDA had in-depth interviews with some 80 world-leading policy-makers and cybersecurity experts in government, business and academia in 27 countries and anonymously surveyed 250 world leaders in 35 countries. As the only specialist security and defense think-tank in Brussels, SDA has become one of the world's leading forums for the discussion of international defense and security policies. The methodology used for rating various countries' state of cyber-readiness is that developed by Robert Lentz, President of Cyber Security Strategies and former Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance. [see here for infographic on rankings]

Top 6 Actions Cited in Report

Real-time global information sharing required Financial incentives for critical improvements in security for both private and public sectors Give more power to law enforcement to combat cross-border cyber crime Best practice-led international security standards need to be developed Diplomatic challenges facing global cyber treaties need to be addressed Public awareness campaigns that go beyond current programs to help citizens

Real-time sharing of global intelligence was a core recommendation of the report, citing the building of trust between industry stakeholders by setting up bodies to share information and best practices, like the Common Assurance Maturity Model (CAMM) and the Cloud Security Alliance (CSA). "The core problem is that the cyber criminal has greater agility, given large funding streams and no legal boundaries to sharing information, and can thus choreograph well-orchestrated attacks into systems," says Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector, McAfee. "Until we can pool our data and equip our people and machines with intelligence, we are playing chess with only half the pieces."

Experts interviewed also agreed that developments like smart phones and cloud computing mean we are seeing a whole new set of problems linked to inter-connectivity and sovereignty that require new regulations and new thinking. Last year, McAfee issued a Q3 threat report that stated that the total amount of malware targeted at Android devices jumped 76 percent from Q2 of 2010 to Q2 of last year, to become the most attacked mobile operating system.

Other key report findings from the SDA report include the following:

Need to address expected shortage of cyber workforce: More than half (56%) of the respondents highlight a coming skills shortage. Low level of preparedness for cyber attacks: China, Russia, Italy and Poland fall behind Finland, Israel, Sweden, Denmark, Estonia, France, Germany, Netherlands, UK, Spain and the United States. Cybersecurity exercises are not receiving strong participation from industry: Although almost everyone believes that exercises are important, only 20% of those surveyed in the private sector have taken part in such exercises. Risk assessment: Prioritize information protection, knowing that no one size fits all. The three key goals that need to be achieved are confidentiality, integration and availability in different doses according to the situation. Balance between security and privacy: Improve attribution capability by selectively reducing anonymity without sacrificing the privacy rights.

While many respondents believed that global treaties were an essential factor in the development of sound policy, some also suggested the establishment of cyber-confidence building measures as alternatives to global treaties, or as a stopgap measure, since treaties are seen as unverifiable, unenforceable and impractical. Stewart Barker, the former Assistant Secretary of Homeland Security under President George W. Bush, stated that

treaties "delude western countries into thinking they have some protection against tactics that have been unilaterally abandoned by other treaty signatories."

About the report: McAfee asked the Security & Defence Agenda (SDA) as an independent think-tank to produce the most extensive report on Cyber Defense. The report stack ranks the degree to which governments are prepared to withstand cyber attacks. This SDA report sets out to reflect the many different views on what cyber-security means, and how to move towards it. To build up a multi-faceted picture of opinion worldwide, SDA interviewed world leaders to highlight what they see as the key issues.

To download "The Cyber Defense Report" report please visit www.mcafee.com/

Dincoy, Rana

From: Bendelier, Kenneth
Sent: February-01-12 12:41 PM
To: Dincoy, Rana; Klassen, Nathan
Subject: Anonymous

s.16(2)(c)

- Anonymous
- AnonOps - GeneralActions
Source: anonops
Complete item: [redacted]

Description:
STOP War Against Iran.
STOP Economic shocks.
NO MORE S.O.P.A / A.C.T.A. / Biden-Sinde-Wert-Law / ...
NO MORE Censorship.
OPEN DATA.
FREE Manning, FREE Assange, FREE Anons.
FREE KNOWLEDGE.

SPREAD THE WORD.
EXPECT US!

Ken's Assessment: No worries Anonymous, we'll have all these requests fulfilled by noon tomorrow. Thank you for pointing these issues out to us.

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-993-5042
Facsimile | Télécopieur +1 613-954-3097
Kenneth.Bendelier@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

s.16(2)(c)

Williston, Sandra

From: Beaudoin, Luc
Sent: February-01-12 7:08 PM
To: CYBERDO
Subject: Anonymous

To add to existing anonymous activity
Anonymous claim to have breached the Irish Department of Foreign Affairs (www.dfa.ie) and posted userids and passwords to pastebin http://pastebin.com/[redacted]

[redacted]

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-01-12 8:40 AM
To: Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Black, Dave; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hebert, Brigitte; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki; * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 1, 2012/ le 1 février 2012

Print Media

Kim Dotcom faces charges - Megaupload founder facing extradition
In a New Zealand jail awaiting extradition to the U.S. on charges of racketeering, money-laundering and copyright crimes, (Kim) Dotcom has found himself at the centre of a high-stakes battle over Internet freedom versus copyright protection. It is a fight touching institutions from Congress to Silicon Valley and pitting the recording industry against some hip-hop artists who see Megaupload as a way to bypass record-label middlemen. In the days after Dotcom's arrest, the case has triggered an angry response from the hacker group Anonymous, which began an attack that briefly shut down websites, including the Justice Department, FBI, Universal Music and others. Vancouver Province

Online Media

Cyber Assault Aiming at Defense Department's Access Cards Sourced to China

Service members are reportedly getting an e-mail that has a formal-appearing PDF file infected with one new PC-virus facilitating keystroke logging, says California-located cyber-security company Alien Vault's lab manager Jaime Blasco. Miliatry.com published this in news on January 24, 2012. The virus, by recording keystrokes, garners the service member's PIN for Common Access Card, a type of smart-card as he reaches for a government system. According to Blasco, the cyber assault possibly has its source in China since the malware's written code contains Chinese characters. Blasco also explains that from the time of tracing the attack, the security company discovered software, which was solely utilized in China. Alien Vault's researchers are 99% sure, though not 100%, but quite certain that the attack originated out of China, Blasco adds. DoD BUZZ published this in news on January 24, 2012. SPAMFighter News

Report: Israel well prepared for cyber war
According to SDA-McAfee report, Jewish state experiences 1,000 cyber attacks per minute, but is most prepared to defend itself and deal with them. On the other hand, Israel initiates most attacks against its enemies – alongside Russia, China. "Israel has a national computer emergency readiness team (CERT), it participates in the informal CERT communities, it has a cyber strategy and a cyber command," says a report on cyber-preparedness authored by Brussels' specialist security and defense think-tank Security & Defense Agenda (SDA) with the support of computer security company McAfee. The report gives Israel a score of 4.5 out of 5 for its preparedness for a cyber attack. YNet News

An apocalyptic fantasy or an actual threat? How crippling would a cyberattack on the nation's power grid be?
Former chairman of the Joint Chiefs of Staff Adm. Michael Mullen, who retired in September, said during his tenure that cyberattacks pose an "existential threat" to the United States. While spies, cyberthieves and garden-variety hackers have caused untold economic loss to governmental agencies, companies and individuals by stealing information, the threat of a downed power grid and damage to other critical infrastructure presents a far greater risk, security analysts say. Measures are under way to bolster security, but some analysts say they offer too little. Asbury Park Press

'Make cyber laws enforcing websites to respond faster to govt'
Setting up a regulatory mechanism and making a law to force websites to respond faster would be a better solution than completely blocking websites if they carry objectionable content, a cyber security expert said here today. "I support not completely blocking popular social networking websites. In terms of illegal content, the government should create a regulatory authority where they will closely work with all these different websites. Whenever there is something offensive that is posted, it will be removed," Ankit Fadia, a prominent computer security expert and ethical hacker, told PTI. The regulatory mechanism should be broad-based without the government representatives alone having monopoly, he said. Daily News and Analysis (India)

"Slain" Kelihos botnet still spams from beyond the grave
A botnet capable of delivering almost four billion spam messages per day has been confirmed resurrected—more than four months after Microsoft celebrated its untimely demise. Researchers with Kaspersky Lab reported on Tuesday that Kelihos, a peer-to-peer botnet that also goes by the name Hlux, continues to spew spam in a variety of languages. A new version of the underlying malware appeared as early as September 28, 2011, a day after Microsoft took credit for disrupting the rogue network by commandeering the infected computers and obtaining a court order seizing the Internet addresses used to help control them. The resurrection highlights the difficulty of permanently severing botnets from the Internet. ARS Technica

Update: Windows Media Player vulnerability
New research from M86 Labs adds further insight on the MIDI exploit first highlighted by Trend Micro last week. The attack uses the methodology described by Vupen; a non-trivial exploit that works in Internet Explorer 6 to 9. Microsoft fixed this vulnerability in its January patch release. M86 describes how an infected web page hosted in South Korea loads a malicious MIDI file. The MIDI file is used to download an executable which is itself a downloader. This fetches the ultimate payload; a basic rootkit. Info Security

Defense companies persistently targeted by cyber spies
Researchers from security companies Zscaler and Seculert have issued a warning about bogus emails targeting employees of defense-related organizations around the world in order to trick them into installing malware. "Dear Sir, It is a conference that you may possibly be interested in. More information is attached below," says in the recent emails. The attached file is a specially crafted PDF that, at first glance, looks like a completely harmless invitation to a relevant industry conference such as the IEEE Aerospace Conference or an Iraq Peace Conference. But, once downloaded and opened, the file exploits vulnerabilities within Adobe Reader in order to drop and run a Trojan that opens a backdoor into the system. Help Net Security

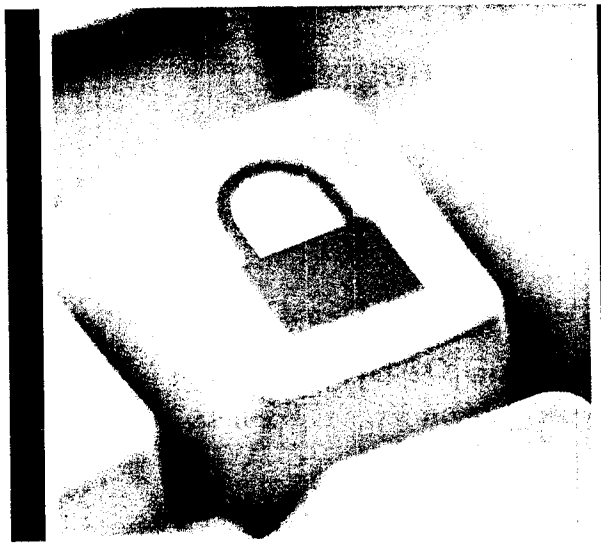
BitDefender Finds Fresh Threat that's Mixture of Malicious Programs
BitDefender, which analyzed 10m contaminated files, found approximately 40,000 samples of "Frankenmalware." Reportedly, these samples represent some 0.4% of detected malicious programs. Thus, according to the company, the

situation suggests about 260,000 hybrid samples as potentially floating in cyber-space. ITProPortal published this on January 24, 2011. Understandably, the company began its research of the malware sandwiches when it discovered the Rimecud worm that a file infector, Vitrob contaminated. The former malicious program filches passwords for e-mail accounts, social-networking, online shopping, e-banking, amidst other functions. In the meantime, Vitrob lets the remote attacker issue commands, while the file-infector effectively evades firewalls as well as makes sure it stays on the host PC via performing a code-insertion inside one critical process namely Winlogon. SPAMFighter News

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



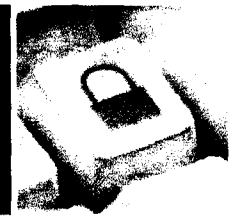
Canadian Cyber Incident Response Centre

CTCP Update

Feb 2012

Canada

CCIRC – Recent Changes



BUILDING A **SAFE** AND **RESILIENT CANADA**

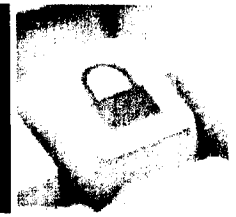
In October of 2011, CCIRC transferred from the Emergency Management Services (EMS) of the GC to the National Cyber Security Doctorate of Public Safety (NCSD)

NCSD and CCIRC now form the Operational and Policy based leadership roles within the Department of Public Safety, resulting in an improved alignment with National Cyber Strategy Pillars.

NCSD Subsections

- Canadian Cyber Incident Response Centre
- Technical Advice
- Policy
- Engagement and Partnerships

CCIRC – A New National Mandate



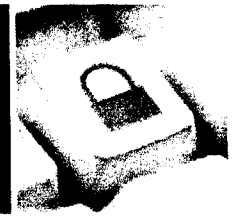
BUILDING A **SAFE** AND **RESILIENT CANADA**

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention, mitigation, and response to cyber events.

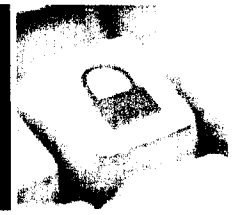
CCIRC provides authoritative advice to, and coordinates information sharing and event response among, all levels of government, international counterparts, critical infrastructure operators and information technology vendors.

CCIRC – Organizational Structure



- Organized into three functions:
  - **Incident Handling** – assists partners in identifying, mitigating, and managing incidents
  - **Technical Support** – operates CCIRC lab infrastructure and provides technical analysis support to incident handling and analysis
  - **Strategic Initiatives and Situational Awareness** – builds and maintains operational relationships with partners, and produces strategic analysis products for decision makers

Public Safety Canada Agenda

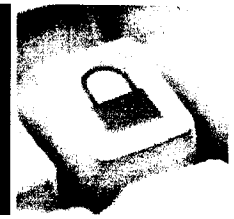


BUILDING A **SAFE** AND **RESILIENT CANADA**

- Closely aligned to the pillars of Canada's Cyber Security Strategy:
  1. Secure Government systems.
     - Provide strategic policy leadership and establish clear federal roles and responsibilities
     - Strengthen the security of federal systems
     - Promote awareness throughout the Government of Canada
  2. Partner to secure systems outside the Government of Canada.
     - Engage with provinces and territories as owners, operators and regulators of critical infrastructure services, and as partners in education and awareness
     - Leverage and build upon public-private partnerships to secure critical infrastructure and promote awareness
     - Liaise with international partners on cyber security operational and policy issues
     - Work with academic and research institutions to educate, develop and foster innovation
  3. Help Canadians to be secure online.
     - Awareness of the need to act
     - Information about how to act
     - Protection from those who act criminally

- The department is responsible for the coordination of the overall Government of Canada's efforts in implementing the Strategy

Where CCIRC fits in *Canada's Cyber Security Strategy*



BUILDING A **SAFE** AND **RESILIENT CANADA**

Securing Federal Government Systems

Key actors:
- CSEC
- Shared Services
- TBS CIOB
- CF

Partnering to Secure Vital Systems Outside the Federal Government

Key actors:
- PS CCIRC, NCSD, CISCD
- CI Sector lead departments

Existing effort:
- PT, select CI (telecom, energy, finance)
- 05 CERTs

Future effort:
- trusted vendors
- international CERTs
- remaining CI sectors
- economic interests
- academia

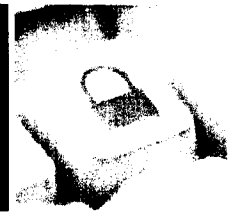
Helping Canadians to be Secure Online

Key actors:
- PS Communications
- law enforcement
- Industry Canada
- CRTC
- Privacy Commissioner
- Competition Bureau

Audiences:
- Home users
- Academia
- Small business

State-sponsored cyber espionage ← ***Risk*** → **Crime**

CCIRC – National Focus



BUILDING A **SAFE** AND **RESILIENT CANADA**

These partners... *provide information to...* *which provides these services:*

Government S&I community

Critical Infrastructure

Provinces and territories

Five Eyes and International CERTs

Trusted vendors

Academia

Cyber security expert community

Open source

CCIRC

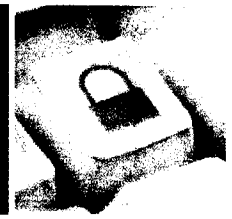
Incident Handling and National Event Coordination and Assistance
- Direct technical assistance to partners and coordination of Government response to cyber events of national significance
- Audience: technical staff in partner organizations responding to cyber incidents
- Metric: 749 incidents responded to in 2011; 197 notifications to partners of compromised systems, 9 requests issued to shut down malicious systems in Nov/Dec 2011

Provision of Mitigation Advice
- Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice
- Audience: technical staff in partner organizations
- Metric: 27 Cyber Flashes, 6 Alerts, 49 Advisories, and 13 Technical Notes in 2011

Reporting and Analysis
- Daily, weekly, monthly and annual reports providing summary, trend, and strategic analysis
- Audience: technical staff, decision makers (under development)

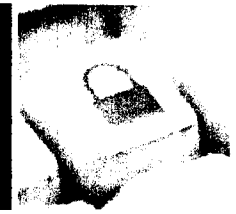
Public Safety Canada | Sécurité publique Canada

Current challenges



- **Incident Handling and National Event Coordination and Assistance**
  - we can't say no – difficult to prioritize clients and services without clearly defined mission and mandate; prospective client base too broad
  - ambiguity of roles in an emergency – absence of a national emergency policy for cyber creates ambiguity for Government and Public Safety
  - limited profile – increased awareness of CCIRC and a credible brand will increase incident reporting
- **Provision of Mitigation Advice**
  - technology – lab infrastructure aging
  - people – attraction and retention of specialized, bilingual, TOP SECRET staff an ongoing challenge
  - policy – sharing sensitive information
  - accommodations – lack of long-term plan to obtain permanent and highly secure space hampers ability to handle classified information
- **Reporting and Analysis**
  - strategic analysis product for broader audience to be developed

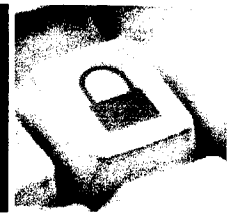
Progress in 2011



- Incident Handling and National Event Coordination and Assistance
  - 6 positions staffed this year; 8 remaining to attain full complement of 22; process underway for 4 more CS03s
  - working with U.S. on plan to inventory and explore potential alignment of information products (e.g., flashes, alerts, technical reports) (NCSD*)
- Provision of Mitigation Advice
  - initiated investment in lab infrastructure
  - development of an Industrial Control System (ICS) test-bed in conjunction with Defence R&D Canada and the private sector
  - launched development of secure web portal for info exchange with CI / PT
  - information-sharing MOUs under development with selected PTs and CI sectors (NCSD*)
- Reporting and Analysis
  - working with S&I community on potential joint products (NCSD*)

* Other divisions within NCSD engaged or leading

Near term objectives (January – March)

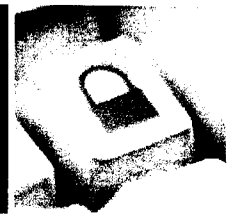


- Incident Handling and National Event Coordination and Assistance
  - initiate discussions with PTs on national cyber incident response (NCSD)
  - conduct federal tabletop exercises to clarify roles in a national response (NCSD/CCIRC)
  - consult U.S. on initial draft of Canada-U.S. Cyber Security Action Plan to consolidate and drive commitments under Beyond the Borders and other forums (NCSD)
  - launch anticipatory staffing for Cyber Defence initiative's potential 14 new FTEs for CCIRC with projected start date of April 1, 2012 (CCIRC)
  - develop standardized training regime and integration packages (NCSD)
- Provision of Mitigation Advice
  - increased engagement with PT and private sector partners (NCSD, CCIRC)
  - launch secure portal as repository for CCIRC products and mitigation advice (CCIRC)
  - work with corporate branch on short-term accommodations plan for CCIRC
- Reporting and Analysis
  - identification of partner requirements and defining new products and services (NCSD)

Medium term objectives (April - September)

- Incident Handling and National Event Coordination and Assistance
  - explore potential short-term personnel exchange with CSEC's Cyber Threat Evaluation Centre for new fiscal year
  - participate in and conduct cyber based exercises to support operational objectives: PTs and CI, Cyber Storm 4, CMX
  - begin implementation of alignment of information products with US-CERT
  - finalize plans with PS-Comms on CCIRC name change, re-branding, re-launching to enhance credibility, visibility, and help to address staff attraction and retention
  - initiate work to develop a cyber Emergency Support Function (ESF) under the Federal Emergency Response Plan (FERP)
- Provision of Mitigation Advice
  - work with corporate branch on long-term accommodations plan for CCIRC and NCSD
  - [redacted]
  - explore options for automation in lab testing and analysis, more technology
- Reporting and Analysis
  - pilot production of new products and services for new audiences (CCIRC)

NCSD: Policy Agenda



- Develop a Performance Measurement Strategy, as part of implementing Canada's Cyber Security Strategy
- Develop a Canadian position towards participation in emerging dialogue on norms and standards for international conduct in cyberspace (in anticipation of the United Kingdom Conference in November)
- Consider options for a cyber legislative review aimed at ensuring that the Government has flexibility, credibility and effectiveness in dealing with future cyber security challenges
- Following establishment of a forum of cyber security policy leads/interlocutors, strengthening the intergovernmental engagement on cyber security
- Partnerships: In partnership with lead departments, build on progress made with priority critical infrastructure sectors (Telecommunications (CSTAC); Energy) and engage with the Financial Sector

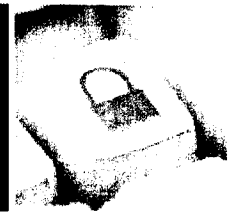
Communications: Public Awareness Campaign

- A **multi-year cyber security public awareness campaign** will be the **cornerstone of a high profile and phased communications strategy** that will provide Canadians with information on cyber threats in order for them to take action to protect themselves and their personal information
- To this end, Public Safety is undertaking proactive communications initiatives, including a national public awareness advertising campaign (getcybersafe.gc.ca), international coordination of messaging and cyber incident management
- Public Safety Canada is the federal focal point for the coordination of cyber security communications activities
- Working Group allows for broad awareness of and contribution toward creative development, Web content, incident management and other core communications activities

Operational Partnerships

- Recent Partnerships Development:
  - Team Cymru;
  - Microsoft;
  - Canadian Electrical Association;
  - Canadian Association of Petroleum Producers;
  - CRTC – Enforcer for new Regulation to fight spam, phishing and vishing
    - Includes collaboration with:
      - Industry Canada
      - Competition Bureau
      - Office of Privacy Commissionnaire
      - Private Sector (Spam Reporting Centre Bid)

Operational Events

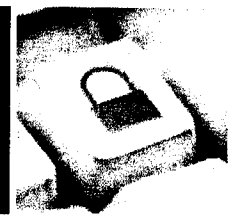


- Jul 2011 – Jan 2012
  - 387 managed events

- Hacktivism:
  - ACTA, SCADA, Israel-Palestine,
  - Pastebin and XSSed !

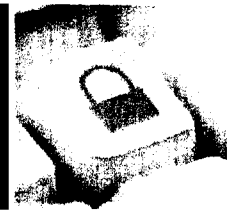
- Crimeware
  - SQL injections (ASP.net and other)
  - Wordpress
  - OWA account phishing
  - Black Hole, Zero-Access, Incognito, exploiting Java vulnerabilities
  - DNSChanger

Operational Events



- APT:
  - Oil Industry (merger and acquisition) s.16(2)(c)
  - G20 France
  - ShadyRAT (McAfee)
  - [redacted]
  - Certificate Authority Compromise (Diginotar)
  - DUQU (HU-CERT), NITRO (Symantec), LURID (Trend Micro), Htran (Secureworks)
- Vulnerabilities
  - ICS exposed to Web (Shodan and ICS-CERT)
  - cURL implementation in e-commerce sites.

DNSChanger

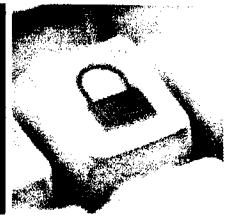


- An opportunity to Notify
  - FBI / Court Order to seize and provide DNS service: 8 Nov – 8 Mar
  - Victims damage mitigated.

s.16(2)(c)

- Need to Notify
  - Vulnerable to future hostile activities
  - IP space pollution
- Initial count in Canada:
  -
- Current:
  -
- Rate:
- CCIRC notifications: 2 to 5 times a week.

DNSChanger Remediation by CTCP

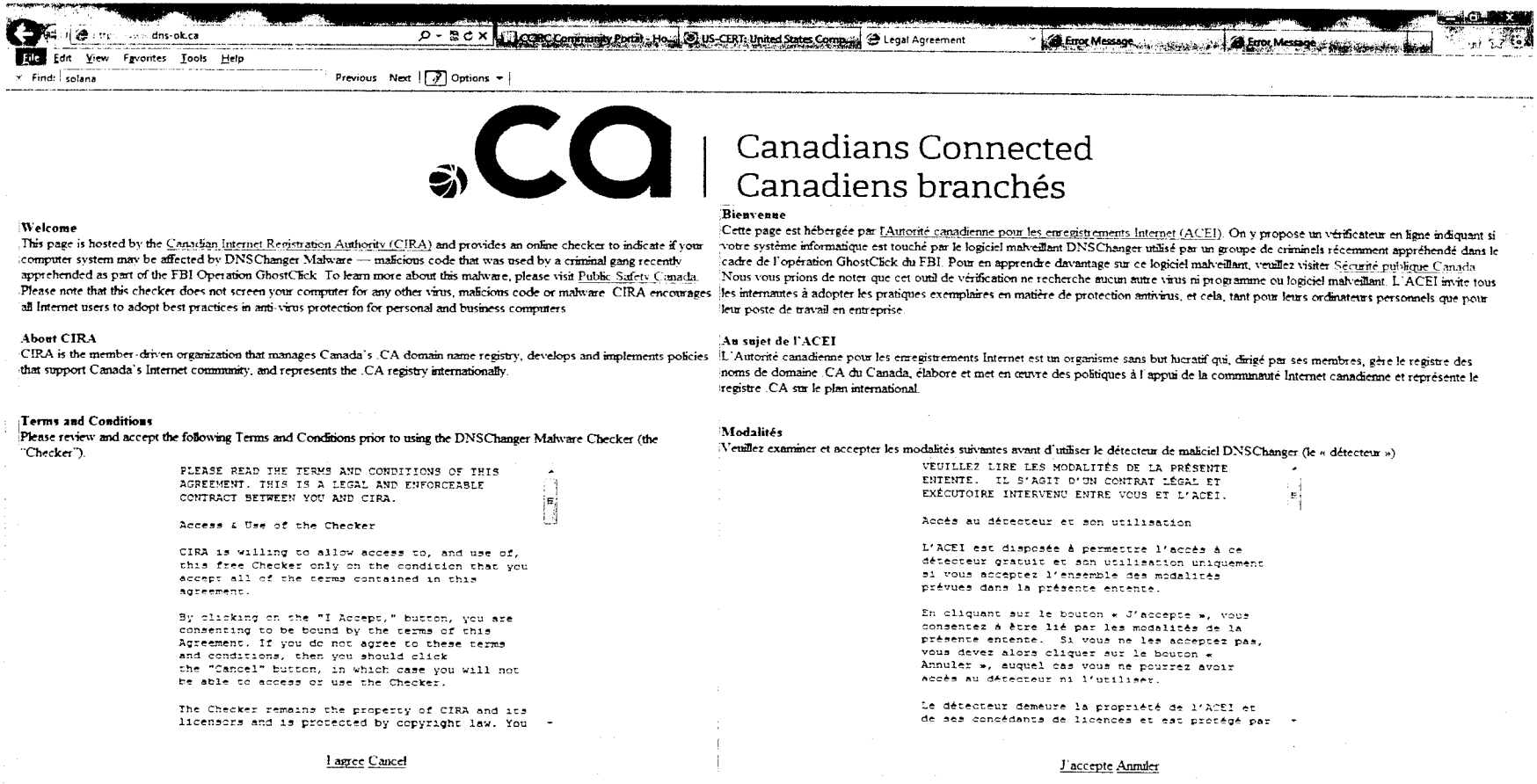


BUILDING A **SAFE** AND **RESILIENT CANADA**

Public Saf
Canada

DNSChanger Eye-Chart

BUILDING A **SAFE** AND **RESILIENT CANADA**



DNSChanger Eye-Chart

CANADA

Your computer system does not appear to be affected by DNSChanger Malware

A RED banner at the top and bottom of this page indicates your computer system appears to be using a Domain Name System (DNS) that was part of the criminal infrastructure seized during Operation GhostClick. You are encouraged to consult the following Public Safety Canada document for further information:
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-002-eng.aspx.

A GREEN banner at the top and bottom of this page indicates your computer system uses a DNS which is not known to be associated with the criminal DNS infrastructure associated with Operation GhostClick.

How does the checker work?

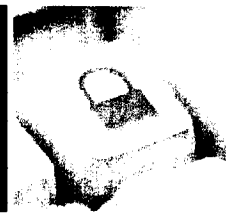
The GREEN or RED banners are determined based on the DNS request performed by your computer in order to obtain the Internet Protocol (IP) address associated with DNS-OK.ca. This request is forwarded to CIRA's DNS infrastructure by your DNS (typically provided automatically to your computer or home router by your Internet Service Provider). The IP address of your requesting DNS is compared to known Operation GhostClick IP addresses, which results in a RED or GREEN banner page.

If you have any questions or need clarification, please contact your Internet Service Provider (ISP).

.ca

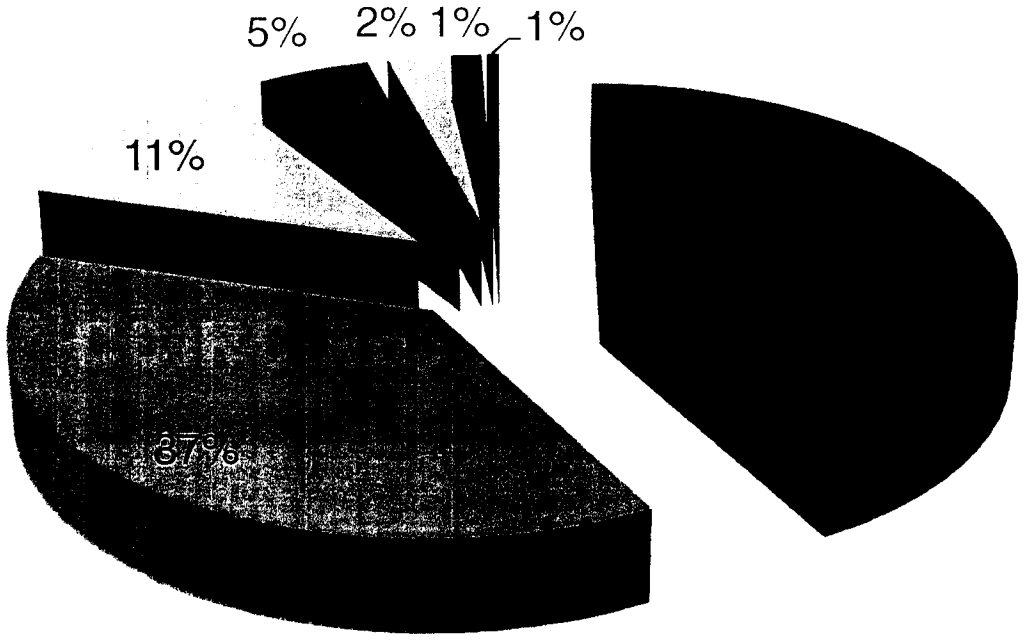
Your computer system does not appear to be affected by DNSChanger Malware

CCIRC Reported Events Jul 2011-Jan 2012



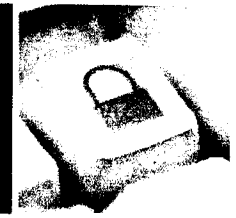
BUILDING A **SAFE** AND **RESILIENT CANADA**

Events



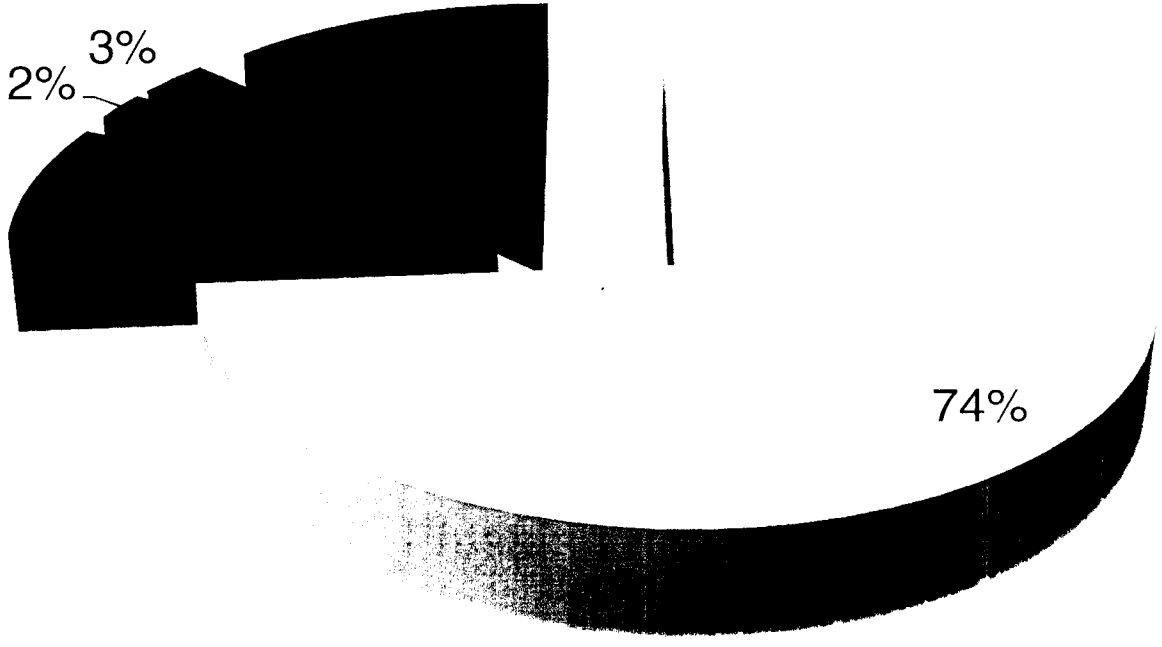
- Cat 3 - MALICIOUS CODE / COMPROMISE
- Cat 7 - PHISHING / TARGETED EMAILS
- Cat 6 - INVESTIGATION / RESEARCH
- Cat 4 - IMPROPER USAGE / MISCONFIG
- Cat 1 - UNAUTHORIZED ACCESS / CREDENTIAL THEFT
- Cat 5 - SCANS/PROBES/ATTEMPTED ACCESS
- GridEx

Phishing Reports

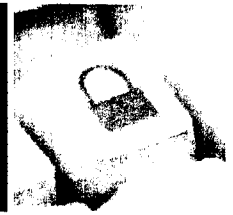


BUILDING A **SAFE** AND **RESILIENT CANADA**

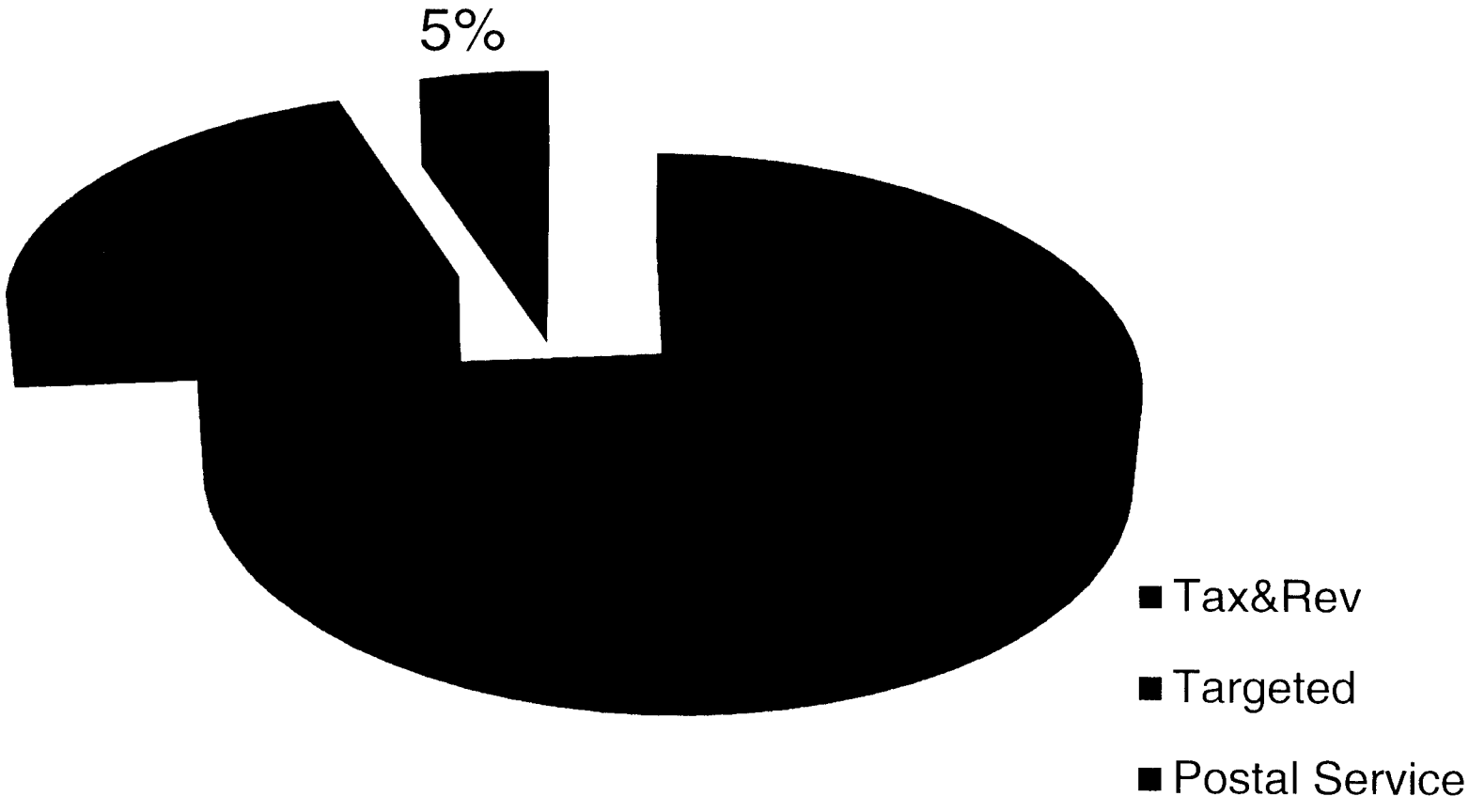
Phishing Reports to CCIRC
Jul 2011 - Jan 2012



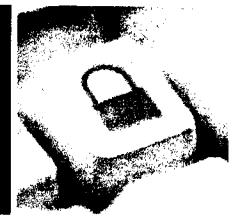
Phishing Reports



Federal



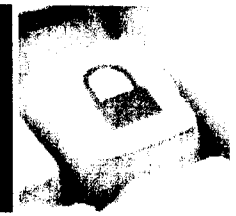
ATI requests...



- "Malicious site hosted on MEMBER take down"
  - MEMBER exempted un 20(1)C -> Economic damage.

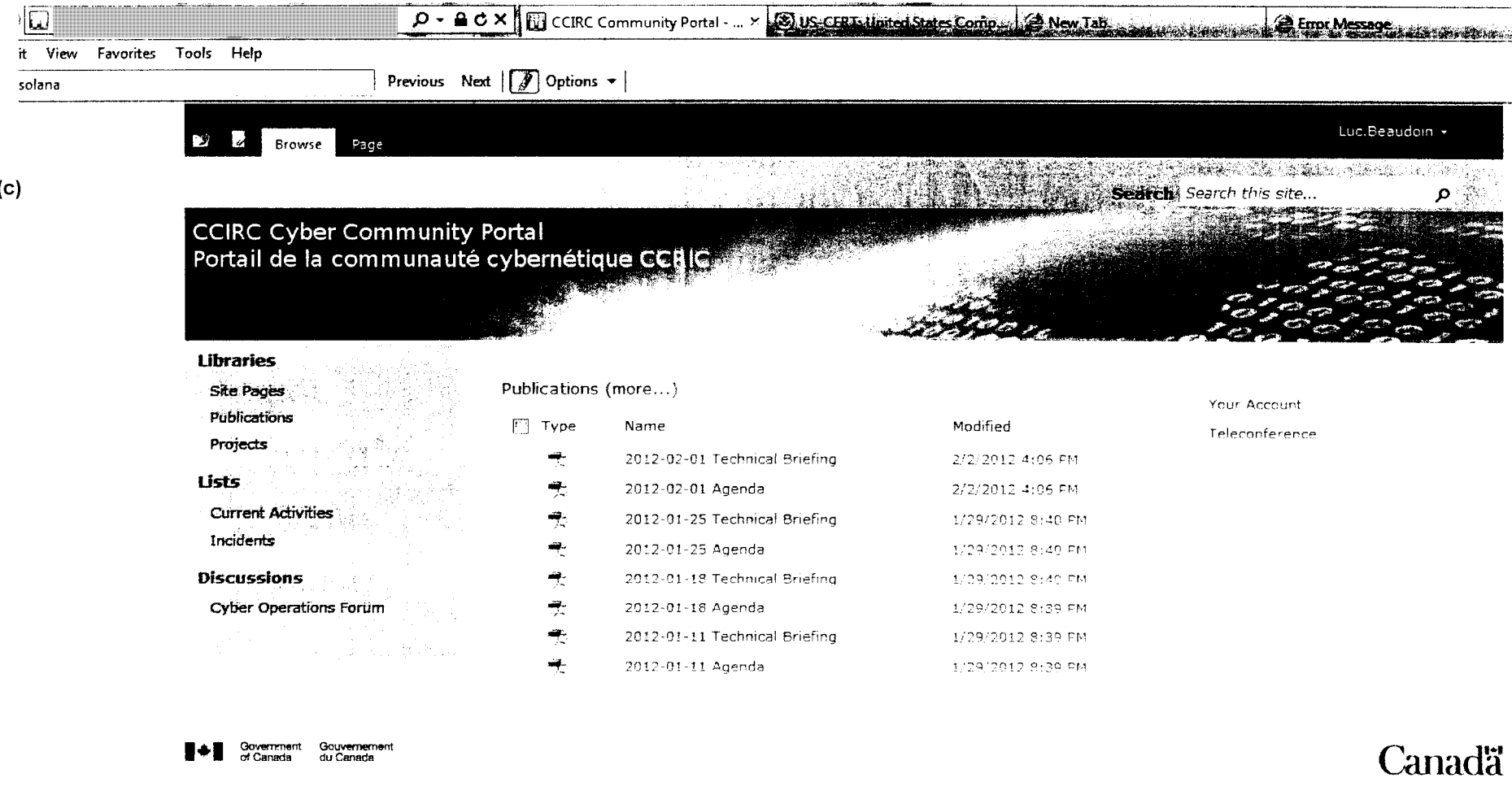
- If you are contacted by an ATI coordinator…

Canadian Cyber Community Portal

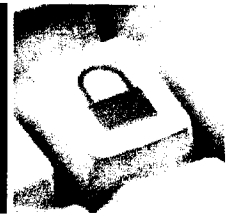


BUILDING A **SAFE** AND **RESILIENT CANADA**

s.16(2)(c)



Technical Capabilities

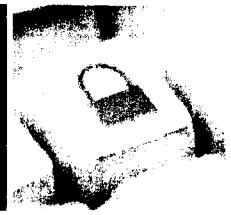


- Automated malware analysis tools being reviewed:

s.16(2)(c)

- implementation in the next quarter
-
-
- Significant overhaul of lab infrastructure

Questions?



Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-01-12 8:11 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
February 1, 2012 / le 1 février 2012

MINISTER / MINISTRE

Top Mountie says he is moving fast to end harassment on force
A day after the RCMP Public Complaints Commission issued a call for citizen input in its probe of harassment complaints involving the Mounties, Canada's new RC-MP commissioner outlined the steps he's already taken to address the issue. Testifying before a Commons committee Tuesday, Bob Paulson said he has centralized oversight of all harassment complaints in Ottawa to ensure they are dealt with in a timely fashion. Paulson also faced a barrage of questions Tuesday about whether the federal government was trying to muzzle him. He denied the allegations, which surfaced earlier this month after Senator Colin Kenny unveiled details of an email exchange he had with Paulson in which he was told that all meetings with the commissioner had to be routed through **Public Safety Minister Vic Toews' office**. Paulson told parliamentarians that it's always been the RCMP's practice to inform **the minister** responsible for the force about meetings that may have political implications and that the guidelines have simply been consolidated into a single communications protocol. He even hinted that the real reason he "routed" Kenny through **the minister's office** was because he didn't really want to meet with the outspoken Liberal who has a keen interest in justice issues. "I'd just as soon not meet with Sen. Kenny, to be honest with you," Paulson said, refusing to elaborate later. Ottawa Citizen, A3 (Edmonton Journal, Calgary Herald)

Top Mountie dogged by accusation he's muzzled
The commissioner of the RCMP has batted away allegations the federal government is trying to muzzle him. He was called to testify over recent allegations that **Public Safety Minster Vic Toews** stopped him from meeting Liberal Senator Colin Kenny, prompting the NDP to accuse the Conservatives of trying to control Mountie communications. Calgary Sun, 23 (Edmonton Sun); Toronto Star; The Province; * National Post

We're now a banana republic
A letter to the editor states, "It would seem that **Vic Toews** has a problem with memory. The utopian parliamentary system he speaks of is not in Canada. I have watched Parliament for quite a few years. Among other egregious behaviour, the dysfuntionality of parliamentary committees is legendary - ask any opposition member. Under this government, Parliament has degenerated almost beyond redemption. It is ludicrous to expect Canadians to believe anything coming out of the PMO, where all messages originate..." Toronto Star, A24

Smugglers dump Canada-bound Tamils in Togo
Two hundred Tamil refugees from Sri Lanka are stranded in West Africa, BBC reports, after the human smuggling ring they hired to bring them to Canada marooned them in Togo. The BBC says the contingent travelled by ship from Sri Lanka to India, then on to Ethiopia before flying to Togo. After being assured they could fly to Canada from neighbouring Ghana, they say their human smuggler abandoned them, the report says. **Public Safety Minister Vic Toews** said Tuesday he could not confirm reports about the wayward refugee claimants. "***I understand that there's some rumours going around in respect of another illegal migrant boat,***" he said. ***"I can assure you that our agencies work closely with governments around the world in order to stop criminal activities with respect to human smuggling"..."We will continue to work with allies overseas and ensure that human smugglers do not involve themselves and criminally take advantage of unfortunate people,***" he added. **Toews** said the government hopes to quickly pass a bill titled the Preventing Human Smugglers from Abusing Canada's Immigration System Act. "***We urge our opposition parties here to support that legislation to ensure that we have the appropriate tools by which to deal with human smuggling and criminal operations,***" he said. Ottawa Citizen, A6 (Edmonton Journal, Times & Transcript, Vancouver Sun, Calgary Herald, National Post); Edmonton Sun (Winnipeg Sun, Toronto Sun, London Free Press, Calgary Sun)

Ministers scolded over prison transfers

Public Safety Minister Vic Toews and his two Conservative predecessors have been criticized in a recent Federal Court decision for repeatedly failing to provide adequate reasons when refusing to let Canadians jailed abroad be transferred to a prison in Canada. The ruling is the latest case to pit the government against judges who say the **public safety minister** has not used his discretionary powers in a transparent, reasonable way. In the latest court case, Mr. Justice Robert Barnes ruled on Jan. 19 that **Mr. Toews** didn't provide proper grounds to explain why he turned down a bid by Richard Goulet, a Quebec man serving time at a low-security penitentiary in Pennsylvania for smuggling marijuana. The judge noted that in 12 previous cases, **Mr. Toews** and his predecessors have failed to follow the requirement in the transfer of offenders act to justify their decision. The cases, starting in 2008, were decided by **Mr. Toews** and his predecessors Peter Van Loan and Stockwell Day. In several of those files, **the minister's** decision went against assessments by Correctional Service of Canada that the applicants were at a low risk of reoffending. Mr. Goulet, a bankrupt construction contractor who is serving a seven-year sentence, has no previous criminal record, and a Correctional Service Canada report given to **the minister** said the 42-year-old Quebecker is not likely to reoffend. **Mr. Toews's** decision wasn't reasonable because it was "a recitation of some of the relevant facts and a bare conclusion that ran contrary to the overwhelming weight of the evidence [in the CSC report]," the judge noted. He ordered **Mr. Toews** to review the case again and provide more thorough reasons if he rejects it. A **spokeswoman for Public Safety** Canada said the court's decision will be appealed. Globe and Mail, A5

Pro gun-registry reports suppressed
The NDP accused the government of suppressing RCMP reports on Canada's long-gun registry Tuesday, saying the government delayed releasing two reports because they clashed with Tory messaging on gun control. NDP justice critic Jack Harris raised the issue in question period Tuesday. **Public Safety Minister Vic Toews** told the House of Commons he released the report at the earliest opportunity. "***I understand that the report was provided by the RCMP to the Department of Public Safety on December 16***," he said. ***"It was then forwarded by the Department of Public Safety to my office on December 20 and we tabled it on the first available tabling date, as I understand it.***" Montreal Gazette, A11 (Times & Transcript); Waterloo Region Record (The Guardian)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Flood deal accepted**
On Monday the members of the Sakimay First Nation voted to accept the $21-million flood claim settlement. The Sakimay First Nations will receive $21,191,732 as part of a settlement agreement. The settlement and compensation were arrived at after lengthy negotiations between Sakimay and the federal and provincial governments. Leader-Post, A3

*** U.S. panel defends call to censor bird flu studies**
A potentially deadlier form of the bird flu virus poses one of the gravest known threats to humans and justifies an unprecedented call to censor the research that produced it, a top U.S. biosecurity official said on Tuesday. Whig-Standard, 13; The Guardian

*** H5N1**
Les magazines scientifiques Science et Nature publiaient hier les explications formulées par le Bureau national américain de la science pour la biosécurité (NSABB) qui recommande de censurer pour des raisons de sécurité deux articles scientifiques qui décrivent par le menu comment ont été créés des mutants de la souche H5N1 de la grippe aviaire, lesquels mutants seraient désormais capables de se transmettre entre mammifères, voire entre humains -- et de ce fait, feraient réapparaître le spectre d'une pandémie. Le Devoir, A2

*** L'influenza s'est rarement tenu aussi tranquille au Québec**
Même si le nombre de cas est en hausse depuis quelques jours, la saison de la grippe saisonnière a rarement été aussi calme au Québec. Le virus de l'influenza circule peu, c'est "exceptionnel", et il faut croire que la réponse immunitaire de la population est bonne, estime l'Institut national de santé publique du Québec (INSPQ). La Presse, A9 (Le Soleil, Le Quotidien)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** U.S. intelligence chiefs give mixed news**
Decapitation strikes killed Osama bin Laden and other top al-Qaeda leaders in the past year but new, even more dire threats loom - among them a nuclear-armed Iran or paralyzing cyber-attacks - President Barack Obama's top intelligence chiefs warned Tuesday. The killing of top al-Qaeda leaders marginalized the group's operational threat, said James Clapper, Director of National Intelligence. Globe and Mail, A6

*** Le Canada expulse deux diplomates russes**
Deux diplomates russes ont été renvoyés du Canada en lien avec une affaire d'espionnage impliquant un sous-lieutenant de la marine canadienne, a annoncé hier la chaîne de télévision CTV, citant des sources qu'elle n'a pas identifiées. L'un de ces diplomates, Dimitri Guerasimov, était en poste au consulat russe à Toronto, tandis que l'autre, Sergueï Joukov, était l'attaché militaire à l'ambassade à Ottawa, a indiqué le quotidien The Globe and Mail. La Presse, A19 (Journal Montreal)

*** THOSE WHO HATE CANADA**
A letter states, "It boggles my mind when we can have people who clearly hate the West, be it for its culture, religion, or even its democratic values, come to this country and call it home. They thrust their barbaric ideology, its sixth-century religious law and archaic cultural traditions on us, while spitting, disrespecting and devaluing Canada's own culture, history and religious background. From the Shafias who murdered their three female children and first wife over a false idea of honour. To Khadr, a misguided child soldier who clearly has the family background to prove his disdain and hatred for the West. My ultimate question to those people who hate Canada, the U.S and the West is: Why move to a country you clearly hate? I can sum it up to three reasons: 1) Better wages, 2) Free education, health care and social programs, 3) A lax justice system that usually favours the politically correct crowd. If you hate Canada and the West, please go back to your country of origin. Canada will be a better place." Ottawa Sun, 14

CYBER SECURITY / CYBERSÉCURITÉ

*** Kim Dotcom faces charges - Megaupload founder facing extradition**
In a New Zealand jail awaiting extradition to the U.S. on charges of racketeering, money-laundering and copyright crimes, (Kim) Dotcom has found himself at the centre of a high-stakes battle over Internet freedom versus copyright protection. It is a fight touching institutions from Congress to Silicon Valley and pitting the recording industry against some hip-hop artists who see Megaupload as a way to bypass record-label middlemen. In the days after Dotcom's arrest, the case has triggered an angry response from the hacker group Anonymous, which began an attack that briefly shut down websites, including the Justice Department, FBI, Universal Music and others. Vancouver Province, A28 (Calgary Herald)

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

RCMP commissioner asserts his independence
RCMP Commissioner Bob Paulson is backtracking on his call for MPs and senators to go through the Department of Public Safety to hold a meeting with him, saying he will safeguard his independence from the rest of government "like a terrier." Commissioner Paulson told a parliamentary committee on Tuesday he intends to give notice to his political bosses only about meetings that might be of interest to them, such as with diplomats or politicians. He added that he has no obligation to debrief the government after he meets with RCMP outsiders. Regarding an e-mail in which he recently called on Liberal Senator Colin Kenny to "route" his request through **Public Safety**, Commissioner Paulson suggested that it was a polite brush-off. Globe and Mail, A4; Windsor Star

Dead wrong on guns
An opinion piece states, "Matt Gurney is dead wrong when he states that the gun registry has no statistical connection to the decline in Canada's suicide rate. I suggest he read the 2008 Master's thesis of Marie-Pier Gagné on this specific subject. Controlling for virtually every factor imaginable, it clearly demonstrated that the registry could be clearly shown to have reduced firearm related-suicide deaths by 250 per/100,000 population each and every year..." National Post, A11

Bring back the right to self-defence
An opinion piece states, "On Monday, Ian Thomson of Port Colborne, Ont., went on trial on two charges of unsafe storage of a firearm, relating to a well-publicized self-defence incident...Four men were later arrested and charged with arson (yet not, strangely, for attempted murder or assault with a deadly weapon) for the attack, thought to be related to a long-running property dispute between Mr. Thomson and his neighbour. But Mr. Thomson himself was then arrested and charged with the counts of unsafe storage of a firearm, as well as unsafe use of a firearm and pointing a firearm...The federal government, in part due to public outcry relating to Mr. Thomson's case and other similar stories, has promised to review the myriad laws that serve to make self-defence cases so complex and difficult...Mr. Thomson has already been a victim of one attack. The government has no business now subjecting him to an assault upon his liberty." National Post, A10

Red Deer man's death linked to 'bad' ecstasy

A 38-year-old man from Red Deer died last month after taking ecstasy that may have contained a chemical linked to other deaths in Alberta and British Columbia, police say. The man was taken to hospital on Dec. 10 after he took what was believed to be ecstasy, RCMP said in a news release. Preliminary toxicology results from the medical examiner's office show that the dominant drug in the man's body was paramethoxymethamphet-amine (PMMA), a chemical linked to the deaths of at least six people in Calgary who took ecstasy before they died. Police said the final results from the autopsy are not yet available. It is not known where the man purchased the ecstasy, said Cpl. Kathe Deheer with the Red Deer RCMP. Edmonton Journal, A5; * Calgary Sun * Calgary Sun; * Calgary Herald; * Times & Transcript; * Yellowknifer; * Red Deer Advocate; * Edmonton Sun; * Edmonton Sun

Gangs catch eye of cops
A spike in the number of shootings in the city has police extending a crackdown on gun violence in Ottawa. Extra officers assigned to help the police's guns and gangs unit investigate a surge in gunplay across the city in recent weeks was supposed to end on Tuesday. But with six shootings and three stabbings (not counting a homicide) since the start of January, the 60-day campaign is being extended another 30 days, until March 1. Ottawa Sun, 11

*** Keep meetings in committee**
A letter to the editor states, "Senator Colin Kenny's point that only about two dozen parliamentarians "have expressed serious interest in security issues," is in itself reason enough to deny him a meeting with the RCMP commissioner. If we run a democratically elected government, which we do, then I submit that parliamentary committees should be where and when the RCMP commissioner meets and not with individual members of the Commons or Senate..." Toronto Star, A24

*** Report slams Mounties' treatment of suspect**
The RCMP watchdog is blasting cops in B.C. for "excessive" use of Tasers on a suspect in custody who later died. Seven officers from the Prince George RCMP were involved in the arrest and transport of Clay Alvin Willey on July 21, 2003. Willey was pepper-sprayed, punched, kicked, hog-tied, dragged face-down across a concrete floor and stun-gunned by two officers simultaneously. The Commission for Public Complaints Against the RCMP found that the use of force by constables John Graham, Holly Fowler and Kevin Rutten during the initial arrest -- including the pepper- spraying and hog-tying -- was "reasonable under the circumstances." Edmonton Sun, 26 (London Free Press); Toronto Star; The Province; Times Colonist

*** Ex-Mountie accused in theft**
RCMP in Cranbrook have charged a former Mountie with theft under $5,000 after a seized laptop went missing. At a press conference Tuesday in the B.C. town, about 390 km southwest of Calgary, Supt. Mike Sekela said the former member -- then a constable -- was suspended from duty in October when the investigation was launched and he resigned in December. The investigation stemmed from a complaint in October made by a pawn shop owner who called police asking for the return of a laptop seized by the former officer. Calgary Sun, 16

*** *Mountie latest to call photo radar mere cash grab***
A retired Mountie vows he won't set foot in Winnipeg again until he has to show up for his day in court to fight two traffic tickets totalling $600 -- fines he claims go more to pad Mayor Sam Katz's pledge to freeze property taxes than road safety. Arborg resident David Sigvaldason, who served 12 years with the RCMP in British Columbia before setting up a business in the Interlake town, also said the city's ongoing debate about photo radar and police speed traps is a black eye for the city. Winnipeg Free Press, A4

*** Le registre des armes à feu n'est pas la solution**
Un piece d'opinion déclare, « Je suis une mère de famille, propriétaire d'une arme à feu, tireuse sportive, chasseuse, diplômée du CÉGEP, j'ai un bon travail et, surtout, je suis une personne respectueuse des lois. Je suis celle qui prône la tolérance et la non-violence. Je compatis et suis sensible à la douleur des victimes de violence et leurs familles...Commençons par le plus simple : le coût. Les partis d'oppositions et autres groupes de défense du registre des armes à feu répètent sans cesse que le coût du registre est marginal, soit environ 2 à 4 millions par année...J'aimerais que les gens fassent preuve de professionnalisme et soient critiques face à l'information véhiculée, quitte à la vérifier par eux-mêmes. Faites votre propre analyse objective des faits même si je sais bien que ce n'est pas le point fort de notre société. J'espère juste que d'ici là cesseront la désinformation et les campagnes de peur et que je pourrai continuer à pratiquer le tir, sport qui après tout est assez noble pour être aux Olympiques. » La Tribune, 17

*** Seized pot plants worth $416K**
Winnipeg police seized $416,000 worth of marijuana plants in a bust Sunday night. They raided a home in the 400-block of Agnes Street around 8:30 p.m. Jan. 29, seizing 372 pot plants and $10,000 in grow op equipment. No arrests were made in the bust. Winnipeg Sun, 13

*** Civilian oversight of police a must**

The continuing fall-out over the violent arrest of Adam Nobody during the G20 raises serious doubts about the adequacy of civilian oversight of the police. Eighteen months later, one officer, Const. Babak Andalib-Goortani, has been charged criminally with assault by the province's Special Investigations Unit (SIU). Another provincial body, the Office of the Independent Police Review Director (OIPRD) has recommended Andalib-Goortani and four others--Constables Michael Adams, David Donaldson, Geoffrey Fardell and Oliver Simpson, face disciplinary charges. Toronto Sun, 20

*** B.C. Mountie suing RCMP legal-aid society**
A B.C. Mountie who is suing the RCMP over a series of alleged sexual assaults at the hands of a male colleague has filed a new lawsuit. Karen Katz is taking a society that funds legal aid for Mounties to small claims court for failing to help her in her sexual-assault suit in B.C. Supreme Court. In the new writ filed in small claims court, Katz, a Mountie since 1988, says that since 1998 she has been a member of the Mounted Police Members Legal Fund, a registered society that boasts nearly 17,000 members. The Province, A12

*** Changes for Crown prosecutors in rural areas**
A recent organizational change involving Crown prosecutors who work in rural communities around Calgary should help enhance the working relationship with RCMP officers, say officials. Under the newly created Calgary Rural and Regional Response Office prosecutions branch, prosecutors in rural areas, what is called the "circuit unit," are now permanently assigned to the district courts. Calgary Herald, B2

*** CMP dog taken out of service after mauling**
An RCMP dog handler has been placed on administrative duty and his dog taken out of service while an investigation into a mauling of a North Surrey teen is undertaken. Police were called to a break-in at a gas station in the area of the 14900-block 108th Avenue in Surrey at 2 a.m. on Saturday. A few dozen energy drinks were allegedly stolen. The handler, who has 8½ years of experience in the RCMP and 16 months of experience as a handler, was able to track a suspect. The Province, A4; The Guardian

*** Penhold gains satellite RCMP office**
Innisfail detachment has 10 officers, a schools resource officer and two corporals. A vacant staff sergeant position has not yet been filled. A corporal and four officers are responsible for rural areas, but Penhold is regularly patrolled by any officers available. The Town of Penhold is making space for an RCMP satellite office. In a move to save residents the drive to the Innisfail detachment for minor police business, Penhold is donating office space at the multiplex for a part-time RCMP office. Red Deer Advocate, C2

*** Saisie de chandails du Canadien**
Les policiers de la Gendarmerie royale du Canada (GRC) ont saisi près de 1 000 articles de mode contrefaits, dont des imitations de chandails officiels du Canadien de Montréal et des anciens Nordiques de Québec, hier avant-midi, dans un commerce de Rivière-du-Loup, dans le Bas-Saint-Laurent. Journal de Montréal, 18

*** Crown surprises defence with take on gun law**
Canada's laws on the storage and handling of guns and ammunition are so complicated that a veteran judge needed to adjourn court to allow two experienced lawyers more time for legal arguments and a search of case law to help parse and dissect them. It was a dud of an ending after two days of trial in the case of Ian Thomson, a 54-year-old Port Colborne man who fired three shots from a legally owned gun to scare off three masked men who were firebombing his secluded farmhouse while one threatened: "Are you ready to die?" National Post, A5

*** Québec suggère une médiation**
Le gouvernement du Québec veut nommer l'ex-juge Louise Otis comme médiatrice auprès des Hurons-Wendat et des Innus de Mashteuiatsh, qui se disputent la réserve faunique des Laurentides. Les premiers sont d'accord, les seconds posent leurs conditions. Le ministre responsable des Affaires autochtones, Geoffrey Kelley, a lu le rapport du juge à la retraite John Gomery sur les accrochages entre les deux nations pendant la saison de chasse à l'orignal. Bien qu'il juge "ordinaire" que M. Gomery ait distribué des blâmes au gouvernement provincial et au fédéral aussi sans avoir recueilli sa version des faits, le ministre s'est servi des conclusions pour demander aux chefs impliqués de baisser le ton. Le Quotidien, 4

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Officer 'grief-stricken' over probe delay
Wracked by personal grief and disillusioned by a loss of confidence in the Vancouver Police Department and RCMP, Vancouver police Det. Const. Lori Shenher broke down on the stand at the Missing Women's Commission of Inquiry on Tuesday. Shenher's two days of testimony painted a very grim picture of policing in the Lower Mainland, suggesting badly

flawed efforts by the VPD and RCMP, which possibly allowed drug-addicted prostitutes to die needlessly. Leader-Post, A7 (Starphoenix, The Province, Times Colonist, Starphoenix); Globe and Mail; National Post; Windsor Star; * Vancouver Sun; * Waterloo Region Record (Red Deer Advocate, Whitehorse Star)

*** A killer in plain sight**
An editorial states, "The heartbreak just never ends for family and friends of Robert Pickton's murder victims. This week Vancouver Police Det. Const. Lori Shenher provided some of the most graphic testimony yet that police had Pickton squarely in their sights as a potential serial killer for years before he was finally charged...Victims' families deserve the truth, however painful. And the public needs to know that police have learned the appropriate lessons." Toronto Star, A24

*** World-class incompetence**
An opinion piece states, "For revelations of incompetence, ineptitude and sheer professional bumbling, it would be difficult to top the details emerging from the inquiry into police handling of the Robert Pickton case. The evidence says it all, and it is coming from the mouths of the very people who handled the case. Detective-Constable Lori Shenher says she realized quickly that Pickton was probably the serial killer who was murdering Vancouver area women when she got involved in the case in the summer of 1998. "I thought, 'Bingo, this is the kind of guy we're looking for,' " she told the inquiry on Monday...It doesn't require "the benefit of hindsight, and when measured against today's current investigative standards and practices," to appreciate how appallingly police mishandled virtually every aspect of the Pickton murders. As ineptitude goes, this was world class. It should be matched by an equal level of shame on the part of police, but so far there's no sign it is." National Post, A12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** Human trafficking haven seeks funds**
Red Deer may soon be home to a safe haven for victims of human trafficking in Canada. The doors could be open as early as September, should funding come through in the next federal budget or other avenues, says David Bouchard, president of the city's Magdalene House Society. Human trafficking is the illegal trade of human beings for slavery, sexual exploitation or forced labour. Red Deer Advocate, C2

*** Seize ans de prison pour contrebande de comprimés d'ecstasy**
Une Canadienne qui s'est fait prendre à tenter d'entrer aux États-Unis avec plus de 70 000 comprimés d'ecstasy a été condamnée lundi à près de 16 ans d'emprisonnement. La Montréalaise Tara Haynes, 34 ans, a été reconnue coupable en août de contrebande de comprimés d'une substance contrôlée. Le Soleil, 11 (L'Acadie Nouvelle)

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Province touts tuition squeeze
Ontario's post-secondary education minister took the feds to task Tuesday, as he promoted a new initiative to trim students' tuition. "I would love to see a national education and training strategy under the federal government," said Glen Murray during a press conference at Algonquin College. "I wish they paid as much attention to this as they did to prisons." Murray said the federal government could make a big difference to students if the $10 billion it put into prisons was invested in education instead. Ottawa Sun, 8

*** Feces, urine attacks against guards on rise**
Guards at B.C. jails say they are increasingly being targeted in a new kind of attack - where inmates are throwing feces and urine at them. Vancouver Sun, A6

*** Police 'Whitewash' stats, study says**
The majority of Canadian police forces are "whitewashing" crime statistics by refusing to provide information about the race of people they come into contact with, says a new report by two Ontario criminologists. Toronto Star, A8

*** Woman who chopped up roommate to appear before National Parole Board**
A Calgary woman convicted of chopping her roommate to death with an axe and concealing dismembered body parts in boxes is going before the National Parole Board today. Calgary Herald, B1

*** High-risk sex offender coming to 'Peg: cops**

Police are warning that convicted sex offender Brett Russell Jeffrey Pilch, 46, is being released from prison and moving to Winnipeg. Pilch has a history of sexually harassing women he doesn't know, police say. Females are also at risk of possible physical sexual violence. Winnipeg Sun, 14

*** No parole for 17 years for beating boss to death**
Parole ineligibility was set at 17 years Tuesday for a young Kitchener man who beat his boss to death as he slept more than four years ago. Cory-James Kaufmann, 23, pleaded guilty last November to second-degree murder in the death of Ray Wechzelberger, 59, in September, 2007. He was automatically sentenced to life in prison. At his sentencing hearing, Justice Steve Glithero decided he cannot apply for parole for 17 years from the date of his arrest, which would be in 12 years and eight months. The Record, B1

*** Report cites web of deceit, scant signs of remorse**
Ian Thow's history of deceit, lack of remorse and an inadequate plan for life after prison combined to keep the former investment adviser behind bars for at least another year, according to a National Parole Board report. Times Colonist, A1

*** ROPE squad tracks offender to Six Nations**
A federal offender, wanted on a Canada-wide warrant for breaching his parole, has been located by police on Six Nations. Nicholas Hill, 25, was arrested around 1 p.m. Tuesday by the Repeat Offender Parole Enforcement (ROPE) Squad. Hamilton Spectator, A2

*** Crime 'fix' primitive, pointless**
An opinion piece states, "Governing based solely on perceptions of public sentiment is a little like playing chess with yourself: You can never actually win without also losing... Statistics Canada continues to report that overall rate of offence is 17 per cent lower than it was a decade ago, a finding that recently moved Steve Sullivan, executive director of Ottawa Victims Services, to suggest that "if the government is telling taxpayers it is going to spend millions and billions of dollars on getting tough on crime, I think it at least has to have some evidence that it is addressing a real problem. Neither these statistics nor the other surveys we have would suggest that we are in some kind of crime wave." And yet, at a time when the feds are looking for billions of dollars in spending cuts (and will likely find them by laying off thousands of public employees and tinkering with old age security), the budget for Correctional Service of Canada is expected to jump to $3.1 billion by 2013, or roughly 90 per cent since 2006..." Times & Transcript, D6

PUBLIC SERVICE / FONCTION PUBLIQUE

Pension row could be diversion
It might just be my overly suspicious nature, but has anyone else considered that Prime Minister Stephen Harper's so-called assault on public pensions is really about something else? The StarPhoenix, A10

*** PMO staff salaries sought**
The federal NDP is calling on Treasury Board president Tony Clement to bring the same light to salaries in the Prime Minister's Office as the government shone on the highly paid staff at the CBC. The government on Monday introduced a written response to a written question from an MP who asked for salary details of top CBC executives and on-air staff. The response indicated more than 700 CBC staff earn $100,000-plus annually, though it did not provide the names MP Brent Rathbeger had asked for before Christmas. He also had asked for the pay levels of CBC newscaster Peter Mansbridge and host George Stroumboulopoulos, but those were not provided. Clement declined to give the total number of $100,000-plus salaries in the PMO. Victoria Times-Colonist, A8 (Ottawa Citizen); Toronto Sun (Winnipeg Sun; London Free Press; Ottawa Sun; Edmonton Sun)l; National Post

*** Tories won't commit to MP pension cuts - All spending will be reviewed, government says**
The federal Conservative government won't commit to scaling back lucrative pensions for MPs, as it searches for billions of dollars in cuts to federal programs and considers overhauling Old Age Security. Federal politicians of all stripes are under increasing pressure to take a haircut on what spending watchdogs call a "goldplated" pension plan, especially as government reins in expenditures to help eliminate a $31-billion deficit by 2015-16. The final decision on politicians' pensions falls with Treasury Board president Tony Clement, who said Tuesday all spending - including pensions for MPs - will be examined. But the government refuses to commit to cutting pension benefits for parliamentarians. Victoria Times-Colonist, B4 (Calgary Herald; Fredericton Daily Gleaner; Moncton Times and Transcript; Winnipeg Free Press)

*** Reform MPs' pensions first**
An opinion piece states "It might be understandable if a number of Canadians didn't appreciate Prime Minister Stephen Harper talking recently about reforming public sector pensions and Old Age Security (OAS) social assistance payments. After all, nobody likes the idea of their retirement plans changing, whether it is by way of a downturn in the market or a

change in a government policy. This is likely especially true recently, with Harper's musings coming on the heels of two reports on MP pensions, one by the not-for-profit Canadian Taxpayers Federation and the other from the esteemed C.D. Howe Institute. What these reports made abundantly clear is, Harper must reform MPs' pensions first, if he has any hope of looking at anyone else's. Canadians have been phoning, writing, and emailing their politicians in huge numbers, letting them know how they feel about platinum-plated MP pensions. With the next federal budget coming soon, taxpayers need to turn up the heat, and make sure the pork-laden MP pension plan is put on the chopping block, front and centre, with a big carving knife close at hand for Harper. It's the necessary first step in long, but ultimately needed, process." Waterloo Region-Record, A7

*** CBC mum on who's paid what**
The CBC pays 730 staffers more than $100,000 in salary per year, but won't say who they are. "Their salary information is also protected in accordance with the federal Privacy Act," wrote Heritage Minister James Moore in response to written questions in the House of Commons. When the Tory MP tabled his CBC questions, the NDP countered with a question about salaries of staffers in the Prime Minister's Office. Treasury Board president Tony Clement responded that PMO pay is comparable to the public service. Edmonton Sun, 28 (Ottawa Sun, London Free Press, Winnipeg Sun)

*** Arbitration awards hit taxpayers hard**
The key to Premier Dalton McGuinty's success in getting re-elected three times is this: He takes the line of least resistance. The best example is the way the government's dealt with public sector union pay demands. Ottawa Sun, 15 (Toronto Sun)

*** Canadians need pensions like their public servants**
A letter states, "Barbara Yaffe does a great disservice rolling together her criticism of MP and public service pensions. As her own figures show, members of Parliament contribute four per cent toward their plan while public servants contribute 35 per cent. Further, the government has raised public employee contributions to bring their share up to 40 per cent by 2013..." Vancouver Sun, A10

INTERNATIONAL / INTERNATIONAL

*** Man relocated to United States now facing terrorism charge**
A man from Uzbekistan whom the United States and the United Nations helped relocate to the Western U.S. state of Colorado was arrested Jan. 21 and now faces a terrorism charge. Jamshid Muhtorov opposed his home country's dictator following a 2005 massacre, endured a brutal detention, and saw his sister arrested on a false murder charge. The Record, A4

*** Iran has means to build bomb, but hasn't decided to do so yet, say U.S. intelligence officials**
Top U.S. intelligence officials on Tuesday asserted that Iran has the means to build a nuclear weapon but has not yet decided to follow through, in contrast to Israel's insistence that time is running out to stop Iran from developing such a weapon. Red Deer Advocate, D5

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Pages 1895 to / à 1902
are withheld pursuant to sections
sont retenues en vertu des articles

20(1)(b), 20(1)(c)

of the Access to Information
de la Loi sur l'accès à l'information

Page 1903

is withheld pursuant to sections

est retenue en vertu des articles

19(1), 20(1)(b), 20(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 1904 to / à 1998
are withheld pursuant to sections
sont retenues en vertu des articles

20(1)(b), 20(1)(c)

of the Access to Information
de la Loi sur l'accès à l'information

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-02-12 9:05 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: ADDENDUM: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 2, 2012 / le 2 février 2012

Online Media / Médias en ligne

Hacked neo-Nazi websites reveal Canadian connections
The names of dozens of alleged white supremacists in Canada are contained in files leaked by computer hackers in Europe intent on exposing hate movements, CBC News has learned. The alleged white supremacists' names were revealed earlier this month by members of a loose-knit group of hackers called Anonymous on a website called nazi-leaks.net, which is now offline. CBC News

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From: Beaudoin, Luc
Sent: February-03-12 1:13 PM
To: Cameron, Bud; Turbide, Frank
Cc: Bendelier, Kenneth
Subject: Re: Well, if anyone is looking to understand Anonymous TT&P

Add a + at the end of the goo.gl link for more info...

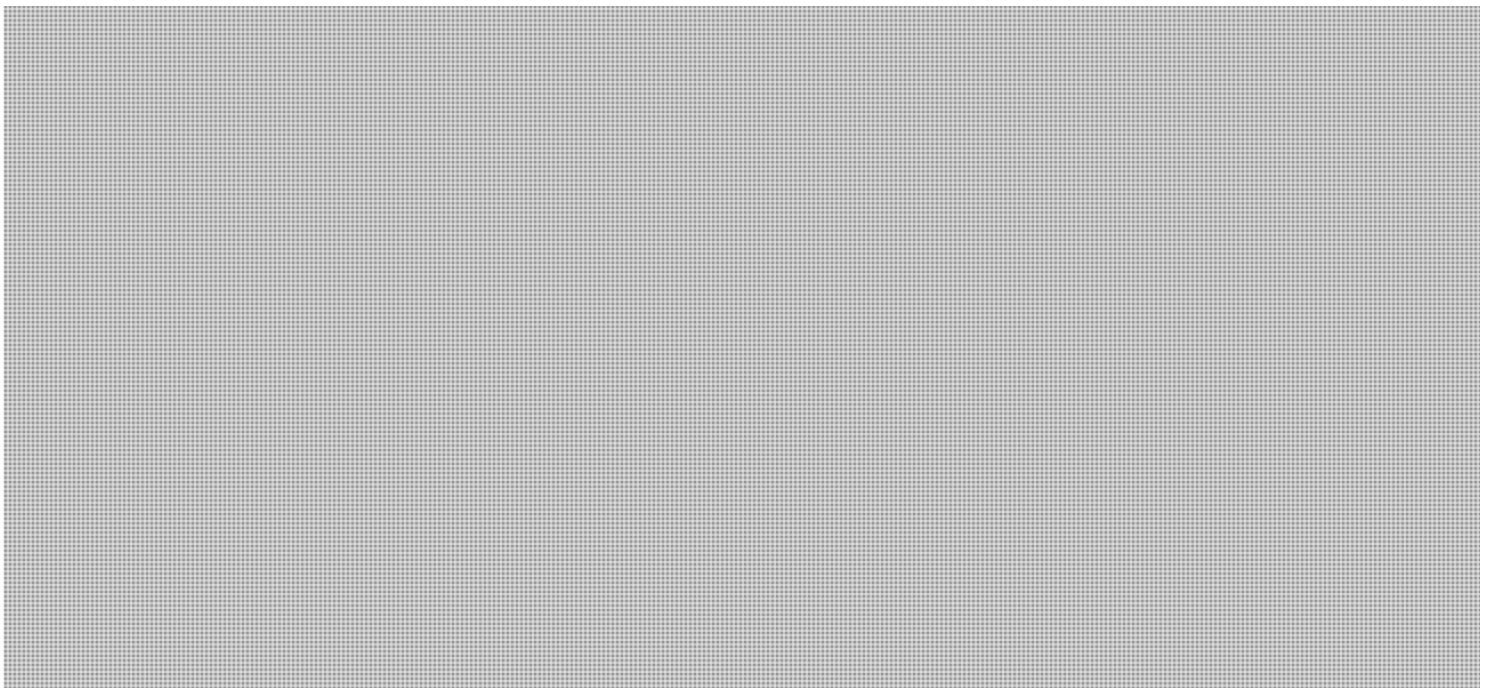
Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: Cameron, Bud
Sent: Friday, February 03, 2012 11:32 AM
To: Beaudoin, Luc
Cc: Bendelier, Kenneth
Subject: RE: Well, if anyone is looking to understand Anonymous TT&P

Seems like Ken is awfully knowledgeable about the inner workings of Anon.
Should we turn him in?

From: Bendelier, Kenneth
Sent: February-03-12 9:08 AM
To: *
Subject: Well, if anyone is looking to understand Anonymous TT&P



Pages 2001 to / à 2002

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-993-5042
Facsimile | Télécopieur +1 613-954-3097
Kenneth.Bendelier@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

s.16(2)(c)

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

Williston, Sandra

From: Beaudoin, Luc
Sent: February-03-12 10:38 AM
To: CYBERDO
Subject: Anonymous released fbi

s.15(1) - Int'l
s.16(2)(c)

[redacted]. This was on a maillist... Could be interesting
>
[redacted]

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-03-12 8:35 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted]; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 3, 2012 / le 3 février 2012

Online Media / Médias en ligne

Neo-Nazi member calls hacking 'an invasion of privacy'
Some Canadians whose associations with white supremacist and neo-Nazi groups were recently revealed, are defending their involvement with the organizations, while others deny having anything to do with the groups anymore. CBC News reported Wednesday that the names of 74 Canadians were found in files leaked by computer hackers in Europe who were intent on exposing hate movements. The identities were revealed on a website called nazi-leaks.net, which is now offline. "It is an invasion of privacy," said Joel Henry, of Langley, B.C., in a telephone interview with CBC News Thursday. Police and government security organizations should be able to make use of the hacked information, according to Simon Fraser University professor Andre Gerolymatos, who has written extensively on espionage. CBC News; Yahoo! News Canada

FBI: Cyber threat might surpass terror threat
Today, FBI Director Robert Mueller told the U.S. House Permanent Select Committee on Intelligence that he believes "the cyber threat will equal or surpass the threat from counter terrorism in the foreseeable future." He elaborated on the breadth of the threat, saying "there is very little we do in this day and age that is not on or somehow associated with the internet. The theft of intellectual property, the theft of research and development, the theft of the plans and programs of a

corporation for the future, of all which are vulnerable to being exploited by attackers." On Tuesday, Mueller testified at the Senate Select Intelligence committee's hearing on worldwide threats. He had similar warnings about cyber security, and elaborated on three ways the FBI and intelligence agencies need to address the concern. CBS News; Infosecurity Magazine

Intelligence Leaders Urge Congress to Act on Cyber Laws

The threat to U.S.-based computer networks is one of the country's most pressing security problems, and Congress needs to act on it soon, the director of national intelligence told a congressional panel today. James R. Clapper Jr. said he and all of the U.S. intelligence leadership agree the United States is in a type of cyber Cold War, losing some $300 billion annually to cyber-based corporate espionage, and sustaining daily intrusions against public systems controlling everything from major defense weapons systems and public air traffic to electricity and banking. Clapper was joined by CIA Director David H. Petraeus, Defense Intelligence Agency Director Army Lt. Gen. Ronald L. Burgess Jr. and FBI Director Robert S. Mueller for a House Select Intelligence Committee hearing on worldwide threats. He urged lawmakers to pass a bill that forces intelligence sharing between the government and the private sector, such as the Defense Industrial Base pilot program that then-Deputy Defense Secretary William J. Lynn III launched last year. U.S. Department of Defense News Release

Security Slackers Risk Internet Blackout on March 8

Companies and home users whose computers or routers are infected by the DNSChanger Trojan risk being unable to access the Web come March 8, 2012. That could represent a substantial number of users, too, as half of Fortune 500 companies and government agencies are infected with the malware, according to a new report. Back in November, the feds famously took down the DNSChanger botnet network, which a cyber criminal gang was using to redirect Internet traffic to phony websites that existed simply to serve up ads. The feds replaced the criminals' servers with legitimate ones that would push along traffic to its intended destination. That surrogate network was supposed to be temporary -- in operation just long enough for companies and home users to remove DNSChanger malware from their machines. Said network is slated to be unplugged on March 8. Once the surrogate server network is unplugged, computers infected with DNSChanger will not be able to access the Internet: The malware will send requests to servers that will no longer be online. PC World; BCS

Symantec warns of Android Trojans that mutate with every download

Researchers from security vendor Symantec have identified a new premium-rate SMS Android Trojan horse that modifies its code every time it gets downloaded in order to bypass antivirus detection. This technique is known as server-side polymorphism and has already existed in the world of desktop malware for many years, but mobile malware creators have only now begun to adopt it. A special mechanism that runs on the distribution server modifies certain parts of the Trojan in order to ensure that every malicious app that gets downloaded is unique. This is different from local polymorphism where the malware modifies its own code every time it gets executed. Symantec has identified multiple variants of this Trojan horse, which it detects as Android.Opfake, and all of them are distributed from Russian websites. PC World Australia

MSUpdate trojan attacked companies in the defence sector

Unknown attackers have tried to use an invitation to a prestigious conference to inject a trojan into companies in the defence sector. The security firms Seculert and Zscaler report that opening an attached PDF flyer caused recipients' computers to be infected with spyware via a previously undisclosed hole in Acrobat Reader. According to the report, the attack mainly targeted government-related organisations, including military and aerospace contractors, in Europe and in the US. The security firms said that the attacks started back in 2009 and peaked in autumn 2010. Talking to The H's associates at heise Security, Seculert CTO Aviv Raff added that compromised computers, some of which had been infected for two years, were only discovered a few weeks ago. A zero day hole in Adobe Reader was exploited to inject the msupdater.exe trojan into systems; once injected, the trojan did its best to look like a regular update process... The H Security; Infoboom; CIO Insight

Trojan found breaking Yahoo CAPTCHA security in minutes

Researchers have discovered a malware engine that appears to be able to break the CAPTCHA security used by Yahoo's webmail service after only a handful of attempts. There is nothing new in malware that tries to break CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) - a low-level war has been ongoing since this type of security was first implemented almost a decade ago - but what matters is how quickly and invisibly this can de done. Websense has posted an online video showing the effectiveness of the engine it found working as part of the Cridex banking Trojan malware in breaking down Yahoo's CAPTCHA process. Cridex itself is a traditional if rather dangerous login harvester that targets online banks and social media sites from victim PCs, uploading stolen data to a command and control server. PC World New Zealand

Drive-by Downloads Observed in Over 50% of Malware Assaults

Sophos the company for data protection and IT security, which released its new "Security Threat Report 2012," evaluates in detail the threat scenario starting with hacktivism as well as notes that over 50% of malware assaults against Web-surfers currently comprise drive-by download assaults. Specifically as per the report, a certain attack code for drive-by download is responsible for 31% of the total assaults over the Web spotted during H2-2011. SPAM Fighter

Brazil-Focused Hackers Hit HSBC's Global Banking Sites
Hackers on Thursday kept up their campaign to cripple Brazilian banking websites and, in a new twist, their efforts appeared to affect both local and global websites of U.K.'s HSBC Holdings PLC. This is the fourth attack in as many days by the Anonymous Brasil group, which says the effort is part of a campaign aimed at social activism in Brazil, and not theft. Earlier this week, the attacks hampered operations on the websites of Banco do Brasil SA, Itaú Unibanco Holding SA and Banco Bradesco SA. A spokesman for HSBC in New York confirmed the bank experienced "technical difficulties" with some of its websites, but said the issues are now resolved. The issue was part of the "unauthorized Internet activity" in Brazil that affected the North American sites, he added. But "customer accounts have not been compromised in the U.S. or Canada," the spokesman said. Wall Street Journal

Android Bouncer boots out 40 per cent of malware
The Android Market, like Newcastle's Bigg Market, is getting too rowdy, but with malware and viruses instead of Scouse hen parties. Now Google's Bouncer is manning the doors, looking for potential troublemakers and booting out offending apps. Google says it's been working on Bouncer for several months now -- and the search giant already claims to have achieved a 40 per cent drop in malware. Bouncer scans both new and existing apps for spyware and trojans that could steal your data or mess with your phone, as well as monitoring the behaviour of developers so it can kick out offenders and stop them from coming back. It also virtually runs all apps on the market to see how it would perform on an Android device. If it detects a new type of threat, it rescans everything to see if it's present elsewhere. CNet; Computerworld; The H Security; Wall Street Journal

Banking malware 'a growing threat', as new variant of Zeus is detected
Malware that steals users' identity and empties their bank accounts has been cited as a growing threat to Britain. According to Parliament's Science and Technology Select Committee report, which was released this week, a lack of awareness is to blame and it called for greater use of the Get Safe Online website. The report claimed that infection with malware takes cyber crime to a different level as "experts use their technical skills to, among other things, take over computers worldwide to steal bank details and identity information". It also claimed that Dr Richard Clayton, research assistant at the University of Cambridge who was involved in gathering the research, did not believe it was possible to bring the population up to the level of technical knowledge required to defend itself; instead we needed to "rely on those who make the software to adapt it in such a way that you no longer need to read the URL in order to be safe". SC Magazine UK

Hackers manage to outsmart online banking security systems
They use the Man in the Browser (MitB) scheme to steal account holders money. Hackers have started targeting banking institutions by managing to outwit the latest online banking security techniques. The hackers fool the account holders with an offer of training in a new "upgraded security system" after being logged into the bank's real site. They later move out the money out of the account holders, without leaving any traces of evidence to the user about the theft, according to the BBC. This method of victimising users, which has been dubbed the Man in the Browser (MitB), uses malware to manipulate what is seen on the screen or keyed in by the user. CBR Online

Sophos says Counterclank is not Android malware
SECURITY OUTFIT Sophos has classed the controversial Counterclank Trojan as advertising not malware. At the beginning of the week Symantec revealed the Counterclank Trojan, which it claimed was the biggest malware distribution of the year. Mobile security firm Lookout disagreed, saying it was just an aggressive form of an ad network, an assessment with which Sophos agrees. Symantec found the code present in 13 apps on the Android Market and classed it as malware because it sends information about the phone to a remote server called Apperhand. Vanja Svajcer, principal virus researcher at Sophos said, "It turns out that the Apperhand framework is related to an advertising framework used more than half a year ago by the Plankton app." The Inquirer; PC Magazine

Kelihos botnet makes a comeback
A once-dead botnet has been resurrected and resumed its spamming ways. The original Kelihos botnet compromised only about 41,000 computers but was capable of sending 3.8 billion spam e-mails each day promoting unregulated pharmaceuticals, fraudulent stock scams and, in some cases, sites dealing with sexual exploitation of children. Microsoft and Kaspersky Lab took down the malware last September using a "sinkhole" technique that tricked the infected computers into getting their instructions from a computer the companies controlled. However, while the technique was effective at disabling the botnet quickly, it was merely a temporary fix as many computers remained infected, and "as this particular case showed, it is not very effective if the botnet's masters are still at large," Kaspersky Lab's Maria Garnaeva

said in a blog post. "Our investigation revealed that the new version appeared as early as September 28, right after Microsoft and Kaspersky Lab announced the neutralization of the original Hlux/Kelihos botnet." CNet

Facebook, Microsoft, Google, Yahoo team up for anti-phishing standards

Fifteen tech giants and email service providers have put their heads together to combat phishing, the practice of sending a deceptive email that spoofs a legitimate entity. The Domain-based Message Authentication, Reporting and Conformance (www.dmarc.org) has developed standards to combat the threat from phishing as well as spam. DMARC.org said it "draws upon a history of private industry collaboration with 18 months of dedicated work, to outline an enhanced vision for email authentication that can scale up to today's Internet needs." DMARC.org is an unincorporated working group made up of 15 of the world's leading email providers, financial institutions and service providers, including: AOL, Gmail, Hotmail, Yahoo! Mail (email), Bank of America, Fidelity Investments, PayPal (financial institutions), American Greetings, Facebook, LinkedIn (social media properties), Agari, Cloudmark, eCert, Return Path, and Trusted Domain Project (email security solutions providers). The group aims to develop Internet standards to reduce the threat of email phishing and to improve coordination between email providers and mail sender domain owners. GMA News; Sophos

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Bendelier, Kenneth

From: Bendelier, Kenneth
Sent: February-03-12 9:08 AM
To: [redacted]
Subject: Well, if anyone is looking to understand Anonymous TT&P s.16(2)(c)

Description:
6 FEBRUARY 15 Action against Mining and Energy companies in South America.

[redacted]

Pages 2011 to / à 2012

are withheld pursuant to section

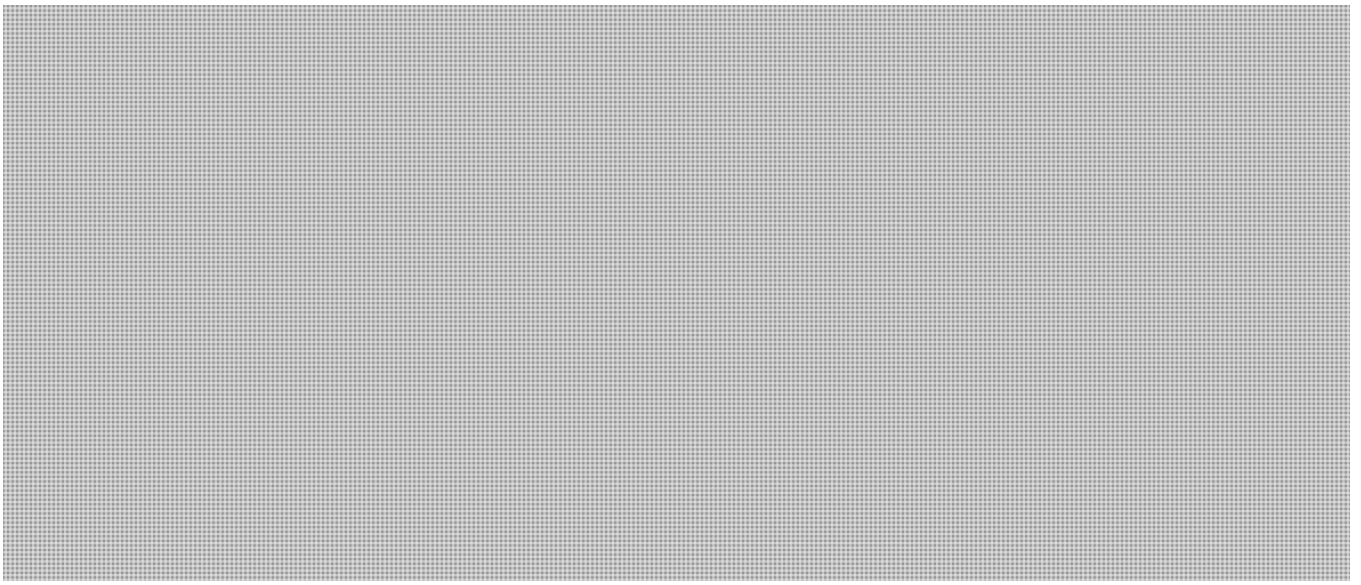
sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

s.16(2)(c)



Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-993-5042
Facsimile | Télécopieur +1 613-954-3097
Kenneth.Bendelier@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

Bendelier, Kenneth

From: Beaudoin, Luc S
Sent: January-24-12 1:08 PM
To: Beaudoin, Luc S
Subject: JS LOIC
Attachments: SAR-12-12-021-01 - Anonymous response to the seizure of MegaUpload2.pdf

Very interesting report by US-CERT on recent anonymous activities and the use of JS LOIC.

Distribution is GREEN (ie: OK to share with need-to-know partners but not to post publicly)

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Bonvie, Jeff

From: Bonvie, Jeff
Sent: February-03-12 1:49 PM
To: Grigsby, Alexandre; Dvorkin, Corey; Bradley, Kees
Subject: Oops...

If you didn't see this previously...

http://www.wired.com/threatlevel/2012/02/anonymous-scotland-yard/

Williston, Sandra

From: Luc Beaudoin <[redacted]>
Sent: February-04-12 11:45 AM
To: [redacted]
Cc: Beaudoin, Luc
Subject: FBI and Anonymous

s.16(2)(c)
s.19(1)

For RCMP attention/info.

I shoundn t but I wonder why they are not on this distro.

lessons learned: let s change our govIRT #code once in a while !

http://pastebin.com/[redacted]

[redacted]

Pages 2017 to / à 2018

are withheld pursuant to sections

sont retenues en vertu des articles

16(2)(c), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-04-12 10:37 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne - Final / Finale

Daily Media Summary / Revue de presse quotidienne
February 4, 2012 / le 4 février 2012

MINISTER / MINISTRE

NDP MP in hot water again for profanity-laced tirade
Winnipeg NDP MP Pat Martin added fuel to the obscenity-laden firestorm he created this week when he cursed at a Conservative senator who suggested murderers should be given ropes to hang themselves. On Wednesday, Martin cursed Sen. Pierre-Hugues Boisvenu sparking controversy. When demands for an apology were made Thursday, Martin refused. He added perhaps his only mistake was that he didn't include the required honorific when addressing a senator. Boisvenu triggered his own controversy with his comments Wednesday when he was asked about the government's omnibus crime bill, which gives stiffer penalties for certain violent crimes. Boisvenu is an outspoken victims' rights advocate. His daughter was raped and murdered by a repeat offender in Quebec in 2002. He was appointed to the senate in 2009. Manitoba Senior Minister and **Public Safety Minister Vic Toews** demanded Martin apologize. "***Pat Martin's constituents, and indeed all Canadians, would be better served if the MP and his soft-on-crime party, would direct their outrage and vitriol at the criminals who victimize innocent, law-abiding Canadians rather than at a senator whose family has suffered a terrible loss at the hands of a repeat offender***," **Toews said** in a letter to the editor. Telegraph-Journal, A9

Trotting out the bogeyman
An opinion piece states, ""***I don't know if the statistics demonstrate that crime is down ... I'm focused on danger.***" That's **federal Public Safety Minister Vic Toews**, speaking to the Senate Committee on Legal and Constitutional Affairs about the Conservatives' "tough on crime" legislation. If nothing else, the next few years are going to have more than their fair share of unintentional hilarity - because unless I completely misunderstood that particular quote, **Toews** has just confirmed what opponents of the new crime legislation have been saying all along. And that's that the legislation has nothing to do with crime, and everything to do with marketing... Rewind a little further, back to when **Vic Toews** actually did realize that statistics demonstrated that crime rates were down to levels last seen in the early '70s. (He must have since forgotten about those statistics, because he clearly doesn't know about them anymore.) He said that the Tory crime bill was to help address the increase in unreported crimes. "***We see this continuing trend of more and more crimes going unreported, and that ... I believe is an indication of a lack of confidence in the justice system***," **Toews** told CTV in September 2010. "***And that is why our government is taking the measures that we are taking.***" All right. To get this straight, then: it's the increase in unreported crime (that's a great thing to try and measure in any form - it's big, it's bad, it's ... unreported, hence statistically, well, void) and the increase in ... wait for it ... danger..." The Telegram, A20

Hat's not impressed with Tory justice
A satirical opinion piece states, "Mousie MacKay got a beer from the bar at Louie The Leggers and carried it over to the table where Hat McInnes was sitting, sipping on a beverage, and playing with a small computer... "No, the story I was referring to was the one where, once again the **minister of public safety**, boy, that's an Orwellian mouthful, **minister of public safety**. Anyway, yet another judge has criticized the minister for not allowing a Canadian in prison in the States to serve their time in a Canadian prison." "Seven years for a marijuana bust, that's pretty heavy," said Mousie, "But the Americans are paranoid about drugs. Can you imagine how tense things will get if the Liberals try to legalize marijuana? How come the government slammed the door on this guy, a bit of weed doesn't seem like a capital crime?" "That's one of the problems the judge had, **the minister** didn't really provide any reasons for his denial," said Hat, "so the judge has ordered **the minister** to review the case and provide some good reasons for denying the man a chance to serve his sentence in Canada." "So who stopped the marijuana guy from coming back to a Canadian prison?" asked Mousie. "That was **Vic Toews**, another guy who's made up his mind and doesn't want to be confused by the facts..." The Guardian, A15

One to watch...

A letter states, "Bill C-10: The crime bill. It's not so much the crime bill itself that needs watching; a minority of Canadian voters graciously granted Prime Minister Stephen Harper a majority government, so the bill will pass. What will be interesting to watch is how the bill will play out after it is passed. Even some Tory senators wonder why the Harper government is so fixated on crime, in light of statistics that show crime has actually been decreasing for quite some time. **Public Safety Minister Vic Toews** told a Senate committee reviewing the legislation: "***I don't know if the statistics demonstrate that crime is down. I'm focused on danger.***" **The minister** then went on to say his concern is that the public is in danger as long as criminals walk the streets, "***and this legislation addresses that.***" Given the statistical decline of murderers, rapists, violent robbers and other shady types, the question has to be asked: Who is **Toews** afraid of when he walks the streets of Canada? Panhandlers? Homeless people?" Winnipeg Free Press, J12

Have your say
A letter states, "OK, Pat Martin lips off again, and again **Vic Toews** runs to the media. He reminds me of a schoolyard child running to his teacher to tattle on another for saying a bad word. And for what? To say sorry? Really! Canadian politics has come down to this? Now that's obscene." Winnipeg Free Press, A17

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Despite weather, flood forecast in works
Manitoba Water Stewardship is working on a spring flood forecast despite this winter's mild and relatively dry weather. Provincial flood forecasters plan to unveil a preliminary flood outlook before the end of February, spokesman Paul White said Friday. Although much of southern Manitoba has experienced dry conditions since June, ground moisture levels -- one of the factors that increases the probability of localized or regional flooding -- remain significant in some areas of the province. While moisture levels are well below those recorded last winter, when the province began preparing for major spring flooding, conditions are comparable to the early months of 1997, the year of the Flood of the Century in the Red River Valley, White said. But across most of southern Manitoba, the snowpack -- another major factor in determining flooding -- is much lower this year. That can change significantly before the spring snowmelt, as one or two blizzards can be the difference between a major flood and no flooding whatsoever. Winnipeg Free Press, A13

B.C. avalanche kills man
One man is dead after a small group of recreational skiers got caught in an avalanche Friday morning on Meadow Mountain, near Kaslo, B.C. The man's name isn't being released until Mounties notify his family. The B.C. Coroner's Service and RCMP are still investigating the death. Windsor Star, A13; Edmonton Journal; * Vancouver Sun

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Conditions eased for suspect
Mohammad Mahjoub, a Toronto man detained and subsequently held under house arrest for the past 12 years on a national security certificate because of alleged terrorist ties, was granted more freedoms by a federal court Friday. Mahjoub, 51, was arrested in Toronto in 2000 on a security certificate, which allows the government to detain terror suspects indefinitely without charges or a trial. In his decision, Judge Edmond P. Blanchard said the federal government failed to provide "reasonable grounds to believe" that Mahjoub's security threat has not reduced. While Blanchard said there remains "compelling and credible evidence" that Mahjoub "poses a threat to the security of Canada," evidence during the latest review of Mahjoub's case and his current circumstances suggest that this threat "is now significantly diminished." Windsor Star, A13; National Post; The Telegram

Defenceless
Just what legally constitutes a foreign activity in Canada that is detrimental to this country's national security interests these days, anyway? As it turns out, Canada is practically incapable of answering that question with any enforceable coherence. When it comes to the recent and rapid-succession manoeuvres that have given Chinese state-owned entities the spigot key at critical flow points in Canada's oil and gas industry, mysteries abound. But it is now clear that slowly but surely, Canada's regulatory defences have been almost completely hollowed out. Way back in the 1980s, the Security Intelligence Review Committee was urging amendments to the Canadian Security Intelligence Service Act to spell out what Canadians mean when we talk about foreign-power connivings that are "detrimental" to Canada's national interests. "It is almost wholly subjective: no criteria are provided to offer any standard for determining what is 'detrimental'," a SIRC report once pointed out. The definitions in the CSIS Act still don't clearly define what "detrimental" means, but unlike Investment Canada, CSIS has muddled through and is properly content to couple Canada's "national security" with "the security and economic welfare of Canada." Ottawa Citizen, B7

Muslim group slams 'terrorist' treatment

A Canadian Muslim businessman became a terror suspect for telling sales staff in a text message to "blow away" the competition at a New York City trade show, an association said Friday. Moroccan-born Saad Allami was arrested three days after he sent the message in January 2011 and detained while police searched his home, said the Muslim Council of Montreal. Ottawa Citizen, A4; Le Soleil

MacKay quiet on iran plans
Regional troublemaker Iran poses "a grave threat to peace and security" and is "fanatical and dangerous," Prime Minister Stephen Harper said Friday. Harper made the comments during an interview with Postmedia, and warned that Iran would be ready to use a nuclear weapon if it was able to produce one. But in an interview with QMI Agency, Defence Minister Peter MacKay wouldn't speculate whether Canada -- a staunch ally of Israel -- would join that country in a possible strike against the Islamic regime. Toronto Sun, 24

CYBER SECURITY / CYBERSÉCURITÉ

Confidential police call hacked, leaked
Trading jokes and swapping leads, investigators from the FBI and Scotland Yard spent the conference call strategizing about how to bring down the hacking collective known as Anonymous, responsible for a string of embarrassing attacks across the Internet. Unfortunately for the cyber sleuths, the hackers were in on the call too - and now so is the rest of the world. Anonymous published the roughly 15-minute-long recording of the call on the Internet on Friday, gloating in a Twitter message that "the FBI might be curious how we're able to continuously read their internal comms for some time now." The humiliating coup exposed a vulnerability that might have had more serious consequences had someone else been listening in on the line. The leak was one of a slew of Anonymous hacks that hit websites across the United States Friday, including in Boston, where the police site was defaced, and in Salt Lake City, where officials said that personal information of confidential informants and tipsters had been compromised. Anonymous also claimed credit for defacing the Greek Justice Ministry's website and stealing a mountain of data from the Virginia-based law firm that defended a U.S. Marine recently convicted for his role in the bloody 2005 raid in Iraq that became known as the Haditha massacre. Red Deer Advocate, A5; * Ottawa Citizen

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

$1M worth of drugs, 13 charged in 'high-level' raid
Thirteen people alleged by police to be "high-level" drug dealers were charged Friday in connection with the latest large-scale sweep orchestrated by Manitoba's organized crime unit. Project Deplete, a police investigation that began last August and culminated Friday with arrests in Winnipeg and Edmonton, is the latest effort of Manitoba's Integrated Organized Crime Task Force, a joint RCMP-Winnipeg police unit that has famously used informants over the past several years to take down primarily the Hells Angels and their associates, with great success. The latest sweep saw charges laid against people police accuse of being major players in the city's drug trade. Some of the accused have gang associations, others are more "independent," police said. Winnipeg Sun, 2; * Winnipeg Free Press

*** Mountie pleads not guilty to assault**
A Rimbey RCMP officer who was suspended over criminal assault charges pleaded not guilty in Rimbey provincial court on Friday. A trial date of Oct. 2 was set for Const. Jesse Charles Lambright, 52, who was charged with assault and uttering threats in connection to an off-duty relationship. The officer was suspended from duty after the charges were laid. An RCMP code of conduct investigation was also suspended, pending the outcome of Lambright's criminal charges. Red Deer Advocate, A9

*** Toy gun prompts dramatic RCMP takedown at Subway**
A toy gun police say was altered to look like the real thing led to a standoff outside a Kelowna Subway restaurant Thursday. At about 1: 40 p.m., an RCMP officer conducting another surveillance operation at the Capri Centre Mall reported seeing a young man putting a gun into his sweatpants as he walked across the parking lot. RCMP followed the suspect, who was with a group of 12 young men and two women, as they made their way to a Subway food outlet. Staff were removed from the restaurant as police surrounded the site, and a RCMP helicopter circled overhead. Vancouver Sun, A12

DNR finds barrels of pot
Approximately 29 kilograms of marijuana has been seized following the discovery of the drug by New Brunswick Department of Natural Resources Conservation Officers. Last week, conservation officers were working on an illegal possession of moose meat investigation when they discovered the drug in a number of barrels in a wooded area near a

residence in Scoudouc. They then called the District 4 RCMP who began an investigation. Times & Transcript, A6; * L'Acadie Nouvelle

*** RCMP seize drugs at Truro bus terminal**
RCMP seized cocaine and prescription drugs during a bust Thursday at the Acadian Lines bus terminal in Truro. Mounties arrested a 43-year-old man from Cambridge, Ont., during the bust, which netted 825 grams of cocaine and about 400 oxycodone prescription pills. Sylvain Joseph Matte faces charges of possession of cocaine for the purpose of trafficking and possession of oxycodone for the purpose of trafficking. Chronicle-Herald, A5

Police make arrest and seize cocaine, marijuana
A 33-year-old Saint John man has been arrested after police seized a large amount of cocaine and marijuana from the city's east side. Russell William McCain of Canterbury Street faces a number of drug-related charges, police said in a release. McCain's arrest came after a three-month investigation by members of the Saint John Police Force street crime unit and the Fundy Integrated Intelligence Unit. The RCMP and the Rothesay Regional Police Force participated in the drug raid on Thursday. Telegraph-Journal, B3

*** Alleged pimp faces human trafficking rap**
A 42-year-old Hamilton man is facing a litany of charges, including human trafficking, for allegedly coercing women into prostitution. Police claim the man is a pimp who used threats of violence, intimidation and extortion as a means of control. Victor Bettencourt, 42, is charged with human trafficking, procuring a person to engage in prostitution, procuring for living off the avails of prostitution, extortion, two counts of trafficking in cocaine, possession of cocaine for the purpose of trafficking, possession of the proceeds of crime under $5,000 and failing to comply with recognizance by breaching bail terms. Hamilton Spectator, A6

Mountie rescues child from car
Surrey, B.C. Mom Alyse McDonald will be forever grateful to RCMP Const. Aaron Jabs. The off-duty police officer went out his way Wednesday morning to pull McDonald's two-year-old daughter Haylee from the wreckage of the family car, which was upside down in a watery ditch in Delta. Telegraph-Journal, A4

*** Des accusations criminelles contre des adeptes du flip immobilier**
La GRC a arrêté mardi Kinh Ho Quan, 56 ans, et Hermel Bossé, 58 ans, deux individus impliqués dans plusieurs cas de fraudes hypothécaires, principalement dans la région de Montréal. Ils ont été libérés rapidement. On n'a pas pu connaître les conditions de leur libération. Ils comparaîtront en cour le 30 mars. Ils sont accusés de fraude de plus de 5000$. S'ils sont reconnus coupables, ils risquent une peine de prison maximale de 14 ans. Une enquête approfondie menée par l'Unité des fraudes majeures de la Section des délits commerciaux de Montréal de la GRC a porté plus spécifiquement sur 20 transactions suspectes qui se sont toutes avérées frauduleuses pour un total s'élevant à près de 4,5 millions de dollars. La Presse, S4; Le Journal de Montréal

Arrest in $200k scam on senior
A man accused of scamming a 90-year-old B.C. homeowner out of more than $200,000 was busted in northern Manitoba last week and sent back to Vancouver Island. Richard Patterson, 47, was arrested Jan. 25 in Norway House on the strength of a Canada- wide warrant for fraud over $5,000, according to Manitoba RCMP. He was charged by Victoria police last summer for allegedly bilking a 90-year-old resident of the B.C. capital out of more than $200,000 for renovations he was supposed to be doing on the man's house. Winnipeg Sun, 13

Porn sting may yield more arrests
The different investigations, some of which lasted eight months, came to a head Jan. 31 and Feb. 1. Police executed 76 search warrants and laid 213 charges against 60 people, including three young offenders. The people nabbed in Windsor face a range of charges including accessing child pornography, possession of child pornography, distribution of child pornography and luring a child for sexual purposes. Staff Sgt. William Donnelly with Windsor police said additional arrests are possible, but that could take awhile as police sift through child porn photos that are "traded around like hockey cards." Windsor Star, A5

Alleged cyber sicko
She thought she knew him and she wasn't alone. Toronto Police claim many teen girls across the country met Alex Sirop online and believed he was a good-looking 19-year-old. They had no idea when they sent "compromising" images of themselves over the web that a 42-year-old Scarborough man named Shiraz Nariman was allegedly adding them to his collection of child porn. Nariman is one of 54 people rounded up recently by police in Ontario during a massive child pornography sweep. The RCMP first learned of him when a teenage girl, who can't be named, came forward in September 2010. Toronto Sun, 7; Toronto Star

Man charged with making child porn
A man has been charged with producing child pornography following a year-long investigation by the Edmundston City Police Force and the New Brunswick RCMP's Internet Child Exploitation Unit. Shane Evan McCabe, 34, of no fixed address, was arrested on Thursday upon his release from jail where he was serving time for failing to register with the National Sex Offender Registry for past convictions. The investigation began in March 2011 when images of child sexual abuse were found scattered around the City of Edmundston. The Fredericton Police Force, the RCMP's Technological Crime Unit, the National Child Exploitation Coordination Centre, the Canadian Centre for Child Protection (cybertip.ca), the RCMP's Violent Crime Linkage Analysis System and the National Sex Offender Registry also assisted with the investigation. Times & Transcript, A9

Two grow-ops found same day
London police busted two marijuana grow-ops in less than three hours, seizing nearly $600,000 in drugs. Both grow operations, located less than eight kilometres apart, were in middle-class north London neighbourhoods. London Free Press, A8

Police reveal drug lab photos to highlight ecstasy dangers
Filthy conditions, unknown chemicals and a pill press covered in ecstasy: this is what a drug lab looks like. In their latest effort to showcase the dangers associated with street drugs, police released photographs on Friday of an ecstasy lab in Richmond, B.C., in light of the many deaths in Calgary and B.C. tied to ecstasy laced with a toxic chemical. Seven people in Calgary, and one person in Red Deer, have died from taking ecstasy (MDMA) laced with para-methoxymethamphetamine (PMMA). Two additional cases are still awaiting toxicology results. There have been five deaths reported in B.C. The chemical, a cheaper alternative than MDMA, is being cut into ecstasy, but is believed to be more toxic. B.C. RCMP Sgt. Duncan Pound said when officers entered the lab in full protective suits in 2008, they found 750,000 pills and enough drugs to make 3.3 million tablets. Calgary Herald, B1

Date-rape drugs among $17K bust
Mounties in Red Deer say they've made a major seizure of so-called date rape drugs that were meant to be trafficked. On Thursday, Mounties executed a warrant on a Red Deer residence, where a search turned up two kinds of drugs known to be used to incapacitate unwitting victims who are then sexually assaulted. In the search of the house and garage, they found three litres of gamma hydroxybutyric acid (GHB), as well as 10.8g of ketamine, which can be slipped into drinks. Calgary Sun, 20

*** 135 000 cigarettes dans le coffre**
Une Néo-Écossaise a été arrêtée alors qu'elle était en possession de quelque 135 000 cigarettes de contrebande du Québec qui étaient destinées au marché de la région de Halifax. La suspecte, une femme de 35 ans de Timberlea, en Nouvelle-Écosse, a été interpellée par les autorités plus tôt cette semaine lors d'une perquisition effectuée par la GRC et les autorités provinciales dans une Chevrolet Impala 2011. Le Journal de Montréal, 22

*** Notorious B.C. brother guilty of drug conspiracy**
One of three brothers among a notorious family with reputed links to Vancouver's gang world "fabricated" a story that he was simply planning to steal drugs, instead of scheming to traffic them with his ex-girlfriend's father, a B.C. Supreme Court judge said Friday. Jarrod Bacon, 28, and Wayne Scott, 55, were each found guilty of one count to conspire to traffic cocaine by Associate Chief Justice Austin Cullen following a four month trial that ended mid-January. Red Deer Advocate, A3; * Calgary Herald; * Vancouver Sun

Remains found on reserve
Human remains have been found in a vacant home on the Nak'azdli reserve in B.C., RCMP said Friday. The remains were reported to police Wednesday afternoon. The reserve is located about 150 km northwest of Prince George. It is considered a suspicious death at this point, Corp. Annie Linteau said. Edmonton Sun, 23

Civilian oversight of police a must
An opinion piece states, "The continuing fall-out over the violent arrest of Adam Nobody during the G20 raises serious doubts about the adequacy of civilian oversight of the police. Eighteen months later, one officer, Const. Babak Andalib-Goortani, has been charged criminally with assault by the province's Special Investigations Unit. Another provincial body, the Office of the Independent Police Review Director, has recommended Andalib-Goortani and four others -- Constables Michael Adams, David Donaldson, Geoffrey Fardell and Oliver Simpson -- face disciplinary charges. But the SIU says since the standard of evidence for identifying officers is higher for a criminal case than disciplinary hearings, no new criminal charges will be laid... But the larger issue is the lack of co-operation the SIU has received from police, not just in G20 cases in Toronto, but across the province." Ottawa Sun, 12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** Hamilton mother facing deportation loses reprieve**
The final government word for Lucene Charles, the Hamilton mother of three Canadian boys fighting deportation to St. Vincent, is that she must go, expeditiously. Charles, who has been on an emotional roller-coaster ride since losing her final appeal last summer, was told Friday a review of her case supports the original deportation order. She was ordered to return to the Canada Border Services Agency (CBSA) offices on Tuesday to show that she has purchased one-way, non-refundable tickets to St. Vincent for herself and her five-year-old African-born daughter leaving Canada by Feb. 17. Charles, 36, was ordered in January to leave by Feb. 2, but received a reprieve a few days later. She was recently summoned to meet with CBSA agents again on Friday. CBSA officials said Charles is being deported because she entered and remained in Canada without authorization. Hamilton Spectator, A4

*** Un traitement royal pour Mugesera**
Le Rwandais Léon Mugesera a eu droit à un traitement royal lors de sa déportation du Canada vers son pays natal : avion privé, personnel médical et agents de sécurité, a appris l'Agence QMI. L'ancien homme politique a été expulsé du pays la semaine dernière, pour retourner au Rwanda, où il devra faire face à des accusations relativement au génocide survenu en 1994. L'Agence des services frontaliers du Canada (ASFC) a confirmé que le renvoi de M. Mugesera avait nécessité " un vol nolisé avec plusieurs escortes (agents de sécurité) et un infirmier ", pendant un voyage d'une durée de 30 heures. L'ASFC a refusé de dévoiler les coûts de l'extradition, mais selon des informations affichées sur le site Web de Citoyenneté et Immigration, les dépenses relatives aux renvois " peuvent s'élever jusqu'à 300 000 $ lorsqu'il s'agit d'affréter un avion dans certains cas ". Le ministère précise que des coûts d'environ 200 $ par jour s'ajoutent à cela, lorsque la mise en détention s'avère nécessaire. L'ASFC précise qu'un renvoi ne requérant pas d'escorte coûte en moyenne 1 500 $. Cependant, lorsque des agents de l'Agence doivent escorter un individu à bord d'un vol commercial " pour des raisons de sécurité ", le renvoi coûte en moyenne 15 000 $. Le Journal de Montréal, 19

Deportation for dirtbag
Clato Mabior's time on Canadian soil appears to be quickly winding down. Mabior, convicted of aggravated sexual assault for failing to disclose his HIV status to sexual partners, will be deported to Sudan in the next 30 days -- likely on Feb. 15, according to his immigration lawyer. Mabior, 34, was ordered held in custody at a review of his ongoing detention Friday. He's been behind bars on the strength of a deportation order since October 2010. The Immigration and Refugee Board has repeatedly ruled that Mabior is a flight risk and a danger to the public. Winnipeg Sun, 3

*** Une sexagénaire d'origine française menacée d'expulsion pour un vol de 80 $**
Jeannine Poloni, une femme de 67 ans d'origine française est menacée d'expulsion pour avoir volé pour 80 $ de nourriture dans une épicerie et parce qu'on la considère maintenant comme une "grande criminelle ". M me Poloni est arrivée au Canada en 1964. Elle a son statut de résidente permanente, mais n'a jamais fait de demande de citoyenneté canadienne. Elle a travaillé toute sa vie et a fondé une fa-mille au Québec. C'est en 2009 qu'elle a été arrêtée pour avoir volé pour 80 $ de nourriture dans une épicerie et condamnée à une peine de neuf mois de prison avec sursis. Lorsqu'une personne qui n'est pas citoyenne canadienne est condamnée à une peine criminelle de plus de six mois, les autorités peuvent demander son expulsion pour cause de " grande criminalité ". C'est ce qui arrive à M me Poloni. Le Journal de Montréal, 22

The hangover
On May 13, 2011, a prominent Canadian DJ crossed the Alberta-B.C. border near Lake Louise with a case of red wine, daring authorities to arrest him. The Mounties refrained but Terry David Mulligan had made a point of mocking a lingering hangover of Alberta alcohol prohibition 87 years after its repeal. Yet, it's still illegal to cross provincial borders with booze. While flamboyant bootleggers such as Al Capone, furtive speakeasies and rumrunners are colourful legends of the 1920-1933 U.S. prohibition, Canada's own doomed attempt at shutting off the taps has barely had a last recall. Calgary Sun, 18

Mugesera finally finds Rwandan lawyer
Rwandan lawyers haven't been lining up to defend Léon Mugesera - wanted for almost two decades for his role in the 1994 Rwandan genocide - but one has stepped forward, despite possible security issues and little pay. Guy Bertrand, the Quebec City lawyer who helped the suspected war criminal dodge deportation from Canada for years, said it was difficult to find someone willing to take on his client. He fears for the Rwandan attorney's safety but can't afford to hire a bodyguard. For security reasons, Bertrand didn't want to reveal the lawyer's name or put The Gazette in touch with him, but Rwandan news organizations reported he is Donat Mukunzi. Montreal Gazette, A8

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

VICTIMS TREATED CRIMINALLY

It's about time someone started talking about the rights of victims in the criminal justice system. Canada's ombudsman for victims' rights Sue O'Sullivan released a special report this past week on the need for governments, the courts and corrections to start taking the rights of victims of crime far more seriously than they have in the past. And her report is bang-on. I recommend every elected official in Canada read it. I've met enough victims of crime over the years to know exactly what O'Sullivan is talking about. We spend a lot of time in the justice system dealing with the criminals themselves -- their sentences, their rights, etc. -- but not enough time ensuring victims have the legislated rights they deserve. Winnipeg Sun, 5

*** Haitian-born killer got aboriginal-style hearing**

Federal documents have offered a glimpse into a controversial hearing last month in which a Haitian-born convicted killer was able to access an aboriginal-style parole hearing at Manitoba's Stony Mountain Institution, a medium-security facility. Gregory Bromby, 35, was convicted of first-degree murder in 1997 for the stabbing death of 15-year-old Tara Manning in Quebec in 1994. He claims working with aboriginal elders on a special unit at the prison taught him to respect women. The parole hearing was attended by Michael Manning, the Mont-real-based father of the young murder victim. Bromby's attempt at day parole ultimately was denied. Documents released by the Parole Board of Canada say Bromby participated in aboriginal spirituality and ceremonies, while living on a special unit designed to honour the spiritual and cultural ways of aboriginal people. Edmonton Journal, A8

Group aims to 'out' pedophiles

A Christian-oriented activist group said Friday it plans to launch a website for identifying pedophiles. Canada Family Action said its website will be called FindA-Pedophile.com. Brian Rushfeldt, president of the organization, said he hopes to have the site operational by March. The Calgary-based group said the recent bust of 60 people in Ontario on hundreds of child pornography charges is proof that such a resource is needed. Rushfeldt said the information will be gathered from sources such as the courts, police and media reports. Montreal Gazette, A15; Ottawa Sun

Quebec man wants senator prosecuted for suicide comments

A Quebec man has filed a police complaint against Conservative Senator Pierre-Hugues Boisvenu for remarks he believes could lead someone to commit suicide. The complaint came after Boisvenu said Wednesday in Ottawa that some convicted killers - he referred specifically to Paul Bernardo, Clifford Olson and Robert Pickton - should be given a rope in their prison cells in case they want to hang themselves. The senator later apologized for his comments, but 26-year-old Jacques McBrearty said Boisvenu went too far. The Sûreté du Québec will investigate the complaint, which could eventually be handed over to the RCMP since the events occurred in Ontario, where Boisvenu lives. Montreal Gazette, A10; * Waterloo Region Record

*** Le sénateur Boisvenu est une victime d'abord**

Tous les collègues conservateurs du sénateur Pierre-Hugues Boisvenu viennent maintenant à sa défense. Ils disent qu'on n'a pas le droit d'attaquer ses propos parce qu'il est une victime et qu'il a donc parlé avec ses émotions. Lorsque le sénateur conservateur, mercredi, a émis son opinion sur la peine de mort, lâchant sa phrase devenue rapidement célèbre, " il faudrait que chaque assassin (ait) le droit à sa corde dans sa cellule ", le premier ministre Stephen Harper a cherché à étouffer l'affaire le jour même en soulignant que le sénateur avait retiré ses propos. Mais comme M. Boisvenu continue de partager publiquement son opinion sur la peine de mort, la nuançant plus ou moins, se vantant même d'avoir reçu des centaines d'appuis pour son commentaire, la défense du gouvernement a changé. A l'intérieur comme à l'extérieur des Communes, les élus conservateurs disent dorénavant que personne n'a le droit d'attaquer M. Boisvenu à cause de sa douloureuse histoire familiale, faisant référence à l'assassinat de sa fille. La Tribune, 14

*** Pas une première pour le sénateur Boisvenu**

Même si les propos du sénateur Pierre-Hugues Boisvenu ont suscité la controverse d'un bout à l'autre du pays, cette semaine, ce n'est pas la première fois qu'il tient un tel discours. Dans une entrevue accordée au Journal de Québec en juillet 2010, le sénateur conservateur s'interrogeait sur les coûts que l'État doit payer pour garder incarcérés les criminels dangereux dont la " réhabilitation est impossible ". " Est-ce que, dans ces cas-là, on devrait laisser le libre choix au criminel ? Est-ce que, dans ces cas-là, on pourrait dire : " Regardez, on tire la plogue " ? ", soulevait alors M. Boisvenu. Le sénateur admettait aussi être favorable " dans certains cas " à la peine de mort, par exemple ceux des meurtriers en série Clifford Olsen et Robert Pickton. Le Journal de Montréal, 19

*** Sex attacker high risk to re-offend**

A "high-risk" repeat sex offender who admitted in court Friday to brutally raping an Edmonton woman in the river valley is to face a dangerous offender hearing. Anthony Winston Clark, 34, pleaded guilty in Court of Queen's Bench to kid-

napping, sexual assault causing bodily harm, attempted choking and uttering death threats. If Clark is designated a dangerous offender, he will be handed an indefinite prison sentence. Edmonton Sun, 4

Kamloops jail too easy to break in to
A review conducted before two recent break-ins at the Kamloops Regional Correctional Centre, apparently to smuggle contraband - possibly drugs - to prisoners, revealed the Interior British Columbia jail must beef up its security practices. Dean Purdy, spokesman for the B.C. Government Employees' Union, said in each case someone scaled the jail's two-metre high perimeter fence and cut a hole in a cell window in the segregation unit. Early reports suggested a laser was used to drill into one of the pieces of Lexan glass. The Daily News has learned a blowtorch was used. Purdy believes the breaches were made to smuggle contraband - possibly drugs - into the prison. The incident raises alarm bells for the union, which is conducting its own investigation along with the province's corrections branch and RCMP. Edmonton Journal, A19

No honour in killing
Imams across North America are condemning the act of "honour killing" on the heels of the guilty verdict and life sentences handed to the Shafia family last Sunday. Mohammad Shafia, 59, his second wife Tooba Mohammad Yahya, 42, and the couple's son, Hamed, 21, were each convicted on four counts of first-degree murder for killing Shafia daughters Zainab, 19, Sahar, 17, Geeti, 13, and Mohammad's first wife, Rona Amir Mohammad, 52. "There is no such thing in Islam that if somebody is bringing disgrace to your family's honour that you go out and kill that per-son," said Imam Syed Soharwardy, founder of the Islamic Supreme Council of Canada. Soharwardy will be issuing a Fatwa on Saturday, a type of religious edict, with more than 34 signatures from imams across North America supporting its position against honour killings, domestic violence and misogyny. Toronto Sun, 9; * National Post

*** This regressive bill will undermine previous work**
Re: the Canadian Bar Association's (CBA's) position on the omnibus crime bill.
A letter states, "We write further to the story written by Nadine Sander-Green on Jan. 27 stating that our justice minister, Mike Nixon, reconfirmed his support for Bill C-10. With respect, the CBA and particularly the Criminal Law Section of the Yukon branch of the CBA strongly disagree with the omnibus federal crime bill... Many years of research have shown what actually reduces crime: a) addressing child poverty; b) providing services for people with mental illness or FASD; c) diverting young offenders from the adult justice system; and d) rehabilitating prisoners and helping them to reintegrate into society. Bill C-10 will actually eliminate conditional sentences for minor and property offenders and instead send those offenders to jail. Mandatory minimums replacing conditional sentences will victimize the most vulnerable by shipping people from remote, rural and northern communities far from their families to serve time. In Yukon, aboriginal people are already over-represented in the justice system." Whitehorse Daily Star, 12

*** Mon agresseur aussi a des droits**
Lettre ouverte au sénateur Pierre-Hugues Boisvenu
Une lettre écrit par Steve Foster, président-directeur général du CQGL dit, « Vos dernières déclarations, selon lesquelles chaque assassin devrait avoir sa corde dans sa cellule pour se pendre et que nous devrions réévaluer la peine de mort pour les cas irrécupérables, m'ont grandement attristé. J'aimerais partager avec vous et le public ce texte pour offrir matière à réflexion... » Le Soleil, 34

*** Senator's remarks ill-advised - but consider his pain**
An opinion piece states, "The Conservative senator who suggested that murderers in Canadian prisons be given rope with which to hang themselves is an emblem of the degradation of our political discourse... Sen. Pierre-Hugues Boisvenu, a victim's rights campaigner appointed to the Senate by Stephen Harper in 2009, ignored the fact that 28 prisoners in federal custody have killed themselves since 2008 and that hanging is the means of choice for 90 per cent of such suicides. So Boisvenu's offer of prison-issue paraphernalia was unnecessary. Human beings, even depraved ones, who make this decision will find a way. Boisvenu has since offered a conditional apology to families of suicides. He has not further amplified his suggestion that immigrants be "filtered" for anti-Canadian attitudes like the ones of the murderous Shafia trio. Who would admit to being willing to slaughter a disobedient daughter? And this is how half-baked plans to improve the world appear. They are blurted out... Boisvenu, who has helped build a women's shelter and a youth camp, is a hero, if flawed." Toronto Star, A12

*** À la défense du sénateur**
Un article d'opinion dit, « Au risque de me faire traiter de suppôt de l'extrême droite, je me porte à la défense de Pierre-Hugues Boisvenu. Après tout, si des meurtriers ont le droit à une défense pleine et entière, je ne vois pas pourquoi on refuserait le même privilège à un sénateur qui n'a rien fait de mal, sauf exprimer un point de vue impopulaire auprès d'une certaine élite bien pensante. À moins que vous me disiez qu'aller à l'encontre de la rectitude politique ambiante est plus répréhensible qu'asséner 40 coups de couteau à ses propres enfants. » Le Journal de Montréal, 6

Des propos condamnables
Un article d'opinion dit, « Une fois de plus, une personnalité publique, en l'occurrence un sénateur bien connu au Québec, s'enflamme et tient des propos qui ne devraient jamais sortir de la bouche d'une personne qui exerce une aussi grande influence sur l'opinion publique. Bien que l'incommensurable souffrance associée à la perte d'un enfant puisse nous amener à comprendre ses motivations profondes, il n'en demeure pas moins que ce genre de propos qui viennent plus du coeur que de la tête sont condamnables lorsqu'on occupe une position politique importante. Cette idée de laisser une corde dans la cellule des criminels ayant commis un homicide est barbare et rétrograde et n'a pas sa place dans une société moderne comme la nôtre. » Le Nouvelliste, 21

*** Un sénateur à "tasser"**
Un article d'opinion dit, « Le premier ministre Stephen Harper passe trop facilement l'éponge dans le cas du sénateur Pierre-Hugues Boisvenu qui a dit que chaque assassin devrait avoir une corde dans sa cellule et décider lui-même de la suite de sa vie. Ce sénateur qui a aussi affirmé que l'emprisonnement à vie des Shafia coûtera à l'État canadien quelque 10 millions$ que celui-ci n'aura donc pas pour investir ailleurs parce qu'il les consacrera à l'entretien de criminels où il n'y a aucune possibilité de réhabilitation. Certes, le sénateur s'est-il excusé, comme le relève le premier ministre en réplique à ceux qui critiquent vertement le sénateur et en réclament la démission ou la destitution comme porte-parole officiel du gouvernement en matière de justice et criminalité. Or, M. Harper ne semble pas avoir l'intention de "tasser" le sénateur, ne serait-ce qu'en le mutant à un autre dossier, et M. Boisvenu n'a lui-même pas l'intention de démissionner, que ce soit comme porte-parole officiel ou sénateur. » La Voix de l'Est, 14

*** Propos du sénateur Boisvenu - Pas de voie unique pour soutenir les victimes**
Un article d'opinion dit, « Les personnes qui ont été victimes de violence sont dans une position «privilégiée» pour comprendre les manifestations et les conséquences de cette violence. Comme société, nous devrions les encourager à prendre la parole et nous devrions considérer leur point de vue dans l'élaboration de politiques et de programmes sociaux. Au cours des dernières décennies, plusieurs mesures ont été mises en place en réponse aux revendications de groupes représentant des victimes de violence; certaines de ces mesures s'inscrivaient dans une logique de contrôle social, tandis que d'autres visaient davantage le soutien aux individus et aux communautés. Lorsqu'il est question de violence, je crois que nous devons faire appel à une combinaison de mesures de contrôle et de mesure d'aide. » Le Devoir, B5

PUBLIC SERVICE / FONCTION PUBLIQUE

Whistleblowers in public service face reprisal: integrity group
Public servants who disclose wrongdoing invariably face workplace reprisals despite laws promising protection, says the head of an organization that promotes integrity and accountability within government. David Hutton, executive director of FAIR (Federal Accountability Initiative for Reform), said he's received hundreds of calls from whistleblowers since assuming his volunteer position in 2008. In some jurisdictions, those who punish whistleblowers can lose their jobs, go to jail and be sued. Australia and Britain are "decades ahead of us" in comparison to the "absolutely dreadful" whistleblower law in Canada, Hutton said. He was responding to a report, prepared for the Office of the Public Sector Integrity Commissioner, which says government employees fear career-limiting reprisals if they blow the whistle on wrongdoers in the federal public service. The report summarizes the findings of 10 focus groups held last November to explore public servants' perceptions about disclosing wrongdoing in their workplaces. It paints a picture of a public service that recognizes its responsibility to disclose wrongdoings, at least in principle, but is fearful of the consequences. Ottawa Citizen, A3; Le Droit

INTERNATIONAL / INTERNATIONAL

Inquiry urged over bribery case
Indian opposition leaders are calling for a government inquiry into allegedly corrupt dealings at the country's Ministry of Civil Aviation, following a Globe and Mail report on bribery and bid-rigging allegations that implicate, among others, cabinet minister Praful Patel. The Globe has detailed the allegations against Nazir Karigar, a 64-year-old Indian-born Canadian citizen and the first individual to be charged under Canada's foreign bribery law - the Corruption of Foreign Public Officials Act. As part of its case against Mr. Karigar, the Royal Canadian Mounted Police alleges that he divulged to others that he had channelled a $250,000 bribe to Mr. Patel while he was minister of Civil Aviation, with the help of a political ally, in 2007. Mr. Patel, who is now Heavy Industries Minister, has said he had no knowledge of the scheme. There is no evidence that he accepted the money. The story dominated the Indian media Friday as supporters from the ruling Nationalist Congress Party (NCP) and the government rose to his defence. Globe and Mail, A15

OTHER / AUTRE

Ottawa a fait la promotion des aliments du Canada après le tsunami au Japon
Ottawa a vu dans le violent séisme et le tsunami survenus l'an dernier au Japon une occasion d'aiguiser l'appétit pour la cuisine canadienne. Le gouvernement fédéral a en effet proposé une activité pour faire la promotion de «la marque Canada» sur le marché japonais. Le plan visait à faire connaître des produits comme le sirop d'érable du Québec, le boeuf de l'Alberta et d'autres denrées aux personnes laissées sans abri par la catastrophe. Selon des documents obtenus par La Presse Canadienne, le Canada devait démontrer son appui en organisant un café en plein air et en nourrissant des victimes avec des produits canadiens afin qu'ils puissent se sentir comme s'ils étaient en visite au Canada. L'Acadie Nouvelle, 9; Whitehorse Star

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-04-12 9:07 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne - Part One / Première partie

Daily Media Summary / Revue de presse quotidienne
February 4, 2012 / le 4 février 2012

MINISTER / MINISTRE

NDP MP in hot water again for profanity-laced tirade
Winnipeg NDP MP Pat Martin added fuel to the obscenity-laden firestorm he created this week when he cursed at a Conservative senator who suggested murderers should be given ropes to hang themselves. On Wednesday, Martin cursed Sen. Pierre-Hugues Boisvenu sparking controversy. When demands for an apology were made Thursday, Martin refused. He added perhaps his only mistake was that he didn't include the required honorific when addressing a senator. Boisvenu triggered his own controversy with his comments Wednesday when he was asked about the government's omnibus crime bill, which gives stiffer penalties for certain violent crimes. Boisvenu is an outspoken victims' rights advocate. His daughter was raped and murdered by a repeat offender in Quebec in 2002. He was appointed to the senate in 2009. Manitoba Senior Minister and **Public Safety Minister Vic Toews** demanded Martin apologize. "***Pat Martin's constituents, and indeed all Canadians, would be better served if the MP and his soft-on-crime party, would direct their outrage and vitriol at the criminals who victimize innocent, law-abiding Canadians rather than at a senator whose family has suffered a terrible loss at the hands of a repeat offender***," **Toews said** in a letter to the editor. Telegraph-Journal, A9

Trotting out the bogeyman
An opinion piece states, ""***I don't know if the statistics demonstrate that crime is down ... I'm focused on danger***." That's **federal Public Safety Minister Vic Toews**, speaking to the Senate Committee on Legal and Constitutional Affairs about the Conservatives' "tough on crime" legislation. If nothing else, the next few years are going to have more than their fair share of unintentional hilarity - because unless I completely misunderstood that particular quote, **Toews** has just confirmed what opponents of the new crime legislation have been saying all along. And that's that the legislation has nothing to do with crime, and everything to do with marketing... Rewind a little further, back to when **Vic Toews** actually did realize that statistics demonstrated that crime rates were down to levels last seen in the early '70s. (He must have since forgotten about those statistics, because he clearly doesn't know about them anymore.) He said that the Tory crime bill was to help address the increase in unreported crimes. "***We see this continuing trend of more and more crimes going unreported, and that ... I believe is an indication of a lack of confidence in the justice system***," **Toews** told CTV in September 2010. "***And that is why our government is taking the measures that we are taking***." All right. To get this straight, then: it's the increase in unreported crime (that's a great thing to try and measure in any form - it's big, it's bad, it's ... unreported, hence statistically, well, void) and the increase in ... wait for it ... danger..." The Telegram, A20

Hat's not impressed with Tory justice
A satirical opinion piece states, "Mousie MacKay got a beer from the bar at Louie The Leggers and carried it over to the table where Hat McInnes was sitting, sipping on a beverage, and playing with a small computer... "No, the story I was referring to was the one where, once again the **minister of public safety**, boy, that's an Orwellian mouthful, **minister of public safety**. Anyway, yet another judge has criticized the minister for not allowing a Canadian in prison in the States to serve their time in a Canadian prison." "Seven years for a marijuana bust, that's pretty heavy," said Mousie, "But the Americans are paranoid about drugs. Can you imagine how tense things will get if the Liberals try to legalize marijuana? How come the government slammed the door on this guy, a bit of weed doesn't seem like a capital crime?" "That's one of the problems the judge had, **the minister** didn't really provide any reasons for his denial," said Hat, "so the judge has ordered **the minister** to review the case and provide some good reasons for denying the man a chance to serve his sentence in Canada." "So who stopped the marijuana guy from coming back to a Canadian prison?" asked Mousie. "That was **Vic Toews**, another guy who's made up his mind and doesn't want to be confused by the facts..." The Guardian, A15

One to watch...

A letter states, "Bill C-10: The crime bill. It's not so much the crime bill itself that needs watching; a minority of Canadian voters graciously granted Prime Minister Stephen Harper a majority government, so the bill will pass. What will be interesting to watch is how the bill will play out after it is passed. Even some Tory senators wonder why the Harper government is so fixated on crime, in light of statistics that show crime has actually been decreasing for quite some time. **Public Safety Minister Vic Toews** told a Senate committee reviewing the legislation: "***I don't know if the statistics demonstrate that crime is down. I'm focused on danger.***" **The minister** then went on to say his concern is that the public is in danger as long as criminals walk the streets, "***and this legislation addresses that.***" Given the statistical decline of murderers, rapists, violent robbers and other shady types, the question has to be asked: Who is **Toews** afraid of when he walks the streets of Canada? Panhandlers? Homeless people?" Winnipeg Free Press, J12

Have your say
A letter states, "OK, Pat Martin lips off again, and again **Vic Toews** runs to the media. He reminds me of a schoolyard child running to his teacher to tattle on another for saying a bad word. And for what? To say sorry? Really! Canadian politics has come down to this? Now that's obscene." Winnipeg Free Press, A17

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Despite weather, flood forecast in works
Manitoba Water Stewardship is working on a spring flood forecast despite this winter's mild and relatively dry weather. Provincial flood forecasters plan to unveil a preliminary flood outlook before the end of February, spokesman Paul White said Friday. Although much of southern Manitoba has experienced dry conditions since June, ground moisture levels -- one of the factors that increases the probability of localized or regional flooding -- remain significant in some areas of the province. While moisture levels are well below those recorded last winter, when the province began preparing for major spring flooding, conditions are comparable to the early months of 1997, the year of the Flood of the Century in the Red River Valley, White said. But across most of southern Manitoba, the snowpack -- another major factor in determining flooding -- is much lower this year. That can change significantly before the spring snowmelt, as one or two blizzards can be the difference between a major flood and no flooding whatsoever. Winnipeg Free Press, A13

B.C. avalanche kills man
One man is dead after a small group of recreational skiers got caught in an avalanche Friday morning on Meadow Mountain, near Kaslo, B.C. The man's name isn't being released until Mounties notify his family. The B.C. Coroner's Service and RCMP are still investigating the death. Windsor Star, A13; Edmonton Journal

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Conditions eased for suspect
Mohammad Mahjoub, a Toronto man detained and subsequently held under house arrest for the past 12 years on a national security certificate because of alleged terrorist ties, was granted more freedoms by a federal court Friday. Mahjoub, 51, was arrested in Toronto in 2000 on a security certificate, which allows the government to detain terror suspects indefinitely without charges or a trial. In his decision, Judge Edmond P. Blanchard said the federal government failed to provide "reasonable grounds to believe" that Mahjoub's security threat has not reduced. While Blanchard said there remains "compelling and credible evidence" that Mahjoub "poses a threat to the security of Canada," evidence during the latest review of Mahjoub's case and his current circumstances suggest that this threat "is now significantly diminished." Windsor Star, A13; National Post; The Telegram

Defenceless
Just what legally constitutes a foreign activity in Canada that is detrimental to this country's national security interests these days, anyway? As it turns out, Canada is practically incapable of answering that question with any enforceable coherence. When it comes to the recent and rapid-succession manoeuvres that have given Chinese state-owned entities the spigot key at critical flow points in Canada's oil and gas industry, mysteries abound. But it is now clear that slowly but surely, Canada's regulatory defences have been almost completely hollowed out. Way back in the 1980s, the Security Intelligence Review Committee was urging amendments to the Canadian Security Intelligence Service Act to spell out what Canadians mean when we talk about foreign-power connivings that are "detrimental" to Canada's national interests. "It is almost wholly subjective: no criteria are provided to offer any standard for determining what is 'detrimental'," a SIRC report once pointed out. The definitions in the CSIS Act still don't clearly define what "detrimental" means, but unlike Investment Canada, CSIS has muddled through and is properly content to couple Canada's "national security" with "the security and economic welfare of Canada." Ottawa Citizen, B7

Muslim group slams 'terrorist' treatment

A Canadian Muslim businessman became a terror suspect for telling sales staff in a text message to "blow away" the competition at a New York City trade show, an association said Friday. Moroccan-born Saad Allami was arrested three days after he sent the message in January 2011 and detained while police searched his home, said the Muslim Council of Montreal. Ottawa Citizen, A4; Le Soleil

MacKay quiet on iran plans
Regional troublemaker Iran poses "a grave threat to peace and security" and is "fanatical and dangerous," Prime Minister Stephen Harper said Friday. Harper made the comments during an interview with Postmedia, and warned that Iran would be ready to use a nuclear weapon if it was able to produce one. But in an interview with QMI Agency, Defence Minister Peter MacKay wouldn't speculate whether Canada -- a staunch ally of Israel -- would join that country in a possible strike against the Islamic regime. Toronto Sun, 24

CYBER SECURITY / CYBERSÉCURITÉ

Confidential police call hacked, leaked
Trading jokes and swapping leads, investigators from the FBI and Scotland Yard spent the conference call strategizing about how to bring down the hacking collective known as Anonymous, responsible for a string of embarrassing attacks across the Internet. Unfortunately for the cyber sleuths, the hackers were in on the call too - and now so is the rest of the world. Anonymous published the roughly 15-minute-long recording of the call on the Internet on Friday, gloating in a Twitter message that "the FBI might be curious how we're able to continuously read their internal comms for some time now." The humiliating coup exposed a vulnerability that might have had more serious consequences had someone else been listening in on the line. The leak was one of a slew of Anonymous hacks that hit websites across the United States Friday, including in Boston, where the police site was defaced, and in Salt Lake City, where officials said that personal information of confidential informants and tipsters had been compromised. Anonymous also claimed credit for defacing the Greek Justice Ministry's website and stealing a mountain of data from the Virginia-based law firm that defended a U.S. Marine recently convicted for his role in the bloody 2005 raid in Iraq that became known as the Haditha massacre. Red Deer Advocate, A5

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

$1M worth of drugs, 13 charged in 'high-level' raid
Thirteen people alleged by police to be "high-level" drug dealers were charged Friday in connection with the latest large-scale sweep orchestrated by Manitoba's organized crime unit. Project Deplete, a police investigation that began last August and culminated Friday with arrests in Winnipeg and Edmonton, is the latest effort of Manitoba's Integrated Organized Crime Task Force, a joint RCMP-Winnipeg police unit that has famously used informants over the past several years to take down primarily the Hells Angels and their associates, with great success. The latest sweep saw charges laid against people police accuse of being major players in the city's drug trade. Some of the accused have gang associations, others are more "independent," police said. Winnipeg Sun, 2

DNR finds barrels of pot
Approximately 29 kilograms of marijuana has been seized following the discovery of the drug by New Brunswick Department of Natural Resources Conservation Officers. Last week, conservation officers were working on an illegal possession of moose meat investigation when they discovered the drug in a number of barrels in a wooded area near a residence in Scoudouc. They then called the District 4 RCMP who began an investigation. Times & Transcript, A6

Police make arrest and seize cocaine, marijuana
A 33-year-old Saint John man has been arrested after police seized a large amount of cocaine and marijuana from the city's east side. Russell William McCain of Canterbury Street faces a number of drug-related charges, police said in a release. McCain's arrest came after a three-month investigation by members of the Saint John Police Force street crime unit and the Fundy Integrated Intelligence Unit. The RCMP and the Rothesay Regional Police Force participated in the drug raid on Thursday. Telegraph-Journal, B3

Mountie rescues child from car
Surrey, B.C. Mom Alyse McDonald will be forever grateful to RCMP Const. Aaron Jabs. The off-duty police officer went out his way Wednesday morning to pull McDonald's two-year-old daughter Haylee from the wreckage of the family car, which was upside down in a watery ditch in Delta. Telegraph-Journal, A4

Arrest in $200k scam on senior

A man accused of scamming a 90-year-old B.C. homeowner out of more than $200,000 was busted in northern Manitoba last week and sent back to Vancouver Island. Richard Patterson, 47, was arrested Jan. 25 in Norway House on the strength of a Canada- wide warrant for fraud over $5,000, according to Manitoba RCMP. He was charged by Victoria police last summer for allegedly bilking a 90-year-old resident of the B.C. capital out of more than $200,000 for renovations he was supposed to be doing on the man's house. Winnipeg Sun, 13

Porn sting may yield more arrests
The different investigations, some of which lasted eight months, came to a head Jan. 31 and Feb. 1. Police executed 76 search warrants and laid 213 charges against 60 people, including three young offenders. The people nabbed in Windsor face a range of charges including accessing child pornography, possession of child pornography, distribution of child pornography and luring a child for sexual purposes. Staff Sgt. William Donnelly with Windsor police said additional arrests are possible, but that could take awhile as police sift through child porn photos that are "traded around like hockey cards." Windsor Star, A5

Alleged cyber sicko
She thought she knew him and she wasn't alone. Toronto Police claim many teen girls across the country met Alex Sirop online and believed he was a good-looking 19-year-old. They had no idea when they sent "compromising" images of themselves over the web that a 42-year-old Scarborough man named Shiraz Nariman was allegedly adding them to his collection of child porn. Nariman is one of 54 people rounded up recently by police in Ontario during a massive child pornography sweep. The RCMP first learned of him when a teenage girl, who can't be named, came forward in September 2010. Toronto Sun, 7; Toronto Star

Man charged with making child porn
A man has been charged with producing child pornography following a year-long investigation by the Edmundston City Police Force and the New Brunswick RCMP's Internet Child Exploitation Unit. Shane Evan McCabe, 34, of no fixed address, was arrested on Thursday upon his release from jail where he was serving time for failing to register with the National Sex Offender Registry for past convictions. The investigation began in March 2011 when images of child sexual abuse were found scattered around the City of Edmundston. The Fredericton Police Force, the RCMP's Technological Crime Unit, the National Child Exploitation Coordination Centre, the Canadian Centre for Child Protection (cybertip.ca), the RCMP's Violent Crime Linkage Analysis System and the National Sex Offender Registry also assisted with the investigation. Times & Transcript, A9

Two grow-ops found same day
London police busted two marijuana grow-ops in less than three hours, seizing nearly $600,000 in drugs. Both grow operations, located less than eight kilometres apart, were in middle-class north London neighbourhoods. London Free Press, A8

Police reveal drug lab photos to highlight ecstasy dangers
Filthy conditions, unknown chemicals and a pill press covered in ecstasy: this is what a drug lab looks like. In their latest effort to showcase the dangers associated with street drugs, police released photographs on Friday of an ecstasy lab in Richmond, B.C., in light of the many deaths in Calgary and B.C. tied to ecstasy laced with a toxic chemical. Seven people in Calgary, and one person in Red Deer, have died from taking ecstasy (MDMA) laced with para-methoxymethamphetamine (PMMA). Two additional cases are still awaiting toxicology results. There have been five deaths reported in B.C. The chemical, a cheaper alternative than MDMA, is being cut into ecstasy, but is believed to be more toxic. B.C. RCMP Sgt. Duncan Pound said when officers entered the lab in full protective suits in 2008, they found 750,000 pills and enough drugs to make 3.3 million tablets. Calgary Herald, B1

Date-rape drugs among $17K bust
Mounties in Red Deer say they've made a major seizure of so-called date rape drugs that were meant to be trafficked. On Thursday, Mounties executed a warrant on a Red Deer residence, where a search turned up two kinds of drugs known to be used to incapacitate unwitting victims who are then sexually assaulted. In the search of the house and garage, they found three litres of gamma hydroxybutyric acid (GHB), as well as 10.8g of ketamine, which can be slipped into drinks. Calgary Sun, 20

Remains found on reserve
Human remains have been found in a vacant home on the Nak'azdli reserve in B.C., RCMP said Friday. The remains were reported to police Wednesday afternoon. The reserve is located about 150 km northwest of Prince George. It is considered a suspicious death at this point, Corp. Annie Linteau said. Edmonton Sun, 23

Civilian oversight of police a must

An opinion piece states, "The continuing fall-out over the violent arrest of Adam Nobody during the G20 raises serious doubts about the adequacy of civilian oversight of the police. Eighteen months later, one officer, Const. Babak Andalib-Goortani, has been charged criminally with assault by the province's Special Investigations Unit. Another provincial body, the Office of the Independent Police Review Director, has recommended Andalib-Goortani and four others -- Constables Michael Adams, David Donaldson, Geoffrey Fardell and Oliver Simpson -- face disciplinary charges. But the SIU says since the standard of evidence for identifying officers is higher for a criminal case than disciplinary hearings, no new criminal charges will be laid... But the larger issue is the lack of co-operation the SIU has received from police, not just in G20 cases in Toronto, but across the province." Ottawa Sun, 12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Deportation for dirtbag
Clato Mabior's time on Canadian soil appears to be quickly winding down. Mabior, convicted of aggravated sexual assault for failing to disclose his HIV status to sexual partners, will be deported to Sudan in the next 30 days -- likely on Feb. 15, according to his immigration lawyer. Mabior, 34, was ordered held in custody at a review of his ongoing detention Friday. He's been behind bars on the strength of a deportation order since October 2010. The Immigration and Refugee Board has repeatedly ruled that Mabior is a flight risk and a danger to the public. Winnipeg Sun, 3

The hangover
On May 13, 2011, a prominent Canadian DJ crossed the Alberta-B. C. border near Lake Louise with a case of red wine, daring authorities to arrest him. The Mounties refrained but Terry David Mulligan had made a point of mocking a lingering hangover of Alberta alcohol prohibition 87 years after its repeal. Yet, it's still illegal to cross provincial borders with booze. While flamboyant bootleggers such as Al Capone, furtive speakeasies and rumrunners are colourful legends of the 1920-1933 U.S. prohibition, Canada's own doomed attempt at shutting off the taps has barely had a last recall. Calgary Sun, 18

Mugesera finally finds Rwandan lawyer
Rwandan lawyers haven't been lining up to defend Léon Mugesera - wanted for almost two decades for his role in the 1994 Rwandan genocide - but one has stepped forward, despite possible security issues and little pay. Guy Bertrand, the Quebec City lawyer who helped the suspected war criminal dodge deportation from Canada for years, said it was difficult to find someone willing to take on his client. He fears for the Rwandan attorney's safety but can't afford to hire a bodyguard. For security reasons, Bertrand didn't want to reveal the lawyer's name or put The Gazette in touch with him, but Rwandan news organizations reported he is Donat Mukunzi. Montreal Gazette, A8

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

VICTIMS TREATED CRIMINALLY
It's about time someone started talking about the rights of victims in the criminal justice system. Canada's ombudsman for victims' rights Sue O'Sullivan released a special report this past week on the need for governments, the courts and corrections to start taking the rights of victims of crime far more seriously than they have in the past. And her report is bang-on. I recommend every elected official in Canada read it. I've met enough victims of crime over the years to know exactly what O'Sullivan is talking about. We spend a lot of time in the justice system dealing with the criminals themselves -- their sentences, their rights, etc. -- but not enough time ensuring victims have the legislated rights they deserve. Winnipeg Sun, 5

Group aims to 'out' pedophiles
A Christian-oriented activist group said Friday it plans to launch a website for identifying pedophiles. Canada Family Action said its website will be called FindA-Pedophile.com. Brian Rushfeldt, president of the organization, said he hopes to have the site operational by March. The Calgary-based group said the recent bust of 60 people in Ontario on hundreds of child pornography charges is proof that such a resource is needed. Rushfeldt said the information will be gathered from sources such as the courts, police and media reports. Montreal Gazette, A15; Ottawa Sun

Quebec man wants senator prosecuted for suicide comments
A Quebec man has filed a police complaint against Conservative Senator Pierre-Hugues Boisvenu for remarks he believes could lead someone to commit suicide. The complaint came after Boisvenu said Wednesday in Ottawa that some convicted killers - he referred specifically to Paul Bernardo, Clifford Olson and Robert Pickton - should be given a rope in their prison cells in case they want to hang themselves. The senator later apologized for his comments, but 26-

year-old Jacques McBrearty said Boisvenu went too far. The Sûreté du Québec will investigate the complaint, which could eventually be handed over to the RCMP since the events occurred in Ontario, where Boisvenu lives. Montreal Gazette, A10

Kamloops jail too easy to break in to
A review conducted before two recent break-ins at the Kamloops Regional Correctional Centre, apparently to smuggle contraband - possibly drugs - to prisoners, revealed the Interior British Columbia jail must beef up its security practices. Dean Purdy, spokesman for the B.C. Government Employees' Union, said in each case someone scaled the jail's two-metre high perimeter fence and cut a hole in a cell window in the segregation unit. Early reports suggested a laser was used to drill into one of the pieces of Lexan glass. The Daily News has learned a blowtorch was used. Purdy believes the breaches were made to smuggle contraband - possibly drugs - into the prison. The incident raises alarm bells for the union, which is conducting its own investigation along with the province's corrections branch and RCMP. Edmonton Journal, A19

No honour in killing
Imams across North America are condemning the act of "honour killing" on the heels of the guilty verdict and life sentences handed to the Shafia family last Sunday. Mohammad Shafia, 59, his second wife Tooba Mohammad Yahya, 42, and the couple's son, Hamed, 21, were each convicted on four counts of first-degree murder for killing Shafia daughters Zainab, 19, Sahar, 17, Geeti, 13, and Mohammad's first wife, Rona Amir Mohammad, 52. "There is no such thing in Islam that if somebody is bringing disgrace to your family's honour that you go out and kill that per-son," said Imam Syed Soharwardy, founder of the Islamic Supreme Council of Canada. Soharwardy will be issuing a Fatwa on Saturday, a type of religious edict, with more than 34 signatures from imams across North America supporting its position against honour killings, domestic violence and misogyny. Toronto Sun, 9

Des propos condamnables
Une article d'opinion dit, «Une fois de plus, une personnalité publique, en l'occurrence un sénateur bien connu au Québec, s'enflamme et tient des propos qui ne devraient jamais sortir de la bouche d'une personne qui exerce une aussi grande influence sur l'opinion publique. Bien que l'incommensurable souffrance associée à la perte d'un enfant puisse nous amener à comprendre ses motivations profondes, il n'en demeure pas moins que ce genre de propos qui viennent plus du coeur que de la tête sont condamnables lorsqu'on occupe une position politique importante. Cette idée de laisser une corde dans la cellule des criminels ayant commis un homicide est barbare et rétrograde et n'a pas sa place dans une société moderne comme la nôtre.» Le Nouvelliste, 21

PUBLIC SERVICE / FONCTION PUBLIQUE

Whistleblowers in public service face reprisal: integrity group
Public servants who disclose wrongdoing invariably face workplace reprisals despite laws promising protection, says the head of an organization that promotes integrity and accountability within government. David Hutton, executive director of FAIR (Federal Accountability Initiative for Reform), said he's received hundreds of calls from whistleblowers since assuming his volunteer position in 2008. In some jurisdictions, those who punish whistleblowers can lose their jobs, go to jail and be sued. Australia and Britain are "decades ahead of us" in comparison to the "absolutely dreadful" whistleblower law in Canada, Hutton said. He was responding to a report, prepared for the Office of the Public Sector Integrity Commissioner, which says government employees fear career-limiting reprisals if they blow the whistle on wrongdoers in the federal public service. The report summarizes the findings of 10 focus groups held last November to explore public servants' perceptions about disclosing wrongdoing in their workplaces. It paints a picture of a public service that recognizes its responsibility to disclose wrongdoings, at least in principle, but is fearful of the consequences. Ottawa Citizen, A3

INTERNATIONAL / INTERNATIONAL

Inquiry urged over bribery case
Indian opposition leaders are calling for a government inquiry into allegedly corrupt dealings at the country's Ministry of Civil Aviation, following a Globe and Mail report on bribery and bid-rigging allegations that implicate, among others, cabinet minister Praful Patel. The Globe has detailed the allegations against Nazir Karigar, a 64-year-old Indian-born Canadian citizen and the first individual to be charged under Canada's foreign bribery law - the Corruption of Foreign Public Officials Act. As part of its case against Mr. Karigar, the Royal Canadian Mounted Police alleges that he divulged to others that he had channelled a $250,000 bribe to Mr. Patel while he was minister of Civil Aviation, with the help of a political ally, in 2007. Mr. Patel, who is now Heavy Industries Minister, has said he had no knowledge of the scheme.

There is no evidence that he accepted the money. The story dominated the Indian media Friday as supporters from the ruling Nationalist Congress Party (NCP) and the government rose to his defence. Globe and Mail, A15

OTHER / AUTRE

Ottawa a fait la promotion des aliments du Canada après le tsunami au Japon
Ottawa a vu dans le violent séisme et le tsunami survenus l'an dernier au Japon une occasion d'aiguiser l'appétit pour la cuisine canadienne. Le gouvernement fédéral a en effet proposé une activité pour faire la promotion de «la marque Canada» sur le marché japonais. Le plan visait à faire connaître des produits comme le sirop d'érable du Québec, le boeuf de l'Alberta et d'autres denrées aux personnes laissées sans abri par la catastrophe. Selon des documents obtenus par La Presse Canadienne, le Canada devait démontrer son appui en organisant un café en plein air et en nourrissant des victimes avec des produits canadiens afin qu'ils puissent se sentir comme s'ils étaient en visite au Canada. L'Acadie Nouvelle, 9; Whitehorse Star

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From: [redacted]
Sent: February-05-12 7:26 PM
To: Listserver NCSIP
Subject: Anonymous hacks Police websites, FBI

s.13(1)(a)
s.16(2)(c)

This message sent from: [redacted]

---

http://www.cbc.ca/news/technology/story/2012/02/03/tech-anonymouse-hacking-fbi.html

[redacted]

You are currently subscribed to [redacted]

To unsubscribe click here:

[redacted]

(It may be necessary to cut and paste the above URL if the line is broken)

or send a blank email to [redacted]

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-05-12 8:29 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
February 5, 2012 / le 5 février 2012

MINISTER / MINISTRE

Letters to the Editor Column
A letter written by **Public Safety Minister Vic Toews states**, "NDP MP Pat Martin (Winnipeg Centre) once again demonstrated his willingness to use inappropriate language and engage in vicious personal attacks when he used an obscenity to refer to Senator Pierre-Hugues Boisvenu on Wednesday. Martin previously refused to apologize for his use of social media to direct obscenities at those who have challenged him. The NDP and MP Martin should apologize for the shameful personal attack that has been directed at Senator Boisvenu. Pat Martin's constituents, and indeed all Canadians, would be better served if the MP and his soft on crime party, would direct their outrage and vitriol at the criminals who victimize innocent, law-abiding Canadians rather than at a Senator whose family has suffered a terrible loss at the hands of a repeat offender." Winnipeg Sun, 12

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

No damage reported from 5.6 earthquake
A noon shaker off Ucluelet Saturday went largely unnoticed by most of the town's residents. The 5.6-magnitude earthquake was logged by Natural Resources Canada at 12: 05 p.m. The epicentre was about 180 kilometres west of Ucluelet and 337 kilometres west of Victoria, at a depth of 12.8 kilometres. The relatively mild strength and distance meant there was no risk of a tsunami and no damage reported, said Taimi Mulder, federal earthquake seismologist. In the Officials Sports Lounge in Ucluelet, manager Dale Holliday didn't feel the earth move and neither did his customers. At the Water's Edge Resort, the reaction was much the same. Times Colonist, A6; Edmonton Sun; Le Journal de Montréal

CYBER SECURITY / CYBERSÉCURITÉ

WORLD IN BRIEF
A group linked to the hacker network Anonymous on Saturday said it attacked the Swedish government's website, bringing it down for periods of time by overloading it with traffic. CyberForce used Twitter to claim responsibility, saying "We have succeeded in the attack against the government." It also indicated it may launch more attacks at around midnight Saturday, saying "this op starts at 24.00," but it was not immediately clear whom the targets for those attacks may be. The group said it had used a denial of service attack against the government, which essentially swamps a website with false users. Chronicle-Herald, A8

Hackers post audio of FBI secret call
Hacker group Anonymous, in an embarrassment for law enforcement, released a recording Friday of a conference call between the FBI and Scotland Yard discussing operations against the hacking collective. The Federal Bureau of Investigation confirmed the authenticity of the nearly 17-minute recording posted on YouTube and other sites and said it was "intended for law enforcement officers only and was illegally obtained." "A criminal investigation is under way to identify and hold accountable those responsible," the FBI said in a statement. Along with the audio recording, Anonymous also posted online the email invitation from an FBI agent setting up the call for Jan. 17. According to the FBI, no agency computer systems were breached in connection with the incident. Graham Cluley of computersecurity firm Sophos said the hackers were apparently able to access the call "because they have compromised a police investigator's email account." The Province, A22

Online activists claim to name Alberta white supremacists
Calgarians whose names have been connected to neo-Nazi and white-supremacist groups are angry that their personal identification has been published on the Internet. Earlier this week, an informal computer hacking collective that operates under the name "Anonymous" released the addresses and phone numbers of thousands of people who had registered with websites affiliated with white-supremacist causes. Of the more than 70 Canadian residents revealed, more than a dozen were listed in Calgary and Edmonton. Kelly Ernst, a board member with the Rocky Mountain Civil Liberties Association, agreed the computer collective went too far. Calgary Herald, A3

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

RCMP struggling to fill jobs, internal documents show
Internal RCMP documents show the force scrambling to fill jobs in B.C. despite years of warnings that chronic understaffing is putting police and the public at risk. One in 10 Mountie positions in B.C. sits empty, says a management report obtained by the Times Colonist. Jobs left unfilled due to medical, parental and other forms of extended leave push the vacancy rate to almost 16 per cent provincewide and to 17.4 per cent on Vancouver Island. It raises the question of how the RCMP would come up with the officers to create a new 35-member detachment in Esquimalt, should the provincial government agree to that municipality's decision to do so. A separate but similar 2007 report warned that the RCMP risked burning out its members because their workload was growing while the number of resources thinned. Yet it's clear the problem has not been addressed in many areas of B.C., with detachments regularly calling in officers on overtime or having to borrow members from other detachments to reach minimum staffing levels. But RCMP brass aren't willing to acknowledge shortages are affecting front-line policing. Liberal Senator Colin Kenny, who has said for years the national force is understaffed by 5,000 to 7,000 officers, said the officer shortage will get worse in years to come as more senior officers retire. Instead of the Conservative government passing tougher laws which will put more people behind bars, it should be investing in more national police officers to prevent crime, Kenny said. Times Colonist, A1

Island Mounties run off their feet
In Duncan, RCMP officers are running from call to call, scrambling to keep up and letting the proactive policing that can prevent crime fall by the wayside. In Sooke, the detachment commander routinely calls in Mounties on overtime, including from other detachments, as well as reserve constables just to avoid falling below minimum staffing levels. These are scenarios reflected in internal RCMP documents that show one in 10 Mountie positions in B.C. are vacant. Staffing shortages are even higher due to officers off work on extended leave. The shortage of Mounties has been a long-running concern for the province and the municipalities that contract with the RCMP and pay up to 90 per cent of policing costs. Yet the Mounties pursued the contract to police the Town of Esquimalt, promising 35 officers and a stand-alone detachment for the municipality, which has a population of 17,000 in an area of seven square kilometres. Chief Supt. Kevin DeBruyckere, in charge of career development and resourcing for the RCMP in B.C., said he doesn't see systemic vacancies that would prevent the force from entering into a contract with a municipality the size of Esquimalt. B.C.'s director of police services, Clayton Pecknold, was not available for an interview. A spokeswoman for the Public Safety Ministry said the province is aware of staffing shortages in the RCMP and said it is up to local detachment commanders to address the shortfalls with their mayors. Times Colonist, A3

Small-town Mounties pushed to the limit
Their combined ranks are barely enough for a pickup hockey game, yet officers from a pair of small-town RCMP detachments in southern Alberta found themselves involved in two of the largest investigations in recent memory. On most days, the 10 RCMP officers working in Claresholm and Vulcan are enough to handle the routine complaints common in small-town policing. But a mass murder on the highway outside Claresholm and the abduction and killing of a Vulcan-area senior just three weeks apart tested not only the mettle of those RCMP officers, but also the organization's ability to respond. At their height, both cases involved dozens of investigators drawn from RCMP units across the province. But each also began with a lone officer who, despite being more accustomed to handling complaints about traffic and vandalism, had the training to recognize a major event unfolding. While small towns aren't immune to crime, homicides and serious offences are relatively rare. When they happen, detachments rely on specialized RCMP units based in larger centres. Calgary Herald, A3

SYRIAN EMBASSY VANDALIZED IN OTTAWA: PROTESTERS COMMEMORATE 1982 HAMA MASSACRE
The Syrian Embassy in Ottawa was splashed with what appears to be red paint on Saturday. Protesters held a demonstration in front of the embassy - located in midtown Ottawa, about 10 blocks from Parliament Hill - Saturday morning to commemorate the 1982 Hama Massacre, an uprising in which thousands died, and the events that took place Friday in the Syrian city of Homs. A large quantity of red paint covered the embassy door, mailbox, gates and canopy of the embassy's main entrance Saturday afternoon. The gates to the embassy were locked and nobody was available to

speak about the incident. An RCMP officer photographing the vandalism would not comment. Ottawa Citizen, A1; Toronto Star

Five young men missing
The Vancouver police's missing persons unit is calling for tips on five unsolved cases from 2011 - all young men. Foul play is not suspected in any of the cases at this time, Sgt. Kirk Star said Friday. There were 3,700 missing-person reports last year, Star said. The current inquiry into Vancouver's missing women and flawed Vancouver Police Department and RCMP investigations into Robert Pickton is ongoing, and will make recommendations around improving systemic issues in policing. Star said he is reluctant to comment on the inquiry. The Province, A15

Police drug lab photos highlight dangers
Filthy conditions, unknown chemicals and a pill press covered in ecstasy: this is what a drug lab looks like. In their latest effort to showcase the dangers associated with street drugs, police released photographs Friday of an ecstasy lab in Richmond, B.C., in light of the many deaths in Alberta and B.C. tied to ecstasy laced with a toxic chemical. Seven people in Calgary, and one person in Red Deer, have died from taking ecstasy (MDMA) laced with para-methoxymethamphetamine (PMMA). Two additional cases are still awaiting toxicology results. There have been five deaths reported in B.C. The chemical, a cheaper alternative than MDMA, is being cut into ecstasy. B.C. RCMP Sgt. Duncan Pound said when officers entered the lab in full protective suits in 2008, they found 750,000 pills and enough drugs to make 3.3 million tablets. Edmonton Journal, A5

The ecstasy and the agony
Not so long ago, Myles Murphy popped "E" caps like they were candy. These days, however, the gregarious 19-year-old from Abbotsford has a different take on the so-called "love drug" that is so popular among clubbers and partygoers and whose properties, it is commonly said, jack up the senses to the point where you can "see the music" and "hear the colours." The warning is being echoed by police and public health officials in the wake of a spate of ecstasy-related deaths in Western Canada. It is possible, police and health officials say, that a crackdown on precursor chemicals used to make methylenedioxymethamphetamine, or MDMA - which is ecstasy in its traditional or pure form - has led drug producers to turn to other synthetic drugs, such as PMMA. It is also possible that inexperienced producers intended to add meth into the toxic blend but ended up creating PMMA by accident. Ottawa-based RCMP Cpl. Luc Chicoine, a synthetic-drug expert who provides support to the force's drug investigators, said MDMA is made by mixing MDP2P, a light oil extracted from the bark of a tree, with various chemicals common in paint thinners and drain cleaners. The solution is then mixed with hydrochloric acid to turn it into a powder, which can be consumed as a powder or pressed into tablets or wrapped in capsules. The Province, A4; Calgary Sun

Two men charged in $4M fraud
Two Quebec men face fraud charges following an investigation by the RCMP into a mortgage scam that cost victims more than $4 million. Kinh Ho Quan, 56, and Hermel Bosse, 58, were arrested this week on charges alleging they took part in at least 20 fraudulent transactions totalling nearly $4.5 million and bilked individuals, financial institutions and the Canada Mortgage and Housing Corporation, which provides mortgage loan insurance. According to a news release, the RCMP's Major Fraud Unit of Commercial Crime Section of Montreal probed a total of 80 suspicious transactions worth an estimated $18 million since the investigation was launched in April 2008. The RCMP said many have since had to declare bankruptcy and saw their credit history ruined. The RCMP warn that mortgage fraud "is a form of crime increasingly observed by police." Ottawa Citizen, A3

Cops should collect race stats: study
Canadian police departments should collect race-based crime data, two Ontario criminologists say. Akwasi Owusu-Bempah, a doctoral candidate at the University of Toronto's Centre for Criminology, and Paul Millar, a criminal justice professor at Nipissing University, make their controversial argument in a report titled Whitewashing Criminal Justice in Canada: Preventing Research through Data Suppression. The study appears in the current issue of the Canadian Journal of Law and Society. Edmonton Sun, 29

Man charged after four-year-old approached by suspicious Santa
Police in B.C. have arrested a suspect in a case where a man allegedly tried to lure a child by claiming he was Santa. David Warren Buchanan, 67, has been charged with two counts of attempted child abduction and police say he is a suspect in a third case. Buchanan was arrested Friday in Penticton, B.C., after RCMP spotted his vehicle outside a hotel. Chronicle-Herald, A4; Edmonton Sun

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Prison contraband soars
Cocaine, alcohol, explosives, knives and handcuff keys are part of the haul at federal prisons as officials across the country struggle with a rising tide of contraband. Between 2007 and 2011, the amounts of drugs, intoxicants, weapons and other unauthorized items confiscated by prison staff has steadily risen, in some cases by more than 170 per cent, according to documents obtained by the Star. The number of seizures of intoxicants, for example - LSD, THC, amphetamines and steroids, to name just a few - rose to 1,779 in 2010-11, up from 1,295 three years earlier. Similarly, the number of seizures of weapons, including razor blades, homemade knives, firearms, explosives and pipes, rose by 22 per cent to 900 over the same period. Perhaps most striking is the surge in seizures of other unauthorized items, such as cellphones, tattoo-making materials, lock picks and rope, from 991 to 2,697. "I suspect that detection is getting better, so you do see an increase in seizures," said Howard Sapers, Canada's Correctional Investigator. "What we really don't know is whether drug use inside prisons is up or down, whether the presence of weapons is greater or lesser than it used to be." The Star also asked the Correctional Service of Canada for the number of employees disciplined for bringing contraband items into prison, but the agency said it did not have any such records. However, last September, CSC commissioner Don Head told a parliamentary committee that it had dismissed 12 staff members that year for smuggling contraband into prisons. CSC could not provide the Star with budget expenditures for 2010-11 due to "temporary technical issues," but a 2010 overview of the agency pegs total corrections expenditures 2008-09 at $2.28 billion, up nearly 40 per cent since 2004-05. The average cost of keeping an inmate incarcerated rose from $87,919 to $109,699. Toronto Star, A11

34 imams condemn 'honour' killings
More than 30 American imams signed a fatwa Saturday condemning honour killings, after a Canada court convicted Afghan immigrants for murdering four female relatives accused of damaging the family's reputation. ISCC founder Syed Soharwardy, said the group put out the fatwa "because of the Shafia trial, because it has been a large focus [for] the Islamic community and people said a lot of things," adding that imams wanted to clear up "some misunderstandings about Islam" by non-Muslims. The Province, A21; Toronto Star; Chronicle-Herald; Le Soleil; Le Journal de Montréal

Sicko ID site
Plans by a Calgary-based group to out convicted pedophiles are raising questions among lawyers and police who monitor sex offenders. Canada Family Action, a Christian group, plans to launch findapedophile.comnext month, a site aimed at educating the public on how to identify potential victims and share convict information. It said the idea stems from their belief the sex offender registry is inadequate and not available to the public. Calgary lawyer Raj Sharma scoffed at the plans. RCMP said they haven't heard any details on the site, but the concept is raising questions. Sgt. Rich Veldhoen with Calgary police high-risk offender program believes efforts already in place to monitor violent and sex offenders in the community are working. Calgary Sun, 3

The 'just' punishment that dares not speak its name
An opinion piece states, "Senator Pierre-Hugues Boisvenu was wrong to suggest vicious killers be offered a rope. They shouldn't have any choice in the matter. His suggestion, since retracted, was technically flawed because it's illegal to counsel suicide in this country. It's apparently OK to say if people aren't as sharp, limber, sexy and healthy as they used to be, they should be allowed to off themselves. Just not Paul Bernardo, Clifford Olson or Mohammad Shafia. But clearly most of the beautiful people's objections weren't on this narrow ground. Rather, they found the suggestion too, too shocking." Ottawa Sun, 16

INTERNATIONAL / INTERNATIONAL

Russia, China veto UN resolution on Syria
Russia and China vetoed on Saturday a UN resolution that backed an Arab plan calling on Syrian President Bashar al-Assad to quit, stalling global efforts to end his bloody crackdown on unrest after hundreds were reported killed in the city of Homs. The veto left Canada "disappointed in the extreme," Foreign Affairs Minister John Baird said Saturday. Ottawa Citizen, A1

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-06-12 8:50 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted]; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted]; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 6, 2012 / le 6 février 2012

Print Media / Médias imprimés

Neo-Nazi IDs listed
Calgarians whose names have been connected to neo-Nazi and white-supremacist groups are angry that their personal IDs have been published on the Internet. The computer hacking collective "Anonymous" released the addresses and phone numbers of thousands of people who had registered with websites affiliated with white-supremacist causes. The sites included Blood and Honour and Local 1488. Calgarian Ryan Lorentz said he doesn't know how his name appeared on one of the lists: "I have no idea what that website is." Calgary Herald

Hackers Wiretap FBI Conference Call
The international hackers group known as Anonymous turned the tables on the Federal Bureau of Investigation by listening in on a conference call last month between the bureau, Scotland Yard and other foreign police agencies about their joint investigation of the group and its allies. Anonymous posted a 16-minute recording of the conference call on the Web Friday and crowed via Twitter: "The FBI might be curious how we're able to continuously read their internal comms for some time now." An FBI official said Anonymous had not hacked into the conference call or any other bureau facilities.

Instead, it had obtained an email giving the time, telephone number and access code for the call. "It's not really that sophisticated," said the official. National Post

Online Media / Médias en ligne

Anonymous takes down official Homeland Security website
The U.S. Department of Homeland Security's official website DHS.gov was hacked on Friday afternoon, and Anonymous is claiming responsibility. Also on Friday, Anonymous released an audio recording of a January conference call between FBI agents and Britain's Scotland Yard in which the hacktivist group Anonymous was discussed. The FBI released a statement confirming the authenticity of the recording and has since shifted its investigation to how hactivists linked to the Anonymous network managed to intercept a conference call. In the FBI statement, officials said: "The information was intended for law enforcement officers only and was illegally obtained. A criminal investigation is under way to identify and hold accountable those responsible." Examiner.com

German gov't endorses Chrome as most secure browser - Federal security agency touts sandbox, silent update as features that keep citizens safer online
Germany's cyber security agency today recommended that Windows 7 users run Google's Chrome browser, citing the application's sandbox and auto-update features. In a security best practices guideline, Germany's Federal Office for Information Security, known by its German initials of BSI, said Chrome was the best browser. "Your internet browser is the key component for the use of services on the Web and thus represents the main target for cyber-attacks," said BSI in its published advice. "By using Google Chrome in conjunction with the other measures outlined above, you can significantly reduce the risk of a successful IT attack." BSI ticked off Chrome's anti-exploit sandbox technology, which isolates the browser from the operating system and the rest of the computer; its silent update mechanism and Chrome's habit of bundling Adobe Flash, as its reasons for the recommendation. Computerworld

Kelihos : pas de résurrection mais un nouveau malware
Microsoft dément un retour aux opérations du botnet Kelihos. Un nouveau malware ayant des similitudes avec Kelihos est toutefois apparu. La firme de Redmond revient sur la cas de Kelihos pour apporter des précisions. Pour Microsoft, qui a œuvré au démantèlement du botnet avec l'aide de Kaspersky Lab et Kyrus Tech, le botnet n'a pas ressuscité. « À l'heure actuelle, Kaspersky Lab et Microsoft n'ont aucune preuve que le botnet qui a été démantelé en septembre 2011 est retourné sous le contrôle de cybercriminels ou a repris des activités de spam » Génération-NT

Spammers exploit calendar events
Spammers are using holidays and major events to make their mail more appealing. This is according to the Symantec.cloud Intelligence Report, which shows that more than 10 000 unique domain names were compromised with a redirect script written in PHP that contained a reference to the New Year in the file name. These redirect scripts were hosted on compromised Web sites, and links to these were included in spam e-mails, says Symantec. IT Web Security

Hackers may be able to 'outwit' online banking security devices - Investigators probe malware threat to 2-factor authentication
Hackers may already able to use malware to outwit the latest generation of online banking security devices, security watchers warn. An investigation by BBC Click underlines possible shortcomings in the extra security provided by banking authentication devices such as PINSentry from Barclays and SecureKey from HSBC. Using such two-factor authentication devices means that even if hackers trick consumers into handing over their bank login passwords they still won't be able to raid online banking accounts. UK Register

Google launches Android Bouncer
Google has announced its "Bouncer" service which scans for malicious software on Android smartphones amid a massive spike in use of the phones. "Here's how it works: Once an application is uploaded, the service immediately starts analysing it for known malware, spyware and trojans. It also looks for behaviours that indicate an application might be misbehaving, and compares it against previously analysed apps to detect possible red flags," Hiroshi Lockheimer, Android vice-president of engineering wrote on the Google blog. Google has come out fighting suggestions that its Android platform poses a security threat to smartphones. News 24 (South Africa)

Android : Counterclank ne serait pas un cheval de troie, Symantec se rétracte et rejoint l'avis de Lookout
Le cheval de troie Counterclank découvert par Symantec n'aurait en effet pas des fonctionnalités malveillantes selon la firme de sécurité qui revient sur sa position. Counterclank avait été identifié au sein de 13 applications populaires et aurait infecté près de cinq millions de terminaux Android selon Symantec. Le malware lit les données comme l'historique du navigateur, les informations d'identité, les données de localisation, etc., et transmet celles-ci à un serveur distant. L'éditeur Lookout Mobile avait par contre identifié Counterclank comme appartenant à un réseau de publicité agressif.

Symantec rejoint donc la position de Lookout, et pense que le code d'Android. Counterclank proviendrait d'un kit de développement logiciel (SDK), distribué aux tiers pour les aider à monétiser leurs applications principalement par la recherche. Développez.com

Un trojan polymorphe sur Android détecté par Symantec
Des chercheurs de Symantec ont identifié un trojan pour Android qui envoie des SMS à des numéros surtaxés. La particularité de ce trojan est qu'il modifie son code à chaque fois qu'il est téléchargé pour contourner les antivirus. Symantec lance un avertissement sur l'apparition d'un cheval de Troie pour Android qui envoie des SMS à des numéros surtaxés. Le virus modifie son code à chaque téléchargement. Cette technique est connue comme le polymorphisme serveur et a existé pendant des années sur les malwares pour PC. Les cyber-criminels commencent à l'adopter pour les mobiles. A la différence du polymorphisme local où le malware modifie son code à chaque fois qu'il est exécuté, le polymorphisme serveur transforme certaines parties du cheval de Troie à chaque téléchargement. Le Monde Informatique

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From: Moore, Bruce
Sent: February-06-12 7:50 AM
To: [redacted]
Subject: FW: Anonymous info..

s.13(1)(a)
s.15(1) - Int'l
s.16(2)(c)

From CPNI.

Bruce

-----Original Message-----

[redacted]

Page 2045

is withheld pursuant to section

est retenue en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Hayward, Jane

From: Glazer, David on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-06-12 8:10 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
February 6, 2012 / le 6 février 2012

MINISTER / MINISTRE

Harsher sentences for pot growers than for pedophiles caught PM's eye
Media reports that some pot growers will face harsher mandatory-minimum sentences than child rapists under the Conservative government's new crime bill were enough to catch the attention of Prime Minister Stephen Harper. A request by The Canadian Press for cabinet records on the controversial omnibus crime legislation turned up a single document - much of it blacked out under a broad, discretionary exemption in the Access to Information Act. The Oct. 11, 2011, "memorandum for the prime minister" says its purpose was to inform Harper about the controversial sentencing provisions "in light of recent criticism in the media." Bill C-10, the omnibus crime bill, is currently being studied by the Conservative-dominated Senate, where Justice Minister Rob Nicholson has confirmed some flaws will be corrected. **Public Safety Minister Vic Toews** attempted to have those amendments adopted in late November after the bill had left the House of Commons justice committee, but was ruled out of order by the Speaker. Red Deer Advocate, D4 (The Telegram)

Un bateau nauséabond
Ce sont les deux bateaux par lesquels le scandale a été créé. Les bateaux dont s'est servi le gouvernement Harper pour monter son propre bateau justifiant l'injustifiable. L'Ocean Lady, en octobre 2009. Puis, le MV Sun Sea, en août 2010. A bord de ces deux navires qui ont atteint les côtes de la Colombie-Britannique, 600 demandeurs d'asile du Sri Lanka. Ces bateaux ont été érigés en symbole par le gouvernement conservateur. Épouvantails commodes pour qui veut bafouer les droits des réfugiés, préjugés en vogue à l'appui. Les voyant arriver, **le ministre de la Sécurité publique Vic Toews** a tout de suite brandi la menace de l'invasion. Il a dit craindre que d'autres bateaux remplis de Tamouls prennent d'assaut le Canada. Il a invoqué d'importants problèmes de sécurité, des liens avec des organisations terroristes... La Presse, A3

*** Pedophile site appears legal**
Alberta's top cop doesn't think plans for a controversial website outing convicted pedophiles will run into any legal roadblocks. Solicitor General Jonathan Denis, who's also a lawyer, said while he doesn't necessarily support the move by Canada Family Action, a Christian group set to launch findapedophile.com next month, he doesn't think there will be any legal impediments. Denis also met with federal **Public Safety Minister Vic Toews**, who was very supportive of the proposal. Calgary Sun, 5

*** Prison porn pervert - Sex-killer claiming to embrace aboriginal culture a slammer smuggler**
A Haitian-born sex-killer's embrace of Canadian aboriginal traditions and culture didn't stop him from breaking prison rules by hoarding and displaying porn in his cell, helping an inmate smuggle booze and becoming involved in a jailhouse disturbance over the last few years. Gregory Bromby's recent bid for day parole from a federal prison in Manitoba made national headlines after he was granted a culturally-sensitive, "elder-assisted" hearing despite not being aboriginal. His being allowed to make use of the forum sparked outrage from the father of Tara Manning, the 15-year-old girl Bromby sexually assaulted and stabbed 51 times in the mid-90s. **It also drew concern and a promise of parole reform from the office of federal MP and Public Safety Minister Vic Toews.** Winnipeg Sun, 3 (Edmonton Sun)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Top security for bird flu studies**
If Canadian scientists want to conduct research on H5N1 flu viruses modified to enhance their ability to spread, the work will have to be done in laboratories with the top level of biosecurity, the Public Health Agency of Canada says. For the

time being, the advice is moot; the viruses in question are locked up in labs in the Netherlands and the United States. And while controversy rages over whether the teams that created them should be able to publish their work in scientific journals, it's unlikely those labs will share samples, especially across international borders. Red Deer Advocate, D5

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Alleged terrorist's partner wrestles with competing realities
Mr. Sharif has sat in an Edmonton jail since his arrest as the United States attempts to have him extradited to face seven terrorism-related charges in New York state. In December, U.S. President Barack Obama signed a new law into effect allowing accused terrorists to be held indefinitely in military prisons if they're tied to al-Qaeda or related terrorist groups. Justice Canada doesn't believe it would apply in this case, but some lawyers and observers say that's simply wrong. The law is, at best, untested and murky, and Mr. Sharif could be held. Canada doesn't extradite people if they'll face the death penalty. Indefinite detention, however, is new ground. And the only thing standing between Mr. Sharif and that possible fate under an unproven law is a brief extradition hearing and the chance of potential intervention, however slim, by Justice Minister Rob Nicholson, who signs off on all extraditions. Globe and Mail, A8

*** Terror arrest a wake-up call: Expert**
Finding foreign terrorists on home soil should come as no shock to Canadians who may be partially to blame, says an Edmonton professor of international relations. The arrest of Edmonton-based alleged terrorist Sayfildin Tahir- Sharif -- whose extradition hearing was recently delayed -- demonstrates the potential "that there are people self-radicalizing here, and how easily extremist predilections can go unidentified," said University of Alberta political science professor Andy Knight. London Free Press, B5 (Edmonton Sun, Toronto Sun, Whig-Standard, London Free Press)

*** Le Sun Sea, socle étroit du projet de loi C-4**
Après l'arrivée au Canada de l'Ocean Lady et du MV Sun Sea, deux bateaux remplis de demandeurs d'asile tamouls, le gouvernement de Stephen Harper a annoncé une modification en profondeur de la Loi sur l'immigration et la protection des réfugiés : le projet de loi C-4 est l'un des gros morceaux de la rentrée parlementaire. Mais un an et demi après l'accostage du Sun Sea, seuls 14 demandeurs ont été expulsés vers leur pays d'origine, le Sri Lanka. Et aucune accusation n'a encore été portée contre les passeurs. Dans la communauté tamoule, on s'interroge : le Sun Sea n'est-il pas un socle bien étroit pour la loi C-4 ? Seuls six d'entre eux sont encore détenus par l'Agence des services frontaliers du Canada (ASFC), et 14 ont été expulsés pour des raisons de sécurité. La Presse a communiqué avec les cabinets des ministres de l'Immigration et de la **Sécurité publique** afin de commenter ces chiffres. Ils nous ont renvoyés aux fonctionnaires de l'ASFC, où notre demande est restée lettre morte. La Voix de l'Est, 16 (La Presse)

CYBER SECURITY / CYBERSÉCURITÉ

*** Neo-Nazi IDs listed**
Calgarians whose names have been connected to neo-Nazi and white-supremacist groups are angry that their personal IDs have been published on the Internet. The computer hacking collective "Anonymous" released the addresses and phone numbers of thousands of people who had registered with websites affiliated with white-supremacist causes. The sites included Blood and Honour and Local 1488. Calgarian Ryan Lorentz said he doesn't know how his name appeared on one of the lists: "I have no idea what that website is." Calgary Herald, A16

*** Hackers Wiretap FBI Conference Call**
The international hackers group known as Anonymous turned the tables on the Federal Bureau of Investigation by listening in on a conference call last month between the bureau, Scotland Yard and other foreign police agencies about their joint investigation of the group and its allies. Anonymous posted a 16-minute recording of the conference call on the Web Friday and crowed via Twitter: "The FBI might be curious how we're able to continuously read their internal comms for some time now." An FBI official said Anonymous had not hacked into the conference call or any other bureau facilities. Instead, it had obtained an email giving the time, telephone number and access code for the call. "It's not really that sophisticated," said the official. National Post, A11

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

*** Canadian fraud hits foreign markets**
Canadian investors suffer more from market fraud that occurs on other nations' stock exchanges than in Canadian ones. These were the findings of Project Stockholder, a June 2011 internal report by the RCMP criminal intelligence branch that

was obtained by the Financial Post under the Access to Information Act, although some sections were withheld for security reasons. It is the first and only intelligence overview of capital market fraud in Canada since the RCMP Integrated Market Enforcement Team, or IMET, was created in 2003. National Post, FP1

*** Dramatic ice rescue in Bouctouche**
A man in his fifties was rescued by RCMP members in a helicopter yesterday morning after wandering out a couple icy kilometres on the Bouctouche Bay, nearing open waters of the Northumberland Strait. Times & Transcript, A2

*** UN TIERS PUNIS POUR DES AFFAIRES DE DROGUE**
Le tiers des 123 entrepreneurs de construction du Québec inscrits sur la fameuse liste noire de la Régie du bâtiment n'y figurent pas pour des questions de collusion ou d'évasion fiscale, mais plutôt pour des condamnations pour possession ou trafic de drogue, révèle une analyse effectuée par l'Agence QMI. Cette donnée était passée inaperçue avant que l'Agence QMI ne passe cette liste noire au peigne fin. Ce n'est rien pour rassurer ceux qui s'inquiètent des liens troublants entre le crime organisé et le monde de la construction. Journal Montreal, 5

*** La fille d'un caïd gravitait dans le giron familial**
Le travail de policier semblait tellement ancré dans sa famille qu'on l'aurait cru au-dessus de tout soupçon. Mais de nouveaux détails qui filtrent sur la "taupe du SPVM" montrent qu'à la fin de sa vie, Ian Davidson a caché à ses collègues au moins une fréquentation "dérangeante". Et que sa fameuse expertise technologique pouvait aussi se retourner contre la police lorsqu'il l'utilisait pour son propre compte. La Presse, A5

*** Wanted man sought in stabbing**
A man already wanted on a charge stemming from a Fort Qu'Appelle homicide is now being sought for a stabbing in the Maple Creek area. The focus of both probes is Preston Clarence Buffalocalf, a 25-year-old from the Okanese First Nation. RCMP issued a news release late Friday saying Buffalocalf was being sought in connection with a stabbing on the Nekaneet First Nation, near Maple Creek. A 24-year-old man was taken to hospital on Thursday with unspecified injuries. Police did not find out about the incident until the next day. Regina Leader-Post, A1 (Saskatoon Star-Phoenix)

*** Should extradition be different for natives? - Drug smuggling case raises issue for courts**
Lawyers for Zachary Leonard, 24, a member of the Rainy River First Nations in northwestern Ontario, are urging the Ontario Court of Appeal to block his extradition to Minnesota on charges of drug smuggling, arguing it would discriminate on the basis of race and violate his constitutional rights as an aboriginal person. Those include, they say, an enhanced right to remain in Canada. They want Justice Minister Rob Nicholson to prosecute Leonard at home, an option under the Canada-U.S. extradition treaty. But so far, Nicholson has refused. Toronto Star, A6

*** Pipeline opponents take to streets**
First Nations and residents of a community on British Columbia's North Coast are protesting a proposed pipeline which would carry crude oil from Alberta to the west coast for tanker shipment to places like China. The "No Oil Tankers" rally kicked off Saturday morning in a Prince Rupert, B.C. park and wound its way to a civic centre where First Nations leaders were scheduled to speak and musicians like Bif Naked were expected to perform. Marven Robinson, who is a member of the Gitga'at Nation, says his band organized the event. Charlottetown Guardian, A5; Vancouver Sun

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

*** Chasing Truth**
Cameron Ward once had faith in B.C.'s Missing Women Commission of Inquiry, called to examine how police investigated the disappearance of dozens of sex trade workers from Vancouver's notorious Downtown Eastside. From 1997 to 2002, the period under review, prostitutes were murdered by pig farmer Robert "Willie" Pickton, all along a prime police suspect. Mr. Ward is a lawyer who represents the families of 23 missing and murdered women at the inquiry. Five months into public hearings, his faith in the process has crumbled. National Post, A8

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Harm reduction vs. don't touch the stuff
Thirteen of those total deaths, which all occurred late last year and last month, have been linked to paramethoxymethamphetamine (PMMA) a chemical turning up inside Canadian Ecstasy. The broader public health community has backed the harm reduction approach, Dr. Kendall said, but it has run up against some political ambivalence, including from a federal government pushing a tough on-crime mandate. Prime Minister Stephen Harper

kept harm reduction out of his $63.8-million national anti-drug strategy. When it was unveiled in 2007, he said harm-reduction efforts such as Vancouver's Insite needle exchange clinic were a "second-best strategy at best." National Post, A6

*** We need a fact-based policy**
An opinion piece states, "We need a government that prioritizes helping the poor and middle-class, that promotes strong social programs while also emphasizing economic prosperity and job creation. We need a government that bases its decisions not on pre-set notions driven by ideological assumptions, but bases its decisions on facts, evidence and research. Unfortunately, this does not seem to be the modern conservative approach to government... The fact that the Harper government is targeting Old Age Security - which is not under financial pressure and which is important to keeping many seniors out of poverty - is especially appalling as this government has been increasing spending in areas we do not need - building unneeded prisons as part of the Conservative "tough on crime" approach and spending on fighter jets we also do not need." Telegraph-Journal, A5

*** Ashley Smith was destroyed by prison system: mother**
As most know, Ashley Smith was a troubled Moncton teen whose term of probation for throwing apples at a mail carrier eventually led to an accumulation of more than 100 charges and four years in custody, mostly for incidents that occurred while she was behind bars, mostly in isolation. She died while on suicide watch as guards looked on. While Coralee Smith has spoken to reporters on a few occasions in the past, the speaking engagement in the MacNaughton High School auditorium stands out for the size of the audience who got to hear some of Ashley's family's story. Coralee and Herbie recently donated $20,000 to assist programs to help women who have been incarcerated, a gift acknowledged by Kim Pate, the executive director of the Canadian Association of Elizabeth Fry Societies who shared the stage with Coralee. As for the Women &Wellness event, it raised $41,720 for a number of local mental health initiatives. Times & Transcript, A1

*** Projet de loi C-10 - Harper s'est informé des peines minimales**
Des reportages rapportant que des producteurs de marijuana feraient face à des peines minimales plus sévères que les agresseurs d'enfants en vertu du nouveau projet de loi conservateur sur le crime ont suffi à capter l'attention du premier ministre Stephen Harper. La note d'information adressée au premier ministre, qui a été largement censurée, se termine en indiquant que «des analyses supplémentaires» seront nécessaires si les peines minimales sont approuvées dans le projet de loi du gouvernement -- qui se retrouve maintenant devant le Sénat. Le ministre fédéral de la Justice, Rob Nicholson, a par ailleurs mentionné que certains défauts du projet de loi seront corrigés. Le Devoir, A3 (Le Droit, L'Acadie Nouvelle, La Voix de l'Est, La Tribune), The Record (The Telegram, The Chronicle-Herald)

*** Moncton to host new parolee program**
A new program is in place to help people who are released from prison and it's a joint effort between the Findmyway Community Network in collaboration with the Moncton district parole office. Project organizers are seeking volunteer mentors to offer support to people released from prison in an attempt to break the cycle of crime and connect them to the community. Findmyway project facilitator Bert Johnson says a "Preparing for Release" pilot project was undertaken in the latter part of 2009 and the beginning of 2010. It was offered at Dorchester Penitentiary and 15 offenders who were nearing their release date participated in the program. They were teamed up with mentors and the results were overwhelmingly positive. At follow-up meetings on the subject, which included many CSC employees, it was agreed that the program was a success and should be expanded. Times & Transcript, A1

*** Parole rules punish victim**
An opinion piece states, "Family members mourning the loss of a Red Deer couple killed by a drunk driver on Feb. 7, 2010, are being shortchanged by Canada's parole process - as are other victims of crime. And if they feel the offenders' rights supersede their rights under the system, they are bang on the mark. Canada's ombudsman for crime victims agrees and says this obvious imbalance must be corrected now. There's a general consensus among crime victims in Canada that offenders' rights surpass those of the victims. The ombudsman said in her report that information to crime victims under the current parole system is strictly limited and it is time to strike a better balance. O'Sullivan said many victims are frustrated by rules that limit their participation at parole hearings." Red Deer Advocate, A4

*** Cacher son infection au VIH est-il un crime?**
La Cour suprême entendra deux causes, mercredi, pour déterminer si le fait de ne pas dévoiler à ses partenaires sexuels qu'on est atteint du VIH est un crime, et ce, même si les risques de transmission sont faibles. Le plus haut tribunal du pays doit statuer sur les appels déposés par le Manitoba et le Québec sur cette question. Les procureurs soutiennent que les gens atteints du VIH doivent informer leurs partenaires sans tenir compte des risques de transmission. Les partenaires peuvent alors décider s'ils veulent aller de l'avant en connaissant ces risques. Selon ceux qui défendent les droits des personnes atteintes, cette position les criminalise et ne prend pas en compte les données scientifiques. Tous les observateurs espèrent que la Cour suprême va clarifier sa décision de 1998 qui a été interprétée de façons

différentes par les juges dans tout le pays. Le Soleil, 12 (La Voix de l'Est, L'Acadie Nouvelle, Le Nouvelliste, Le Droit, Le Devoir), The Telegram (Red Deer Advocate)

*** Mais arrêtons de dorloter les criminels**
Un article d'opinion déclare, « Plusieurs ont joué le rôle de "vierge offensée" à la suite des propos du sénateur Boisvenu. Ce dernier a dit tout haut ce que plusieurs pensent tout bas. Quand un criminel se fait prendre et qu'il est condamné à la prison, on déroule le tapis rouge pour lui. Des psy analysent et ré-analysent le mental de cet individu en plus de lui fournir un logement convenable ainsi qu'une nourriture de qualité. On lui fera également faire des activités pour l'occuper. Lorsqu'il aura purgé le tiers de sa peine, il sera encore évalué et un comité décidera à la suite des recommandations médicales si ce criminel représentera un risque pour la société. Si ce dernier a bien joué le jeu, il sera remis en liberté. L'individu qui a assassiné la fille de monsieur Boisvenu était justement un récidiviste qui n'aurait jamais dû être remis en liberté. Ce criminel a bénéficié de tous ses droits alors que la victime, monsieur Boisvenu et sa famille ont été ignorés par le système. C'est précisément ce qui irrite le sénateur. Le système judiciaire accorde des droits privilégiés aux criminels et pratiquement rien aux victimes d'actes répugnants... » Le Nouvelliste, 15

*** Positive partnership**
Community policing means a lot more these days than walking the beat. In keeping with a community focus, the Fredericton Police Force has two Neighbourhood Action Teams, with offices on both the north side and the south side of the city. The Daily Gleaner, A10

*** Boisvenu speaks for many Canadians**
An editorial states, "While it may not have been tactful for Tory Sen. Pierre-Hughes Boisvenu to suggest a rope be placed in the prison cells of the most heinous killers so they could have the option of suicide, we do know most Canadians would agree with him. Most Canadians are fed up with victims being ignored while murderers get coddled, and their rights to privacy are honoured to the point of dishonouring the victims... For almost 30 years, until cancer took out this cancer, Canadian taxpayers had to pay out millions for serial killer Clifford Olson's room and board in protective custody... There are now politically-motivated attempts by the opposition to have Sen. Boisvenu removed from the justice committee now studying Bill C-10, the government crime bill that will raise minimum sentences for serious criminal offences. Why? Because he dared to say what the majority of Canadians think?... In 2002, his daughter was raped and murdered by a serial killer and, despite that horror in his life, he is not a proponent of the death penalty. He is well known, however, for being a victims' rights advocate. He therefore belongs on that committee, and has tragically earned the right to be there." Calgary Sun, 14 (Ottawa Sun, Edmonton Sun)

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Do we cut pensions to buy F-35s?**
An opinion piece states, "The Harper government does not admit to any imperfections - and why should it? It has a majority and in its ranks it boasts "the best finance minister on the planet," as the prime minister called Jim Flaherty at Davos a couple of weeks ago... Common sense is bypassed on other fronts. Spending billions to build more prisons at a time when the serious crime rate is falling is one issue that cries out for rethinking. So is the scrapping of the firearms registry over the objection of police forces, who claim the registry helps to save lives. What if the police are right and Conservative strategists are wrong?..." The Record, A7

*** 100,000 reasons to mute latest Conservative attack on CBC**
An opinion piece states "Heritage Minister James Moore releases the earthshaking discovery that of the people who toil at the CBC, 730 earn $100,000 a year or more! Can you believe it? Eighty-seven per cent of CBC employees do not - let me repeat, DO NOT - fall into the top five per cent of income earners in Canada. Polls suggest most of us think the likes of Rex Murphy, Rick Mercer, Hockey Night in Canada and The National are pretty good value. **On the other hand, Conservatives budgeted $1 billion to host a vanity project - the G8 and G20 summits** - involving countries whose recent economic performance suggests, to quote W.A.C. Bennett, they 'couldn't run a peanut stand.' About $50 million of that was siphoned off to fund "legacy" projects like gazebos in the riding of Tony Clement, the minister who now heads up the Treasury Board and who declines to report how many staff in the Prime Minister's Office earn more than $100,000 a year and who they are. 'Nuf said." Vancouver Sun, A1

INTERNATIONAL / INTERNATIONAL

'Tired of Putin'

Russian dissident Boris Nemtsov doesn't expect to see a touch of the Arab Spring in Moscow's winter, but he aims to bring tens of thousands of protesters into the streets Saturday to demand political reform and an end to Vladimir Putin's presidential ambitions. National Post, A15

*** Israeli attack on Iran feared**
For the first time in nearly two decades of escalating tensions over Iran's nuclear program, world leaders are genuinely concerned an Israeli military attack on the Islamic Republic could be imminent -- an action many fear might trigger a wider war, terrorism and global economic havoc. High-level foreign dignitaries, including the UN chief and the head of the American military, have stopped in Israel in recent weeks, urging leaders to give the diplomatic process more time to work. Israel seems unmoved, and U.S. Defence Secretary Leon Panetta has reportedly concluded that an Israeli attack on Iran is likely in the coming months. Winnipeg Free Press, A9 (The Record, Red Deer Advocate, Hamilton Spectator)

*** Al-Qaeda behind wave of terror in Nigeria**
Al-Qaeda operatives in North Africa have helped to transform Boko Haram into a terrorist group capable of killing hundreds in sophisticated attacks. Ottawa Citizen, A7

*** Taliban can depend on NATO to boost their morale**
An opinion piece states "Last week, on the eve of a major NATO summit meeting in Brussels, a rather bleak report was leaked regarding the future fate of Afghanistan. After conducting extensive interviews with more than 4,000 Taliban prisoners, the survey concluded the insurgents' morale remains high and these religious fighters remain convinced that once NATO withdraws its combat forces from Afghanistan in 2014, the Taliban will reclaim the country. Heading into last weekend's NATO summit, U.S. Secretary of Defence Leon Panetta announced that, in view of the financial crisis in Europe, plans need to be made to downsize future Afghan security forces. In other words, we are going to continue recruiting, arming and half-training a demoralized cadre of some 400,000 Afghans for two more years, then cut their funding, lay them off and withdraw our NATO combat forces at the same time. No wonder the morale of those Taliban prisoners is so high." Halifax Chronicle-Herald, B2

OTHER / AUTRE

PM fears Iran's plans
Prime Minister Stephen Harper insisted he is not preparing the Canadian public for war with Iran but, in his starkest warning yet, said he fears the regime in Tehran is prepared to use nuclear weapons, if it manages to produce them. National Post, A1

Turf wars shouldn't block a national securities regulator
Abandoning the idea of a national securities regulator would be the easy way out. To his credit, Finance Minister Jim Flaherty has made it clear he isn't ready to let the issue die, even after the Supreme Court slapped down the federal government in December for constitutional "overreach." The court, he pointed out, recognized that Ottawa still has a legitimate role in setting national standards, collecting data and mitigating risks that threaten financial markets. The current patchwork of 13 provincial and territorial securities regulators also makes the industry particularly vulnerable to fraud and organized crime, according to a report commissioned recently by the **Public Safety** department and obtained by The Canadian Press under the Access to Information Act. "Complicated multi-jurisdictional regulatory systems" make the industry vulnerable, the report found. Globe and Mail, B1

'Honour killings' are sins
A group of Canada's leading Muslim clerics has issued a fatwa against so-called "honour killings," just a week after three members of an Afghan Canadian family were convicted of a quadruple murder that triggered a national debate about cultural values. Vancouver Sun, B2 (London Free Press); * The Record (The Guardian); * La Presse

*** Brutality allegations probed**
Montreal police are investigating allegations of brutality among their ranks after a video of an officer hitting a protester surfaced on the Internet. It comes on the heels of a decision to suspend two Montreal cops for the repeated Tasering in 2007 of a man who died four days after his arrest. Windsor Star, B1 (Edmonton Journal, Daily Gleaner, Times & Transcript)

*** PM likely to ask China about jailed local man**
The plight of a Burlington man in a Chinese jail for what supporters say are trumped-up terrorism charges is expected to be raised by Prime Minister Stephen Harper during his visit to China. Hamilton Spectator, A1

*** Let's discuss mandatory voting**

An opinion piece states, "Let's be honest: Canadians are becoming political dropouts. There's a declining sense of civic duty or democratic responsibility. Growing numbers of Canadians simply can't be bothered to make it to the polling station anymore... In every jurisdiction that has introduced mandatory voting, voter turnout has increased by at least 10 to 15 per cent. This increase has also been most conspicuous among younger voters, who are now compelled to vote. No one is suggesting, of course, that people have to vote a certain way or can't spoil their ballot by not marking an X anywhere. But they do have to show up at the polls if they want to express their displeasure with politicians or the political system as a whole. Many critics will be quick to say that there is something inherently problematic with a voting system that forces citizens to vote in a "free" and "democratic" society. And what about the depressing prospect of uninformed voters actually determining electoral outcomes? Others will say that it won't fly here, that it is repugnant, and that people are entitled to choices in this country... Fine. But then what is the solution to stemming the precipitous drop in voter turnout that we are staring at in the coming years? Do we really want to see only 40 or 50 per cent of Canadians voting on election day?..." The Guard, A7

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-08-12 8:19 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 8, 2012 / le 8 février 2012

Print Media / Médias imprimés

The unforgiving Internet
With over 400 cases of Internet-related child exploitation reported in Alberta last year, police agencies in the province are sending a reminder about practising safe surfing. Alberta Law Enforcement Response Teams' (ALERT) Internet Child Exploitation (ICE) units are among thousands of agencies around the world taking part in Safer Internet Day, doling out advice for parents, schools, and teens on ways to stay safe online. Edmonton Sun, 17

Car Hackers
Omar Ramos-Lopez was none too pleased when fired from his job at an Austin, Tex., car dealership in 2010. So he decided to get even. Getting revenge on former employers may not be a particularly novel reaction, but his choice of payback was cutting-edge. Texas Auto Center, where Ramos-Lopez worked, installs GPS units in leased cars that can remotely prevent the car from starting, or sound the horn on demand. Such functions come in handy if anyone happens to fall behind on their lease payments. National Post, A17

This bill is no SOPA
While hysterical predictions about copyright reform in Canada have been ratcheted up yet again, this time the claims are so outrageous that they can perhaps best be described as having "jumped the shark." Canadians are being told that Bill

C-11, an act to amend Canada's outdated copyright law, could be used to shut down popular websites such as YouTube, fundamentally change the Internet, sabotage online freedoms and hog-tie innovators. National Post, FP13

Online Media / Médias en ligne

MitB attacks not new, but increasing in scale and sophistication, says ActivIdentity
The BBC ecently highlighted so-called man-in-the-browser (MitB) attacks that enable cyber criminals to get around the latest generation of calculator-style two-factor online banking security devices, but this form of attack is really nothing new. Criminal hackers have been wreaking havoc with the ZeuS Trojan for around ten years, attacking everything from bank accounts to government networks, according to security firm ActivIdentity. Computer Weekly

Increasing Malware and Lax Security Biggest Fears for Users: Sophos
67 per cent of people worldwide feel that malware is now on the rise compared to what it was in 2010, according to security vendor, Sophos. The recent report, titled Security Threat Report 2012, made the discovery after people were asked to identify what they consider to be today's biggest threats on the Internet. CSO Online

UK Cyber Security Skills Are 'wholly Inadequate', Says Former Security Minister
The UK needs to significantly bolster its cyber security skills to fight against cyber threats, according to former security minister Baroness Pauline Neville-Jones. Neville-Jones, who is now the government's Special Representative to Business on Cyber Security, said that a lack of skills will hinder the UK's future ability to tackle the challenges of cyber crime. CSO Online

The Private Sector Responds to Cyber Threats
The House Energy Subcmte. on Communications and Technology begins an "aggressive review" of cybersecurity policies as outlined by Chairman Greg Walden (R-OR). According to a press release from the Subcmte., the hearing will focus on "the supply chain vulnerabilities, the man-in-the-middle attacks, the botnets, and the millions of hacking attempts that our cyberdefenses deflect." C-SPAN

Cyber Crime Fight To Be Bolstered By Three New Regional Hubs
Three new regional 'hubs' have been created to help fight cyber crime in the Humber, Northwest and East Midlands areas, it was announced on Wednesday. Cyber crime, or e-crime, includes offences ranging from online fraud, hacking and computer intrusion to distributing "malicious code". Huffington Post

Hactivists Are Like Criminals, Kaspersky Lab CEO Says
What's the difference between the global hactivist groups and true blood cyber crime? Not much, says Eugene Kaspersky, CEO of Kaspersky Lab, a major Russian IT security firm. "To me there is no difference between hactivists that ruin the internet environment and radical protesters who go out and start fires and blow up cars," he said during a conference in Cancun on Tuesday. Forbes

Let us join hands to make Internet safe
With the Safer Internet Day being observed on Feb 7, it's time for more countries to join hands and make concerted efforts to enhance Internet safety. Unfortunately, China is still often accused of cyber espionage. Such baseless accusations will only create a lose-lose situation and increase suspicion and misunderstanding among countries and regions, while the real troublemakers will go scot-free. China Daily

Power grid updates left system vulnerable to cyberattacks, auditors say
A rush by the Energy Department to use stimulus money to modernize the country's power grid has left the system vulnerable to cyberattacks, the agency's internal watchdog found. Inspector General Gregory H. Friedman found "shortcomings" in the cybersecurity plans of more than a third of the utility companies that got federal funding for "smart grid" projects — from incomplete strategies to prevent an attack to vague steps for stopping one if it started. Washington Post

Police bolster attack on cyber crime
Police are to bolster their campaign to target cyber criminals with the formation of three new regional e-crime control centres, senior officers will announce on Wednesday. The programme, to be launched at the Association of Chief Police Officers' cyber crime conference in Sheffield, is a response to the growing threat of online attacks, which are thought to cost the UK £27bn a year, according to Cabinet Office estimates. Financial Times

Open Group security gurus dissect the cloud: Higher or lower risk?

For some, any move to the cloud — at least the public cloud — means a higher risk for security. For others, relying more on a public cloud provider means better security. There's more of a concentrated and comprehensive focus on security best practices that are perhaps better implemented and monitored centrally in the major public clouds. ZDNet

ICS-CERT warns critical infrastructure companies about brute force attacks
The US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is warning critical infrastructure companies about brute force attacks against industrial control systems with secure shell (SSH) command-line access. Many organizations are seeing a large number of access attempts by remote attackers using SSH scans of internet-facing control systems, ICS-CERT said in a recent security advisory. Infosecurity Magazine

Safer Internet Day 2012: Schools and (ISC)2 Professionals Work Together to Educate Children
Parents are unaware of behavioural pitfalls that lead to their children's tiredness in lessons, exposure to abusive and predatory behaviour, and poor habits as they grow up. Schools across the United Kingdom today marked Safer Internet Day 2012 to tackle uninhibited online attitudes that leave children increasingly vulnerable to cyber bullying, abusive gamers, identity theft and malicious threats. 19 (ISC)2 Safe and Secure Online volunteers are out in force today, visiting children and parents in schools across the UK, including South Wales, Kent, Cumbria, Worcester and Teesside. Infosecurity Magazine

AntiSec leaks Symantec pcAnywhere source code after $50k extortion not paid
ymantec had said it would pay $50,000 to a group of hackers associated with Anonymous and AntiSec in order to keep its source code from being leaked online. This was part of a sting operation and email exchange between hackers and Symantec — except it was actually law enforcement posing as Symantec employee "Sam Thomas" and using a fake e-mail address. Computerworld

Has Facebook alerted you to WW3 breaking out? The good news is, it's NOT true. The bad news, you probably now have a computer virus
A fake news page saying, 'U.S. attacks Iran and Saudi Arabia, the begin (sic) of World War 3,' is the latest virus scam to circulate on Facebook. The story uses CNN's logos, and appears to offer video footage of a breaking news story, but says users need to upgrade their Flash video software to watch. Daily Mail

Malware's the next nuclear bomb: Kaspersky
Governments have begun to create malware in the form of cyberweapons, but given that there's no defence against them, they should be handled like nuclear bombs, according to Kaspersky Labs CEO Eugene Kaspersky. "Many countries have already announced they have military cyberdivisions," Kaspersky said at the Kaspersky Lab Cyber Conference 2012 in Cancun, Mexico, quickly recalling from memory a number of countries including the US, Japan, China, North and South Korea, and India. ZDNet

Internet Explorer dominates browser security as Google faces accusations
Internet Explorer 9 should be the go-to browser for organizations concerned about protecting machines from malicious downloads, according to a new study from NSS Labs: Microsoft's browser trounced rivals Chrome, Firefox, and Safari in the security company's more recent malware-blocking tests, a significant win considering that traditional malware remains among the most prevalent threats to users. InfoWorld

Kelihos botnet variant being assembled, claim Kaspersky and Microsoft
Microsoft insist the Kelihos botnet is dead despite reports last week suggesting otherwise; but the company acknowledged that a new botnet is being assembled using a variant of the original malware. The reappearance of a Kelihos-like army of hijacked computers shows just how difficult it is to eradicate a botnet, security experts said yesterday. Computerworld

St-Louis, Danielle

From: St-Louis, Danielle
Sent: February-08-12 2:38 PM
To: CCIRC Weekly Summary
Subject: CYBERSECURITY SUMMARY FOR CIOs
Attachments: PS-SP-#556287-v4-CYBER_EVENT_AND_NEWS_SUMMARY_FOR_14-28_JANUARY_2012.DOC; PS-SP-#527919-v6-FEEDBACK_FORM_FOR_WEEKLY_SUMMARY_FOR_EXECS.DOC

Good afternoon,

Please find attached the Cyber Security Summary for CIOs of significant cyber events and incidents reported to and observed by CCIRC, with analysis where required. Please note this product is *not* intended for wide circulation since it is still in the pilot phase. Here are the highlights:

Highlights

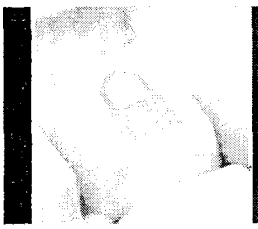
New Events:

- A Canadian federal department with links to ACTA targeted by hackers
- File server log in credentials of a federal department posted on the Internet
- Incidents of Canadian computers hosting malicious software
- [redacted]
- Some Canadian Industrial Control Systems (ICS) reported as being exposed to potential cyber attack".
- Phishing: Fraud attempts in the Financial sector; Cyber criminals impersonating federal organizations
- Website compromises and publicized vulnerabilities in following sectors: Canadian health, non-critical infrastructure sector and a foreign Defence Department

This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Strategic Program Manager, at Kenneth.bendelier@ps-sp.gc.ca.

Thank you,

Danielle St-Louis
Administrative Assistant | Adjointe administrative Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
257 rue Slater St | Ottawa ON K1A 0P9
Telephone | Téléphone: 613-991-7738
Fax | Téléc.: 613-996-0995
E-mail | Courriel: danielle.st-louis@ps-sp.gc.ca



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

CYBER SECURITY SUMMARY FOR CIOs

s.15(1) - Int'l

Reporting Period: JANUARY 14-28, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-002

Purpose

This product is intended to provide Chief Information Officers in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations.

This product also provides contextual background information for the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Overview

Domestically, there were no significant cyber incidents reported over the last two weeks. There were reports of Canadian computers being used for malicious purposes, including attacking a US State Police website. A Canadian federal department linked to the signing of the international Anti-Counterfeiting Agreement (ACTA) was targeted through a malicious e-mail. There was also a message on the Internet by hackers to e-mail or launch a cyber attack against this Department. Internationally, hackers attacked government websites in US, Poland, Ireland and the EU to protest signing of ACTA. There are also continued reports of infected computers in Canada and around the world due to the Ghostclick fraud.

Highlights

New Events:

- A Canadian federal department with links to ACTA targeted by hackers
- File server log in credentials of a federal department posted on the Internet
- Incidents of Canadian computers hosting malicious software
- [redacted]
- Some Canadian Industrial Control Systems (ICS) reported as being exposed to potential cyber attack".
- Phishing: Fraud attempts in the Financial sector; Cyber criminals impersonating federal organizations
- Website compromises and publicized vulnerabilities in following sectors: Canadian health, non-critical infrastructure sector and a foreign Defence Department

CCIRC Products Released during the reporting period:

- Cyber Flash on cyber attacks by Anonymous related to copyrights and intellectual property (CF12-001)

Noteworthy News in the Media:

- Israeli and Palestinian hackers exchange website attacks
- Hackers around the world protest current and intended anti-piracy measures:
    - MegaUpload's shutdown prompts hacker attacks on US government and music industry websites
    - Proposed US copyright law SOPA being protested: Certain websites elect to go dark for one day in protest; Anonymous attacks US government websites such as DOJ & FBI
    - Signing of the international Anti-Counterfeiting Agreement (ACTA) prompting hacker attacks on US, Poland, Ireland and European government websites.

NEW EVENTS REPORTED IN GOVERNMENT AND OTHER CANADIAN CRITICAL INFRASTRUCTURE SECTORS

Federal Government Sector

Operation SACTA (Stop Anti-Counterfeiting Trade Agreement): An online message signed by Anonymous posted a link to a Canadian federal department website, encouraging users to join the anti-ACTA movement, and attack if necessary. This message was posted on a popular text-file sharing website often used by hackers and is presumably encouraging cyber attacks on websites.

CCIRC provided available technical details to CTEC, the federal Government's CERT, for their further investigation.

> ***Comment:*** *There are provisions in the international Anti-Counterfeiting Trade Agreement that have important implications for content sharing on the Internet. This is a multi-lateral trade agreement which Canada has signed. Canada's new proposed copy-right law, Bill C-11 (former Bill C-32), is currently in Parliament at the second reading stage. There is a great deal of opposition to this agreement around the world by the on-line community and websites of other government have recently been attacked by hackers in protest.*

File Server (FTP) Login Credentials of a Federal Department posted on the Internet. CCIRC learned that the FTP login credentials of a federal department were posted on the Internet. CCIRC advised CTEC and provided known technical details.

> ***Comment:*** *FTP login credentials are used to gain access to a file sharing server where users may upload or download files. If a threat actor used these credentials, the result could be information compromise or the use of the server as a launch point for cyber attacks.*

Non-Federal Government Sector

Canadian computers being used in cyber attacks. CCIRC has learned that a cyber attack on a US State Police website was traced to a Canadian university's computer. In addition, another Canadian university's website was found to host malicious software that could infect website visitors. There were also reports of malicious software being hosted at a website hosting service provider's server and at two other unidentified Canadian entities.

CCIRC contacted the known Canadian organizations, with mitigation advice. The RCMP was informed of items of interest. CCIRC warned the website hosting service provider that the website in question was added to various block lists, possibly resulting in reduced legitimate traffic to this website. The malicious software from the university's website has been removed and is no longer being served.

> ***Comment:*** *It is possible that cyber criminals compromised these Canadian computers to use them remotely for malicious purposes, without their owners' knowledge. Organizations that offer computers for public use, such as universities, can be particularly susceptible to such compromises.*

Some Canadian Industrial Control Systems exposed to potential cyber attacks. A trusted international partner alerted CCIRC that information that could allow remote access to certain Canadian houses and apartment buildings' heating and air conditioning systems, was posted on the Internet. CCIRC alerted those responsible for the buildings and houses, offering mitigation advice. There is no report of any cyber attack in these cases at this time.

> ***Comment:*** *Many Industrial Control Systems (ICS), such as the ones used for heating and cooling buildings, are monitored or even maintained remotely through the use of certain software. It is likely that the technicians responsible for the set-up and maintenance of the heating systems for these buildings did not take cyber security into consideration or did not know the standard practices for protecting against such exposure.*
>
> *Since the Stuxnet virus attack on an Iranian nuclear facility, there has been a heightened awareness, both domestically and internationally, of cyber security for ICS. The trusted international partner who alerted CCIRC is focussed primarily on securing ICS. CCIRC recently moderated discussion at a ICS conference in Montreal.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonating Canadian financial institutions, tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in United States and Taiwan.

Cyber criminals also attempted to solicit personal information by impersonating Service Canada and Canada Revenue Agency.

CCIRC notified the impersonated financial institutions of these fraud attempts and the Government CTEC for the federal government cases. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website compromises and publicized vulnerabilities. CCIRC discovered a small health organization's website was defaced and offered mitigation advice. CCIRC also discovered a foreign Defence Department's website was compromised and contacted the organization, as well as CCIRC's equivalent organization. There was also a list of vulnerable websites posted on the Internet, which includes a Canadian university.

There were additional website compromises in the health and non-critical infrastructure sectors. Website usernames and passwords were posted on the Internet by hackers.

> ***Comment:*** *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

Ghostclick Fraud. There were new and continued reports of infected computers in three provincial governments, three provincial health organizations, an airport authority, an energy organization, two banks, 19 Canadian universities, a national media organization and 13 telecommunications companies.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012. There are currently websites around the world for computer users to check whether their machine is infected by the malicious software used in this fraud. These sites can be found by searching with the keywords "dns-ok".

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in. CCIRC is also working with the Canadian Internet Registration Authority (CIRA) to provide notifications to affected users.

Operation Ghostclick was worldwide fraud campaign, exposed in late 2011 by the FBI. Cyber criminals hijacked users' Internet web searches and diverted them to websites that generated advertising and sales revenues. Computers across multiple sectors, in organizations large and small, and those belonging to the general public have been affected.

> ***Comment:*** *Organizations should ensure they have taken the mitigation measures outlined in CCIRC's Information Note. CCIRC noted that the type and size of affected organizations varied, and were spread across Canada. The number of affected telecommunications companies more than likely indicates number of infected client computers of Internet via Service Providers. These Internet Service Providers receive information from CCIRC.*
>
> *Organizations that offer Internet access, including those that provide publically accessible wireless networks, may be particularly vulnerable. In addition to the cooperative effort underway between CCIRC and CIRA, the Canadian government has launched a website for cyber security public education..*

CCIRC PRODUCTS RELEASED:

Hacktivist attacks related to proposed anti-piracy legislation. There have been coordinated distributed denial-of-service (DDoS) attacks on websites by hacktivists, claiming to be associated with Anonymous. There were multiple international targets, which included governments (Canada, US, Poland, Ireland and EU) and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA).

In response, CCIRC issued Cyber Flash CF12-001, titled *"Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property"*. This Cyber Flash, was sent to technical and security contacts within stakeholder organizations in government and other critical infrastructure

sectors . Government and industry organizations involved with the Copyright legislation and copyrighted material were encouraged to assess their risk exposure to coordinated DDoS attacks on their networks.

NOTEWORTHY NEWS IN THE MEDIA:

Israeli and pro-Palestinian hackers exchange website attacks. Open sources reported that the websites of Israel's main stock exchange, several banks and the national airline were attacked. Pro-Palestinian hackers claimed responsibility and even claimed to have posted the login credentials for several industrial control systems in Israel on the Internet. Shortly thereafter, there were reports of suspected Israeli hackers bringing down the Saudi Stock Exchange, interfering with the Abu Dhabi Security Exchange, and publishing e-mail addresses & passwords of 30,000 Arab Facebook users.

> ***Comment:*** *It is now becoming commonplace to carry real-world grievances into the cyber world. There could be an adverse impact from these attacks for Canadians and Canadian businesses that do business with the stock exchanges or banks involved. There were some media reports that some of the Israeli banks could block international access to their sites.*

Hackers around the world attack government websites to protest anti-piracy measures.

- **Retaliation for file-sharing service Mega Upload's shutdown:** Hackers, claiming to be with Anonymous, attacked the websites of the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music.

- **Signing of the international Anti-Counterfeiting Agreement (ACTA) and proposed US copyright laws:** Wikipedia shut down for one day to protest the proposed SOPA and PIPA bills. SOPA and PIPA were also cited by Anonymous as a reason for their attacks on the DOJ and FBI websites. Operation STOP ACTA by Anonymous also prompted hacker attacks on websites for US, Poland, Ireland governments as well as for the European Parliament.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

OUR ORGANIZATION

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest.

CCIRC operates in conjunction with the Government Operations Centre within Public Safety Canada, and is a key component of the government's all-hazards approach to emergency management and national security.

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Dvorkin, Corey

From: Katie.Tolan@international.gc.ca
Sent: February-09-12 12:21 PM
To: Danaitis, Algis; Gordon, Robert; Bokwa, Lisa; Bolton, Stephen; Komm, Chantelle; Larose, Charlene; Currie, Chris; Dvorkin, Corey; Oldham, Craig; Durand, Stéphanie; Galadza, Larisa; Matrisciano, Giovanni; 'Glen.Linder@ps-sp.gc.ca'; Grabs, Robert; Veysey, Gregory; Randall, Jacqueline; Schwartz, Jo-Ann; Spallin, Julie; Moreau, Ken; Khouri, Lisa; Kubicek, Brett; Clairmont, Lynda; MacKinnon, Paul; Senft, Matthew; McAllister, Andrew; MacDonald, Michael; Namercia.DosSantos@ps-sp.gc.ca; Nap, Carole; Filion, Nathalie; Pagotto, Paul; Davies, Patricia; DesRochers, Patrick; Julianne Prokopich; Dincoy, Rana; Banerjee, Ritu; Lesser, Robert; Astravas, Rutha; Beaudoin, Serge C; Taschereau, Marc; Theilmann, Mike; Tolan, Katie; Jarmyn, Tom; Veilleux, Martine; Mahu, Vlad; Wong, Hazel; Wong, Suki; Leguerrier, Yves; Zuccolo, Claudia; Motzney, Barbara; Travers, Evan; 'Fergal.O'Reilly@ps-sp.gc.ca'; Green, Amanda; De Santis, Heather; Hirsch, Darryl; Davies, John; Kingsley, Michèle; Mohammed, Melanie; Thalakada, Nigel; Plunkett, Shawn; Bhupsingh, Trevor; Vershinin, Sergey
Cc: Julianne Prokopich
Subject: WASHINGTON UPDATE JAN 31-FEB 8, 2012
Attachments: 020912 CQ - Collins to File Backscatter Radiation Study Bill.docx; 020912 CQ - Cyber Bill Progress - Reid Is Fundamental.docx; 020912 CQ - Intel Agencies Working on Common IT Platform Internal Threat Detection.docx; 020912 CQ - Study Evaluates International Cybersecurity Preparedness.docx; 020912 CQ -Feasibility of Radiation-Scanning Mandate for Cargo Questioned.docx; 020912 CQ-Republican Pressure Builds on Holder.docx; 020912 Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps.docx

SUMMARY OF KEY ITEMS OF INTEREST:

PEOPLE: (1) **ICE Director John Morton** FEB 7 announced the appointment of **Andrew Lorenzen-Strait** as the **public advocate**. Lorenzen-Strait will be responsible for helping the public understand the prosecutorial discretion policy and other changes as well as addressing complaints about the changes (See ICE Section) (2) The Department of Justice announced FEB 3 **Luke McCormark** will become the DOJ's new chief information officer, starting in late March. (See DOJ Section)

STATEMENT FOR THE RECORD ON THE WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY: Director of National Intelligence (DNI) James R. Clapper delivered an unclassified **Statement for the Record on the Worldwide Threat Assessment** of the US Intelligence Community for the **Senate Select Committee on Intelligence** JAN 31. This statement provides extensive detail about numerous state and nonstate actors, crosscutting political, economic, and military developments and transnational trends, all of which constitute the nation's strategic and tactical landscape. The 30 page statement asserts that although **counterterrorism, counterproliferation, cybersecurity, and counterintelligence are at the immediate forefront of our security concerns**, the DNI notes that it is virtually impossible to rank—in terms of long-term importance—the numerous, potential threats to US national security. The United States no longer faces—as in the Cold War—one dominant threat. Rather, it is the multiplicity and interconnectedness of potential threats—and the actors behind them—that constitute the biggest challenge. Indeed, even the four categories noted above are also inextricably linked, reflecting a quickly changing international environment of rising new powers, rapid diffusion of power to nonstate actors and ever greater access by individuals and small groups to lethal technologies. DNI Clapper spoke of the duty of professionals in the Intelligence Community (IC) to work together as an integrated team to understand and

master this complexity. By providing better strategic and tactical intelligence, members of the IC can partner more effectively with other Government officials at home and abroad to protect vital national interests. In delivering the shorter, more succinct prepared remarks to the Committees, the DNI began by highlighting the global issues of Terrorism and Proliferation followed by a discussion of cyber threats. Excerpts follow.

The assessment within the Intelligence Community, according the DNI Clapper, sees the next two or three years as a **critical transition phase for the terrorist threat**, particularly for al-Qa'ida and like-minded groups. With Usama bin Ladin's death, the global jihadist movement lost its most iconic and inspirational leader. The new al-Qa'ida commander is less charismatic, and the death or capture of prominent al-Qa'ida figures has shrunk the group's top leadership layer. However, even with its degraded capabilities and its focus on smaller, simpler plots, al-Qa'ida remains a threat. As long as pressure is sustained on it, DNI noted the judgement that core al-Qa'ida will be of largely symbolic importance to the global jihadist movement. But regional affiliates, as the ones mentioned , and to a lesser extent, small cells and individuals, will drive the global jihad agenda.

Proliferation – that is, efforts to develop, acquire, or spread weapons of mass destruction – is also a **major global strategic threat.** Among nation-states, Iran's technical advances, particularly in uranium enrichment, strengthen the U.S. assessment that Iran is well capable of producing enough highly enriched uranium for a weapon, if its political leaders, specifically the Supreme Leader himself, choose to do so. North Korea's export of ballistic missiles and associated materials to several countries, including Iran and Syria, illustrate the reach of the North's proliferation activities. DNI Clapper noted that there is no expectation Kim Jong Un, North Korea's new young leader, to change Pyongyang's policy of attempting to export most of its weapons systems.

Of interest, this year's **Statement for the Record, elevated the discussion of Cyber Threats to follow Terrorism and Proliferation.** The cyber threat is one of the most challenging ones faced. The DNI spoke of foreseeing a cyber environment in which emerging technologies are developed and implemented before security responses can be put in place. Among state actors, the U.S. IC is particularly concerned about entities within China and Russia conducting intrusions into U.S. computer networks and stealing U.S. data. And the growing role that non-state actors are playing in cyberspace is a great example of the easy access to potentially disruptive and even lethal technology and know-how by such groups. **Two of the greatest strategic cyber challenges are: First, definitive, real-time attribution of cyber attacks – that is, knowing who carried out such attacks and where these perpetrators are located. And second, managing the enormous vulnerabilities within the I.T. supply chain for U.S. networks**. (See ODNI Section for related links)

THIS WEEK IN WSHDC:

FEB 7 –Less than two months after American troops left, the State Department is preparing to slash by as much as half the enormous diplomatic presence it had planned for Iraq, a sharp sign of declining American influence in the country. Article

FEB 7 – Symantec confirmed that the pcAnywhere source code published on the Web Monday by hackers who tried to extort $50,000 from the company was legitimate. A company spokesman also said that Symantec expects that the rest of the source code stolen from its network in 2006 will also be made public. Article

FEB 7 – The director of the CIA, David H. Petraeus, may visit Myanmar later this year, officials said, in what would be the latest signal of warming relations with the United States as Myanmar emerges from years of military rule and diplomatic isolation. Article

FEB 6 – The Obama administration has closed the U.S. Embassy in Damascus and pulled all American diplomats out of Syria. Article

FEB 4 – Saboteurs stole passwords and sensitive information on tipsters while hacking into the websites of several law enforcement agencies worldwide in attacks attributed to the collective known as Anonymous. Breaches were reported this week in Boston, Syracuse, New York, Salt Lake City and Greece. Anonymous also published a recording on the Internet FEB 3 of a phone call between the FBI and Scotland Yard, gloating in a Twitter message that "the FBI might be curious how we're able to continuously read their internal communications for some time now." Article

FEB 2 –The Obama administration has more than doubled, to about 21,000 names, its secret list of suspected terrorists banned from flying to or within the United States, including about 500 Americans, The Associated Press has learned. The government lowered the bar for the list, even as it says it is closer than ever to defeating al-Qaida. Article

FEB 1 – China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer by an Australian mining giant zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal. Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, eventually hitting seven different law firms as well as Canada's Finance Ministry and the Treasury Board, according to Daniel Tobok, president of Toronto-based Digital Wyzdom. His cyber security company was hired by the law firms to assist in the probe. Article

JAN 31 –Some senior Iranian leaders are now more willing to carry out attacks inside the United States in response to perceived American threats against their country, Director of National Intelligence James R. Clapper Kr., said in prepared testimony to the Senate Intelligence Committee, pointing to last fall's suspected assassination plot against the Saudi ambassador to Washington. Article

WHITE HOUSE:

FEB 6 – President Obama issued additional sanction on the Government of Iran and Iranian financial institutions. Executive Order | President Obama's Statement on Syria

FEB 3 – President Barack Obama continued his commitment to improving employment among veterans by introducing an initiative to hire them as the country's first responders. Press Release

JAN 30 –In a rare official discussion of the covert drone program run by the CIA, President Barack Obama defended the United States' use of drones to strike suspected terrorists in Pakistan and elsewhere during a live web interview. Obama maintained that the drone program has not been responsible for a "huge" number of civilian casualties, and is "kept on a very tight leash" so as to be extremely targeted toward "active terrorists." Article

DHS:

FEB 7 – Joint testimony of David Heyman, Assistant Secretary for the Office of Policy, Rear Admiral Zukunft, Assistant Commandant for U.S. Coast Guard Office of Marine Safety, Security and Stewardship, and Kevin McAleenan, Acting Assistant Commissioner for U.S. Customs and Border Protection Office of Field Operations before the House Committee on Homeland Security, Subcommittee on Border and Maritime Security addressing supply chain security.

FEB 3 – Rand Beers, National Protection and Programs Directorate Under Secretary, before the House Committee on Energy and Commerce, Subcommittee on Environment and the Economy regarding the Department of Homeland Security's efforts to regulate the security of high-risk chemical facilities under the Chemical Facility Anti-terrorism Standards. Testimony

FEB 3 - Testimony of Alan Cohn, Policy's Deputy Assistant Secretary for the Office of Strategic Plans, before the House Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management regarding how DHS is implementing a strategy to counter emerging threats. Testimony

FEB 1 –Secretary Janet Napolitano traveled to Indianapolis to highlight the Department's "If You See Something, Say Something™" public awareness campaign's continued partnership with the National Football League (NFL) to help ensure the safety and security of employees, players and fans during the regular season, and Super Bowl XLVI. Press Release

JAN 31 – As part of these ongoing efforts and in recognition of the one-year anniversary of the White House Startup America Initiative, the DHS announced a series of administrative reforms which will be completed in the future. These reforms reflect the Administration's continuing commitment to attracting and retaining highly-skilled immigrants. Fact Sheet

JAN 30 –DHS Secretary Janet Napolitano delivered the second annual State of Homeland Security Address at the National Press Club in Washington, DC. Napolitano's address highlighted DHS's accomplishments over the past year, and its goals and priorities going forward. Transcript of Address | Video – includes Q&A | The Hill

CBP:

FEB 6 – CBP announced the release of the updated Bonded Warehouse Manual for Customs and Border Protection Officers and bonded Warehouse Proprietors. Bonded Warehouses provide storage facilities for imported cargo that is pending importation into or exportation from the United States. The Bonded Warehouse Manual was last updated in 1990. Press Release

FEB 6 –DHS Secretary Janet Napolitano issued a final rule in the Federal Register which will permanently establish the Global Entry Trusted Traveller Program. FedReg Notice

JAN 31 – The work of CBP featured prominently in Homeland Security Secretary Janet Napolitano's address to Washington, D.C., journalists as she described how "our homeland security and our economic security go hand in hand." Press Release

JAN 31 - CBP and the Kootenai Tribe of Idaho announced the publication of a notice in the Federal Register designating the Kootenai Enhanced Tribal Card (ETC) as a travel document acceptable for entering into the United States through a land or sea port of entry. Press Release

ICE:

FEB 7 –ICE Director John Morton announced the department's first Public Advocate, ICE Senior Advisor Andrew Lorenzen-Strait. Lorenzen-Strait will serve as a point of contact for individuals, including those in immigration proceedings, non-governmental organizations and other community and advocacy groups, who have concerns, questions, recommendations or other issues they would like to raise. Blog Post Article

FEB 2 – Special agents and officers seize more than $4.8 million in fake NFL merchandise and seize 307 websites during 'Operation Fake Sweep' in Indianapolis. Press Release

FEB 2 – Five Los Angeles-area residents have been indicted for operating a human smuggling scheme that relied largely on non-Spanish speaking African-Americans to transport loads of illegal aliens from the U.S.-Mexico border to the Los Angeles area. Press Release

TSA:

FEB 8 –DHS Secretary Janet Napolitano and TSA Administrator John S. Pistole announced the expansion of TSA Pre√™, a passenger pre-screening initiative, to additional airports across the country following the program's success at seven pilot locations, including Baltimore/Washington International and Dulles. Press Release

FEB 7 –Testimony of John Pistole, Administrator of the Transportation Security Administration before the House Committee on Homeland Security, Subcommittee on Transportation Security addressing the TSA Screening Partnership Program.

ODNI:

JAN 31 – Unclassified statement and remarks delivered on the Worldwide Threat Assessment of the Un Intelligence Community for the Senate Select Committee on Intelligence. [See attached for transcript] Threats from cyber-espionage, computer crime, and attacks on critical infrastructure will surpass terrorism as the number one threat facing the United States, FBI Director Robert Mueller testified. Mueller along with ODNI Clapper spelled out for senators on the dire national security implications of threats to U.S. computer networks. But efforts to move a comprehensive cybersecurity bill through the chamber are still meeting resistance. ABC News

JAN 26 - In a tight budget environment, communication and collaboration have become more important to intelligence work than ever, and agencies are working on solutions such as an integrated, cross-agency information technology platform, Director of National Intelligence James Clapper said. (See attached for CQ Article)

DOJ:

FEB 4 – Attorney General Holder delivered remarks at the American Bar Association's National Summit on Indigent Defense in New Orleans.

FEB 3 – Attorney General Holder delivered remarks on "the sacred covenant" between citizens and their government at Tulane University's Law School. Remarks

FEB 3 – Luke McCormark will become the DOJ's new chief information officer, starting in late March. Press Release

FEB 2 – Attorney General Holder testified before the House Committee on Oversight and Government Reform on standards of integrity and professional at the DOJ.

AFGHANISTAN/PAKISTAN WAR:

FEB 7 –The CIA is expected to maintain a large clandestine presence in Iraq and Afghanistan long after the departure of conventional U.S. troops as part of a plan by the Obama administration to rely on a combination of

spies and Special Operations forces to protect U.S. interests in the two longtime war zones, U.S. officials said. Article

FEB 2 –Defense Secretary Leon Panetta said FEB 1 that the United States could end its combat mission in Afghanistan as early as mid-2013, more than a year before the deadline President Barack Obama laid out for withdrawing all U.S. troops from the country. His comments were the first time a U.S. official had put a date on when the United States would relinquish its central role in the conflict. Panetta said that the U.S. troops would play an "advise and assist" role to Afghan forces after mid-2013. Article

GAO

FEB 7 –Supply Chain Security
Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning
GAO-12-422T

FEB 3 –Department of Homeland Security
Additional Actions Needed to Strengthen Strategic Planning and Management Functions
GAO-12-382T

JAN 25 - Over the past decade, the DHS has spent more than $70 million assessing the effects of chemical, biological and radiological weapons. Yet that work has only guided only a portion of the department's emergency response plans, according to the GAO. Report

CONGRESS:

FEB 8 – The Subcommittee on Communications and Technology held a hearing on "Cybersecurity: Threats to Communications Networks and Private-Sector Responses."

Opening Statements: Chairman Walden

Witness List:

Larry Clinton, President and CEO, Internet Security Alliance

Bill Connor, President and CEO, Entrust

Robert Dix, Vice President of Government Affairs & Critical Infrastructure Protection, Juniper

James Lewis, Director and Senior Fellow, Technology and Public Policy Program, CSIS

Phyllis Schneck, Vice President and CTO, Global Public Sector, McAfee Inc.

FEB 7 –With five months until the DHS hits its deadline for scanning all U.S.-bound cargo for radiation, lawmakers are again floating the idea of ditching the mandate because of high costs, technological challenges and logistical issues, which remains far from being fulfilled. Based on the roughly $120 million the government has spent on six cargo-scanning pilot programs, DHS estimates the cost of full compliance to be around $16.8 billion, said Kevin McAleenan, acting assistant commissioner of CBP's Office of Field Operations. [See attached for CQ article]

FEB 6 –The House Homeland Security Subcommittee on Cyber-Security, Infrastructure Protection and Security Technologies marked up the cyber-security bill sponsored by Rep. Dan Lungren (R-Calif.) and unanimously approved it FEB 1. Lungren's Promoting and Enhancing Cyber-Security and Information Sharing Effectiveness Act (PRECISE). Article

FEB 3 –A growing chorus of House Republicans is supporting a legislative effort to express dissatisfaction with the job performance of Attorney General Eric H. Holder Jr. In late January, six lawmakers added their names to the list of cosponsors of a no-confidence resolution (H.R. 490) against Holder. It currently totals 90 GOP members. The lead sponsor, Rep. Paul Gosar, R-Ariz., has criticized the attorney general, saying Holder hasn't cooperated with congressional inquiries about the botched Bureau of Alcohol, Tobacco, Firearms and Explosives operation known as "Fast and Furious." [See attached for CQ article]

FEB 2 –The nation's spymaster said that his "highest legislative priority" is to extend surveillance powers Congress gave the intelligence community in a 2008 law. Committees in both the House and the Senate have already begun talks to grant his wish. [See attached for CQ article]

FEB 1 –Senator Susan Collins, ranking Republican on the Homeland Security and Governmental Affairs Committee, and a bipartisan group of her colleagues - Daniel Akaka (D-Hawaii), Carl Levin (D-Mich.), Tom Coburn (R-Okla.), and Scott Brown (R-Mass.) – introduced legislation to require an independent study of backscatter x-ray scanners and to require signs to alert travelers they have screening alternatives other than the backscatter machines. Article

JAN 30 - It's unusual for a Senate majority leader to become personally invested in a major legislative effort on a complex and technical topic with no obvious political payoff, particularly in an election year. But as the Senate tries to assemble a major bill to overhaul the nation's cyberdefenses, Nevada Democrat Harry Reid has emerged as the focal point. (See attached for CQ Article)

UPCOMING HEARINGS:

FEB 15 @ 2:30pm – The House Committee on Homeland Security will hold a hearing on, "An Examination of the President's FY2012 Budget Request for the Department of Homeland Security." 311 Cannon Bldg

FEB 16 @ 10:00am – The House Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence will hold a hearing on "DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy" 311 Cannon Bldg

THINK TANKS:

FEB 7 – A study entitled *Muslim-American Terrorism in the Decade Since 9/11* study by Charles Kurzman from the Triangle Center on terrorism and Homeland Security at the University of North Carolina, Chapel Hill was released FEB 7.

FEB 2 – James Carafano and Jessica Zuckerman from The Heritage Foundation released commentary on the contradictory legislation governing cargo transit and port security, saying Congress should move toward fostering a more risk-based approach.

JAN 31 – Paul Rosenzweig from The Heritage Foundation published a WebMemo on the promoting cybersecurity through the PRECISE Act.

JAN 30 – Ben Rhodes, White House Deputy National Security Advisory for Strategic Communications discusses new national security challenges facing the Obama Administration at the Center for American Progress. Video

JAN 2012 - Heather Conley of the Center for Strategic and International Studies argues that U.S. Arctic policy must be given a sense of urgency and focus. This report analyzes the drivers of change in the region, examines the key Arctic security actors and institutions and explores the potential for a new security architecture for the Arctic. Read

JAN 2012 - Edward Alden and Bernard Schwartz of the Council on Foreign Relations report that the United States is getting ever closer to creating a system in which it will be more or less impossible to lie one's way into this country through the legal ports of entry. Read

JAN 30 –Two of the most feared aggressors in the cybersecurity world, Russia and China, lag behind the United States and other nations when it comes to digital defenses, according to a new study commissioned by the network security firm McAfee. [See attached for CQ article]

FEB 1 –Nearly a third of all terrorist attacks from 1970 to 2008 occurred in just five metropolitan U.S. counties, but terrorist events continue to occur in rural areas as well; there are 3,143 counties in the United States; researchers found 65 of these counties to be hot-spots for terrorism, that is, each of these counties experienced a greater than the average number of terrorist attacks between 1970 and 2008. Findings were found in a report published by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland.

JAN 31 –Companies including utilities, banks and phone carriers would have to spend almost nine times more on cybersecurity to prevent a digital Pearl Harbor from plunging millions into darkness, paralyzing the financial system or cutting communications, a Bloomberg Government study found. To achieve security capable of stopping 95 percent of attacks – considered by the Traverse City, Michigan-based Ponemon Institute to be the highest attainable level – those surveyed said they would have to boost spending to a group total of $46.6 billion from the current $5.3 billion. [See attached for article and related documents available on request]

UPCOMING EVENTS:

FEB 13 from 9:00-1:00pm– CSIS will host an event on, "Maritime Security: Confronting New and Non-Traditional Challenges in the Age of Austerity." Location: 1800 K St. NW B1 Conference Room

FEB 13 from 12:00-1:30pm – The Hudson Institute will host an event on, "Recent Developments in Cyberwarfare." Gen. James Cartwright (USMC, ret.) who served as Commander of the U.S. Strategic Command will deliver the keynote address. Location: 1015 15th St., NW 6th floor

FEB 22 from 10:00-12:00pm- the HSPI will host "A Conversation on Cyber Security Legislation with Michael Chertoff and Michael McConnell. Location: 1957 E St., NW 7th Floor RSVP

FEB 22 from 10:30-12:00pm – The Bipartisan Policy Institute will host FCC Chairman Julius Genachowski who will address new cyber security policies. Location: 1225 Eye St., NW Suite 1000

ARTICLES/ REPORTS OF INTEREST:

FEB 6 –A Look at the Secretive World of Air Marshals. CBS News. Article/Video

FEB 6 – U.K. Grants Bail to Radical Muslim Cleric. The Wall Street Journal. Article

FEB 4 – Border Patrol OT Up As Arrests Drop. Associated Press. Article

JAN 25 – The National Northern Border Counternarcotics Strategy: Closing a Window of Criminal Opportunity. HSPI: Security Debrief. Article

JAN 23 - The Next Homeland Security Secretary. Defense Media Network. Article

Kathleen Tolan
Counsellor
Public Safety and Border Security
Public Safety Canada
501 Pennsylvania Avenue, N.W.
Washington, D.C. 20001-2114
Tel: (202) 448-6338 Cell: 202 497-5898
Fax: (202) 682-7792
Email: katie.tolan@international.gc.ca

s.16(2)(c)
s.15(1) - Subv

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-09-12 8:42 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted]; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 9, 2012 / le 9 février 2012

Print Media / Médias imprimés

NASA hacker faces charges
A Romanian man known as "Ice Man" has been indicted for hacking into computers at the National Aeronautics and Space Administration's Jet Propulsion Laboratory in Southern California, U.S. federal prosecutors said Wednesday. Windsor Star, A11

Online Media / Médias en ligne

SDA, McAfee mark Canada's card
The Canadian government could try harder in matters of cyber security, according to a report ranking countries on their security stance. Canada received a mediocre ranking in the report, which was co-produced by McAfee and the Security Defence Agenda (SDA), a Brussels-based security think tank. SC Magazine

UK cyber strategy implementation 'too slow', says former security minister

The UK government needs to set out a clear timetable for the implementation of its cyber security strategy, former security minister Baroness Pauline-Neville Jones has said. Neville-Jones, who is now the government's Special Representative to Business on Cyber Security, said that since the government is only starting to implement the policies of the strategy, significant progress will not be seen another 18 months. Computerworld UK

'The internet should be a demilitarised zone'
In a world where governments are spending tens of billions of pounds arming themselves for a cyberwar, Eugene Kaspersky's message is an unfashionable one. As chief executive of one of the largest computer security firms, he flies around the world telling politicians and officials they should instead be working to make the internet a military-free zone. The Telegraph (UK)

Cyber criminals eye Olympics as opportunity to con people
Researchers at internet and software security firm Websense have unearthed a number of Olympic ticket scam sites. The researchers found that most of them had multiple backlinks, suggesting they have been widely spammed over the internet in addition to being promoted via Google AdWords. The Times of India

Can Hackers Destroy The Internet?
Botnets, trojans, SQL injections and DDoS attacks. Most internet users have no idea what those things are, or how they are shaping the future of their connected lives. One thing is certain, more computers and wireless devices are going to be compromised this year than were last year. Some companies will go out of business as a result. State secrets will be revealed. A mysterious charge will appear on your credit card bill each month. Forbes

Cyber bill to put US in charge of global cyber security
In the wake of the SOPA outcry, another controversial bill that puts the US in charge of global cyber dealings is simmering. While industry and public uproar has stalled the controversial online anti-piracy bills known as SOPA and PIPA, American legislators are maintaining an aggressive stance on cybercrime, preparing to vote on a new bill that, if passed, will force other countries to play by US rules. Sydney Morning Herald

Police e-crime hubs announced
Three regional policing e-crime hubs are to be established in the UK, as the Government looks to boost the nation's protection against threats. IT PRO

Hackers break into gov't cyber security head's site
Arab hackers yesterday penetrated the website of the Tel Aviv University Security Studies Program, run by Prof. Isaac Ben-Israel, the head of the National Cyber Defense Authority. The website has resumed regular operations. Globes

Telecom firm KPN targeted by hackers
Telecoms firm KPN was targeted by hackers last month, who managed to break into the company's computer systems and access confidential private and corporate client details, Nos radio reports. DutchNews.nl

Syrian government loves the password 12345
The Syrian government could use some training on web security. Anonymous has released hundreds of e-mails the group claims it obtained by hacking a mail server used by Syrian President Bashar al Assad's office. But a look at the list of e-mail addresses and passwords released shows a hack wasn't necessary—all that was needed to gain access to Syria's sensitive information was one of the world's most common passwords: 12345. Of the 78 passwords Anonymous leaked, 31 used 12345. Others used easy to guess passwords like iloveyou, testing, system and 123456. Both iloveyou and 12345 made SplashData's list of the worst passwords of 2011. Canada.com

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

s.15(1) - Def

Moore, Bruce

From: Beaudoin, Luc S.
Sent: Friday, February 10, 2012 10:51 AM
To: Cameron, David M.; Turbide, Francois A; Moore, Bruce; Bendelier, Kenneth M.; Williston, Sandra
Subject: FW: Anonymous report

Classification: UNCLASSIFIED

very good spill on anonymous....

-----Original Message-----
From: [redacted] [mailto: [redacted]@cse-cst.gc.ca]
Sent: Thursday, February 09, 2012 12:26 PM
To: Beaudoin, Luc S.
Subject: Anonymous report

Classification: UNCLASSIFIED

Hi Luc,
Please find attached a copy of the Anonymous report. The report focuses on the tradecraft used, the targets and also the potential of GC being targeted.

<<Anonymous-CTA-GC-1111-01.DOC>>

Thank you for the information you had provided. It was very useful.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

Beaudoin, Luc S.

From: [redacted]@cse-cst.gc.ca]
Sent: Thursday, February 09, 2012 12:26 PM
To: Beaudoin, Luc S.
Subject: Anonymous report

s.15(1) - Def
s.16(2)(c)

Anonymous-CTA-GC-1111-01.DOC (...

Classification: UNCLASSIFIED

Hi Luc,
Please find attached a copy of the Anonymous report. The report focuses on the tradecraft used, the targets and also the potential of GC being targeted.

<<Anonymous-CTA-GC-1111-01.DOC>>

Thank you for the information you had provided. It was very useful.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

Beaudoin, Luc S.

From: [redacted]@cse-cst.gc.ca]
Sent: Thursday, November 10, 2011 11:13 AM
To: Beaudoin, Luc S.
Cc: [redacted]
Subject: RE: ANONYMOUS report

Classification: CONFIDENTIAL

Hi Luc,
I will talk to RCMP o[redacted]t, I am hoping to touch base with them next week. Would Thursday, Nov 17, at 11-12 work out for you? [redacted] would like to come by as well for this.

Thanks,
[redacted]

From: Beaudoin, Luc S. [mailto:l[redacted]
Sent: November 9, 2011 11:56 AM
To: [redacted] Singh, Gurbinder (RCMP); Alves de Jesus, Tiago (RCMP)
Subject: RE: ANONYMOUS report

Classification: CONFIDENTIAL

much more information on non-government targets.

Could you come over here next week ?

you should monitor the next Copyright-law debates related to digital content (Bill C-32 I believe)...UK and Aus equivalent of our intellectual property office (under IC I think) got attacked as soon as their equivalent laws came into effects.

L

-----Original Message-----
From: @cse-cst.gc.ca]
Sent: Tuesday, November 08, 2011 3:38 PM
To: Beaudoin, Luc S.; Singh, Gurbinder; Alves de Jesus, Tiago
Subject: RE: ANONYMOUS report

s.13(1)(a)
s.15(1) - Def
s.16(2)(c)

Classification: CONFIDENTIAL

Tiago, thank you for your response, please do pass along anything you find.
thank you, for your response as well,

Luc, I was hoping to get a draft ready by the end of this month, this is an internal timeline and it is somewhat flexible.
If you do have some incidents that you suspect are Anonymous, I can work with you on trying to attribute them.

From: Beaudoin, Luc S. [mailto
Sent: November 8, 2011 3:06 PM
To: ; Singh, Gurbinder (RCMP); Alves de Jesus, Tiago (RCMP)
Subject: RE: ANONYMOUS report

Classification: CONFIDENTIAL

CCIRC is interested in participating. We have had a number of incidents beleived to be associated with Anonymous. The danger is that we do not focus on attribution, so it may be difficult to validate the true actor behind some of these highly publicised events.

When do you need this by ?

-----Original Message-----
From: @cse-cst.gc.ca]
Sent: Monday, November 07, 2011 4:43 PM
To: Singh, Gurbinder; Alves de Jesus, Tiago; Beaudoin, Luc S.
Subject: ANONYMOUS report

Classification: CONFIDENTIAL

Hello,
I am the supervisor for in CTEC. Your contact information has been

passed onto me by [redacted] My team will shortly start drafting a report focusing on the ANONYMOUS group. The basis of this report would be to understand the group and to assess the threat it poses to Canadian government.

A very rough format of the report is listed below:

s.15(1) - Def
s.16(2)(c)

- Who are they
- Their targets
- Their tradecraft/behaviour (why do they target and when)
- Canada related activities
-Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

Beaudoin, Luc S.

From: [redacted]
Sent: Wednesday, November 09, 2011 10:07 AM
To: [redacted] Beaudoin, Luc S.; Singh, Gurbinder; Alves de Jesus, Tiago
Subject: RE: ANONYMOUS report

[redacted]

That is [redacted] is the my last name but that's OK

>>> "[redacted]cse-cst.gc.ca> 11/8/2011 3:37 pm >>>
Classification: CONFIDENTIAL

Tiago, thank you for your response, please do pass along anything you find. [redacted] thank you, for your response as well,

Luc, I was hoping to get a draft ready by the end of this month, this is an internal timeline and it is somewhat flexible. [redacted] If you do have some incidents that you suspect are Anonymous, I can work with you on trying to attribute them.

From: Beaudoin, Luc S. [mailto:[redacted]
Sent: November 8, 2011 3:06 PM
To: [redacted]; Singh, Gurbinder (RCMP); Alves de Jesus,

- Their tradecraft/behaviour (why do they target and when)
- Canada related activities
-Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

s.15(1) - Def
s.16(2)(c)

Beaudoin, Luc S.

From: Alves de Jesus, Tiago [tjesus@rcmp-grc.gc.ca]
Sent: Tuesday, November 08, 2011 9:59 AM
To: [redacted] Singh, Gurbinder; Beaudoin, Luc S.
Subject: RE: ANONYMOUS report

Classification: CONFIDENTIAL

Good day,

The RCMP's NSCI program does not have any criminal intelligence, at this point in time, on ANONYMOUS. However, if any of our law enforcement partners, both domestic and International, pass on any information it would be my pleasure, if possible, to share it with you.

Have a great day,

Sincerely yours,

Tiago

Tiago Alves de Jesus,PhD
i/c Cyber Unit
National Security Criminal Operations
National Security Criminal Investigations
Royal Canadian Mounted Police

From: [redacted] cse-cst.gc.ca]
Sent: Monday, November 07, 2011 4:43 PM
To: [redacted] Singh, Gurbinder; Alves de Jesus, Tiago; Beaudoin, Luc S (GOC)
Subject: ANONYMOUS report

Classification: CONFIDENTIAL

Hello,

I am the supervisor for [redacted] in CTEC. Your contact information has been passed onto me by Chris Dugal. My team will shortly start drafting a report focusing on the ANONYMOUS group. The basis of this report would be to understand the group and to assess the threat it poses to Canadian government.

A very rough format of the report is listed below:

- Who are they
- Their targets
- Their tradecraft/behaviour (why do they target and when)
- Canada related activities
-Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

s.15(1) - Def

s.16(1)(c)

Beaudoin, Luc S.

From: [redacted]
Sent: Tuesday, November 08, 2011 [redacted]
To: [redacted] Beaudoin, Luc S.; Singh, Gurbinder; Alves de Jesus, Tiago
Cc: [redacted]
Subject: Re: ANONYMOUS report

[redacted]

Good morning [redacted]

[redacted]

>>> "[redacted]cse-cst.gc.ca> 11/7/2011 4:43 pm >>>
Classification: CONFIDENTIAL

Hello,
I am the supervisor for [redacted] in CTEC. Your contact information has been passed onto me by [redacted]. My team will shortly start drafting a report focusing on the ANONYMOUS group. The basis of this report would be to understand the group and to assess the threat it poses to Canadian government.

A very rough format of the report is listed below:

> - Who are they
> - Their targets

> - Their tradecraft/behaviour (why do they target and when)
> - Canada related activities
-Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

s.15(1) - Def
s.16(2)(c)

[redacted]

Beaudoin, Luc S.

From: [redacted]@cse-cst.gc.ca]
Sent: Monday, November 07, 2011 4:43 PM
To: [redacted] Singh, Gurbinder; Alves de Jesus, Tiago; Beaudoin, Luc S.
Subject: ANONYMOUS report

Classification: CONFIDENTIAL

Hello,
I am the supervisor for [redacted] in CTEC. Your contact information has been passed onto me by [redacted] My team will shortly start drafting a report focusing on the ANONYMOUS group. The basis of this report would be to understand the group and to assess the threat it poses to Canadian government.

A very rough format of the report is listed below:

- Who are they
- Their targets
- Their tradecraft/behaviour (why do they target and when)
- Canada related activities
-Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

Williston, Sandra

From: Mulder, Rene
Sent: February-10-12 11:06 AM
To: Bergeron, Dominic; Mack, Laurie; Bakri, Kareem
Subject: Re: Anonymous???

And... What about the anon chatter?

----- Original Message -----
From: Bergeron, Dominic
Sent: Friday, February 10, 2012 10:57 AM
To: Mulder, Rene; Mack, Laurie; Bakri, Kareem
Subject: RE: Anonymous???

Don't bother, daily reports are going to elio

-----Original Message-----
From: Mulder, Rene
Sent: February-10-12 10:57 AM
To: Mack, Laurie; Bergeron, Dominic; Bakri, Kareem
Subject: Anonymous???

I hear something's going on?
I'm gonna send Krul a report on XP systems. He just called me.

Mulder

s.16(2)(c)

Williston, Sandra

From: Bendelier, Kenneth
Sent: February-10-12 9:05 AM
To: Beaudoin, Luc
Subject: German Parliament

Of course, it's unconfirmed...

http://dagobertobellucci.wordpress.com/2012/02/08/germany-anonymous-hacks-into-german-parliament-website/

http://www.cyberwarzone.com/cyberwarfare/anonymous-hacks-german-parliament-website

http://www.mediafire.com/?lqmokhpicdqk69p

http://pastebin.com/[redacted]

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-993-5042
Facsimile | Télécopieur +1 613-954-3097
Kenneth.Bendelier@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

Williston, Sandra

From: Beaudoin, Luc
Sent: February-09-12 12:34 PM
To: [redacted]cse-cst.gc.ca' **s.15(1) - Def**
Subject: Re: Anonymous

Tx. I ll look it up...

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: [redacted]@cse-cst.gc.ca]
Sent: Thursday, February 09, 2012 12:28 PM
To: Beaudoin, Luc
Subject: RE: Anonymous

Hi Luc,
Just wanted to let you know that I have sent you a copy of the report on the high-side.

Thanks,
[redacted]

From: Beaudoin, Luc S [mailto:LucS.Beaudoin@ps-sp.gc.ca]
Sent: November 17, 2011 2:19 PM
To: [redacted]@cse-cst.gc.ca'
Cc: [redacted]
Subject: Anonymous

some material to get you started....

consider this material FOUO within CSEC, containing 3rd party information exempted under section 20.1 and 13.1 of ATIA.

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Dvorkin, Corey

From: Dvorkin, Corey
Sent: February-09-12 12:34 PM
To: Matz, Mark; Green, Amanda; Grigsby, Alexandre; Anderson, Ian; Bradley, Kees; Mohammed, Melanie
Cc: Gordon, Robert; Paul.Charlton@international.gc.ca; DONALD.NEILL@forces.gc.ca; SARA.SIXSMITH@forces.gc.ca
Subject: Worldwide Threat Assessment of the US Intelligence Community

http://www.dni.gov/testimonies/20120131_testimony_ata.pdf

Cyber is on pages 7-8

Alex: notice an entirely different approach as compared to a document we were just discussing.

Major Trends

Cyber threats pose a critical national and economic security concern due to the continued advances in—and growing dependency on—the information technology (IT) that underpins nearly all aspects of modern society. Data collection, processing, storage, and transmission capabilities are increasing exponentially; meanwhile, mobile, wireless, and cloud computing bring the full power of the globally-connected Internet to myriad personal devices and critical infrastructure. Owing to market incentives, innovation in functionality is outpacing innovation in security, and neither the public nor private sector has been successful at fully implementing existing best practices.

The impact of this evolution is seen not only in the scope and nature of cyber security incidents, but also in the range of actors and targets. In the last year, we observed increased breadth and sophistication of computer network operations (CNO) by both state and nonstate actors. Our technical advancements in detection and attribution shed light on malicious activity, but cyber intruders continue to explore new means to circumvent defensive measures.

Among state actors, China and Russia are of particular concern. As indicated in the October 2011 biennial economic espionage report from the National Counterintelligence Executive, entities within these countries are responsible for extensive illicit intrusions into US computer networks and theft of US intellectual property.

Nonstate actors are also playing an increasing role in international and domestic politics through the use of social media technologies. We currently face a cyber environment where emerging technologies are developed and implemented faster than governments can keep pace, as illustrated by the failed efforts at censoring social media during the 2011 Arab Spring revolutions in Tunisia, Egypt, and Libya. Hacker groups, such as Anonymous and Lulz Security (LulzSec), have conducted distributed denial of service (DDoS) attacks and website defacements against government and corporate interests they oppose. The well publicized intrusions into NASDAQ and International Monetary Fund (IMF) networks underscore the vulnerability of key sectors of the US and global economy.

Hackers are also circumventing network security by targeting companies that produce security technologies, highlighting the challenges to securing online data in the face of adaptable intruders. The compromise of US and Dutch digital certificate issuers in 2011 represents a threat to one of the most fundamental technologies used to secure online communications and sensitive transactions, such as online banking. Hackers also accessed the corporate network of the computer security firm RSA in March 2011 and exfiltrated data on the algorithms used in its authentication system.

Subsequently, a US defense contractor revealed that hackers used the information obtained from RSA to access its network.

Outlook

We assess that CNO is likely to increase in coming years. Two of our greatest strategic challenges regarding cyber threats are: (1) the difficulty of providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, definitively attributing them, and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber attacks; and (2) the highly complex vulnerabilities associated with the IT supply chain for US networks. In both cases, US Government engagement with private sector owners and operators of critical infrastructures is essential for mitigating these threats.

Corey Michael Dvorkin
Senior Strategist / Conseiller principale
Cyber Policy / Politiques cyber
National Cyber Security Directorate / Direction générale de la cybersécurité nationale
Public Safety Canada / Sécurité Publique Canada
340 Laurier Avenue West / 340, avenue Laurier Ouest
Ottawa, Ontario, K1A OP8
Tel: (613) 990-9608
corey.dvorkin@ps-sp.gc.ca

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-10-12 8:17 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; Csversko, Christine; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted]; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 10, 2012 / le 10 février 2012

Print Media / Médias imprimés

Youths are vulnerable to Internet luring
Youths ranging in age from 12 to 15 continue to remain targets of online luring, according to figures released this week by the Canadian Centre for Child Protection. The Daily Gleaner, A4

Online Media / Médias en ligne

Analysis: In cyber era, militaries scramble for new skills
With growing worries about the threat of "cyber warfare," militaries around the world are racing to recruit the computer specialists they believe may be central to the conflicts of the 21st century. ut whilst money is plentiful for new forces of "cyber warriors," attracting often individualistic technical specialists and hackers into military hierarchies is another matter. Reuters

Inside INTERPOL's New Cybercrime Innovation Center
INTERPOL, the international policing organization, is building a law enforcement tech geek heaven in Singapore. The INTERPOL Global Complex for Innovation will function as a R&D lab, training facility, and forensics lab for all things cybercrime. Michael Moran, INTERPOL's Acting Assistant Director for Cyber Security and Crime, told Fast Company on Wednesday that the main focus for IGCI would be digital security and innovation research for police officers worldwide investigating cybercrime. Fast Company

Syria's Cyberwar
Since media are strictly controlled by the Syrian government, the internet has played a key role in allowing opposition activists share images of alleged atrocities carried out by security forces. You can argue that a high-stakes war of information is being waged in Syrian cyberspace, and in one battle at least the hacking group Anonymous is claiming victory. CNN

Anonymous Launches Cyber-Crusade against Israel 'Reign of Terror'
Anonymous hacker collective has threatened a cyber-crusade against Israel to end what it claims is a reign of terror. In the latest round of cyber-warfare between pro-Palestinians and pro-Israeli hackers, the hacktivists have released a video on YouTube which accuses Israel of committing crimes against humanity. International Business Times

Android malware connects to botnet and makes premium rate calls by rooting itself
The Android operating system has had yet another serious piece of malware sully its name today, as an Android app called com.google.android.smart has been discovered to be a premium rate texts, calls and botnet scam. Tech Digest

Facebook Video Scam: World War III Begins
A new dimension to cyber crime was highlighted with the spreading of fake news of the commencement of World War III in the US for invading Iran and Saudi Arabia. SPAMfighter

Malware authors get social to improve cyber attacks
Security researchers have found that cyber criminals are offering their attack tools in a software-as-a-service (SaaS) model, and creating social networks to build communities around their products to help suggest new features and find bugs. Computing News

Cyber-space now seen as 'fifth dimension of warfare'
The cyber-security challenge is not a national one - it is a global one, as countries around the world recognise the benefits of working together to tackle criminals, who make use of the worldwide web. As the report we recently commissioned found, just under half of experts now think cyber-security is as important as border security; so there is clearly a demand for governments to be more involved in addressing threats which cross borders. Public Service Europe

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Williston, Sandra

From:
Sent: February-10-12 6:42 PM
To:
Subject: RE: CIA Webstite Down

s.16(2)
s.19(1)
s.20(1)(c)

Ack. Tx.

From:
Sent: February-10-12 6:37 PM
To:
Subject: FW: CIA Webstite Down

FYI – Please see below

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: GOC-COG@PS-SP.GC.CA

From:
Sent: February-10-12 6:36 PM
To: GOC-COG; Darren.Sabourin@rcmp-grc.gc.ca; Kathy MacDonald; Scott.Foster@rcmp-grc.gc.ca; Tiago.Dejesus@rcmp-grc.gc.ca; tim.oneil@rcmp-grc.gc.ca
Subject: CIA Webstite Down

See: https://twitter.com/#!/YourAnonNews/status/168068014758039552 and http://rt.com/usa/news/anonymous-hacked-cia-hackers-049/

I attempted to access the site and it appears to be offline

[redacted]

s.20(1)(c)

UNCLASSIFIED

DATE: February 20, 2012

File No.:
RDIMS No.:

MEMORANDUM FOR THE DIRECTOR GENERAL

ANONYMOUS THREAT TO DOMAIN NAME SERVICE ROOT SERVERS
(Information only)

ISSUE

Internet postings claiming to have been authored by the hackivist group Anonymous indicate a potential Distributed Denial of Service (DDoS) attack against the Domain Name Service (DNS) root servers may take place on the 31st of March 2012. Under the auspices of "Operation Global Blackout", the stated objective of this DDoS attack is to "shut the Internet down".

BACKGROUND

DNS resolves human-readable domain names (e.g. google.com) into routable Internet Protocol (IP) addresses (e.g. 123.123.123.123). While DNS provides a number of supporting capabilities to the operation of the Internet, its core function is analogous to that of a telephone book. Just as the phone system cannot route a person or a business name to a particular phone number, the Internet cannot route to a domain name. Thus, when a phone call needs to be made to an "A. Smith" in Ottawa, a phone user looks this name up in a phone book and finds the phone number assigned to A. Smith. The phone system can then complete the call to the device to which the phone number for A. Smith is assigned. DNS provides a similar service to the Internet.

A **DDoS** attack is a form of cyber-attack in which multiple computers, distributed both geographically and across networks, are coordinated in such a way that their combined efforts are used for a specific objective. In general, DDoS attacks either consume all or most of the network bandwidth available to the target, or they exceed the resource capacity of the targeted device(s). The impact to the end user is that service response is very slow or, in some cases, the requested service is unavailable. There have been two previous DDoS attempts against DNS root servers, one in 2002 and the second in 2007. In both cases, the infrastructure withstood the attacks and, in both cases, lessons learned were applied to make the DNS infrastructure more resilient to DDoS attacks.

Anonymous is a loosely-coupled collective associated with collaborative online hacktivism. The group has recently focussed its efforts against regulatory efforts associated with anti-digital piracy legislation, but has also supported environmental and social justice campaigns. Cyber-attacks attributed to Anonymous have successfully exfiltrated data from targeted organizations. However, the primary attack method employed by Anonymous is DDoS. Anonymous cyber-attacks are often coordinated via various social media sites. Anonymous has made available a number of tools to support DDoS attacks such that any computer user who chooses to participate in a can do so with ease and minimal computer knowledge.

CONSIDERATIONS

The stated purpose of the proposed attack against DNS root servers is to "shut the Internet down". Given previous successful DDoS attacks attributed to Anonymous against, for example, Visa, MasterCard, PayPal HBGary, Amazon, and most recently governments around the world, including the Canadian House of Commons, it is clear that both the intent and capability of Anonymous are legitimate. There are, however, a number of mitigating factors that make the success of Operation Global Blackout doubtful.

The infrastructure itself is both high-capacity and redundant. While, logically, there are 13 root servers on the Internet, the implementation sees the load spread across over 250 physical locations. These are provided with high-capacity network connections. In addition, should a DDoS attack take place, telecommunication providers would redirect or block malicious traffic destined for the root servers in order to maintain network availability. Finally, the distributed nature of DNS makes a complete Internet blackout very unlikely. To use the phone system analogy, suppose it were possible for someone to destroy all copies of the telephone book. Many people maintain a copy of their frequently dialed phone numbers locally, such as in a contact list, on a PDA, business cards, etc. DNS works in a similar fashion where "local" DNS servers, through a process known as *caching*, maintain a record of recently requested domain names and their IP addresses. This process is repeated up the hierarchy and, unless a DDoS attack was sustained for an extended period time (days), name resolution would work in the vast majority of cases.

It can be assessed that, unless prevented through the efforts of law enforcement agencies, a DDoS attack, coordinated by Anonymous against the DNS root servers, will likely take place on 31 March, 2012. However, it is unlikely the stated objective of shutting the Internet down will be achieved. The most likely impact is that there may be temporary instances of slower performance on some network segments.

NEXT STEPS

In addition to CCIRC, law enforcement and agencies responsible for the operation of the DNS infrastructure around the world are monitoring the situation and actively developing

mitigation plans. CCIRC will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Ken Bendelier

CYBERDO

From: Beaudoin, Luc
Sent: February-27-12 1:18 PM
To: [redacted]
Subject: [redacted]

s.16(2)(c)

AMBER
PROTECTED

Bloody PKI stript the content..... here is the unencrypted version of my last email. NOT FOR DISTRIBUTION OUTSIDE CCIRC.

[redacted]

Executive Summary

[redacted]

Pages 2096 to / à 2097

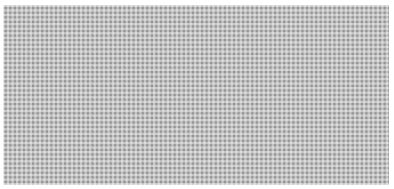
are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information



s.16(2)(c)

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Dvorkin, Corey

From: Katie.Tolan@international.gc.ca
Sent: February-24-12 10:57 AM
To: Danaitis, Algis; Gordon, Robert; Bokwa, Lisa; Bolton, Stephen; Komm, Chantelle; Larose, Charlene; Currie, Chris; Dvorkin, Corey; Oldham, Craig; Durand, Stéphanie; Galadza, Larisa; Matrisciano, Giovanni; 'Glen.Linder@ps-sp.gc.ca'; Grabs, Robert; Veysey, Gregory; Randall, Jacqueline; Schwartz, Jo-Ann; Spallin, Julie; Moreau, Ken; Khouri, Lisa; Kubicek, Brett; Clairmont, Lynda; MacKinnon, Paul; Senft, Matthew; McAllister, Andrew; MacDonald, Michael; Namercia.DosSantos@ps-sp.gc.ca; Nap, Carole; Filion, Nathalie; Pagotto, Paul; Davies, Patricia; DesRochers, Patrick; Julianne Prokopich; Dincoy, Rana; Banerjee, Ritu; Lesser, Robert; Astravas, Rutha; Beaudoin, Serge C; Taschereau, Marc; Theilmann, Mike; Tolan, Katie; Jarmyn, Tom; Veilleux, Martine; Mahu, Vlad; Wong, Hazel; Wong, Suki; Leguerrier, Yves; Zuccolo, Claudia; Motzney, Barbara; Travers, Evan; 'Fergal.O'Reilly@ps-sp.gc.ca'; Green, Amanda; De Santis, Heather; Hirsch, Darryl; Davies, John; Kingsley, Michèle; Mohammed, Melanie; Thalakada, Nigel; Plunkett, Shawn; Bhupsingh, Trevor; Vershinin, Sergey
Cc: Julianne Prokopich
Subject: WASHINGTON UPDATE FEBRUARY 17-FEBRUARY 24, 2012
Attachments: 022412 CQ - Conference on Payroll Tax Cut to Give Spectrum to Emergency Responders.docx

SUMMARY OF KEY ITEMS OF INTEREST

PEOPLE: (1) **U.N. Secretary General Ban Ki-moon** is planning to ask his predecessor, **Kofi Annan**, to serve as his new U.N. envoy to Syria. Article (2) **Frank Montoya, Jr.** has joined the Office of the Director of National Intelligence as the national counterintelligence executive (See ODNI Section). (3) **Carter Morris and Bill Cason** FEB 21 were appointed to be the respective Chairman and Vice-Chairman of the Aviation Security Advisory Committee (ASAC). **John Boles** has been named FEB 17 special agent in charge of the **FBI's Norfolk Division.** [See FBI section for press release]

SECRETARY NAPOLITANO SIGNS LETTER OF INTENT WITH DUTCH MINISTER OF SECURITY: Secretary of Homeland Security Janet Napolitano and **Dutch Minister of Security and Justice Ivo Opstelten** signed (FEB 22) a Letter of Intent to **build upon cooperative cybersecurity initiatives to promote a safe, secure and resilient cyber environment.** The Letter of Intent signed recognizes expanded coordination between the United States and the Netherlands, and outlines several areas to further collaborate on cybersecurity including incident management and response activities, control systems security, and cybersecurity exercises. During the meeting, Secretary Napolitano and Minister Opstelten also discussed the importance of international security partnerships as well as collaborative efforts to **combat terrorism and transnational crime, and ensure a stronger, safer, and more resilient global supply chain.** Secretary Napolitano traveled to the Netherlands last June to meet with her counterparts as part of the Department's ongoing commitment to securing the global supply chain and international transportation systems. (See DHS Section of related link)

THIS WEEK IN WSHDC:

FEB 23 – The first official talks between the United States and North Korea since the coming to power of the youthful leader Kim Jong-un were "serious and substantial," the senior American negotiator said, and would

extend into a second day. Issues ranging from nuclear matters to nutritional assistance were covered in the talks FEB 23. The American negotiator, Glyn T. Davies, indicated little progress had been made so far. Article

FEB 23 –World leaders pledged new help to tackle terrorism and piracy in Somalia, but insisted FEB 23 that the troubled East African nation must quickly form a stable government and threatened penalties against those who hamper its progress. Article

FEB 23 –The Obama administration's top Pentagon lawyer on FEB 22 said that American citizens who join Al Qaeda can be targeted for killing and that courts should have no role in reviewing executive branch decisions about whether someone has met such criteria. "Belligerents who also happen to be U.S. citizens do not enjoy immunity where non-citizen belligerents are valid military objectives," said Jeh C. Johnson, the Defense Department general counsel, in a speech at Yale Law School. Article

FEB 23 –The Pentagon's newest unified command is marshalling troops for a future war that some say already is being fought in the global communication and information networks that make up cyberspace. US Cyber Command is housed within the headquarters of the National Security Agency on the Army's sprawling base at Fort Meade, Md. The command's headquarters has 800 or so personnel, about equal parts civilian and military, plus a number of contractors. Article

FEB 22 –The Obama administration is urging the Supreme Court to halt a legal challenge weighing the constitutionality of a once-secret warrantless surveillance program targeting Americans' communications that Congress eventually legalized in 2008. The FISA Amendments Act allows the government to electronically eavesdrop on Americans' phone calls and e-mails without a probable-cause warrant so long as one of the parties to the communication is outside the United States, and is suspected of a link to terrorism. The administration is asking the Supreme Court to review an appellate decision that said a nearly 4-year-old lawsuit by the ACLU on the matter could move forward. Article

FEB 22 – The Supreme Court issued three decisions, including one ruling that a woman whose gun was seized based on what she said was an unconstitutional search warrant could not sue the police officers who obtained the warrant. Article

FEB 22 –Analysts for a DHS program that monitors social networks like Twitter and Facebook have been instructed to produce reports on policy debates related to the department, a newly disclosed manual shows. The manual, a 2011 reference guide for analysts working with the department's Media Monitoring Capability program, raises questions about recent claims by Homeland Security officials who portrayed the program as limited to gathering information that would help gain operational awareness about attacks, disasters or other emerging problems. Article

Rep. Jackie Speier (D-California), speaking at the hearing of the Subcommittee on Counterterrorism and Intelligence, was "outraged" that the agency has hired a contractor to review a variety of social networking sites, including Facebook and Twitter, and she wants the Department of Homeland Security to cease its social-media and news-monitoring operation.

FEB 23 – A coalition of Internet giants including Google Inc. has agreed to support a do-not-track button to be embedded in most Web browsers—a move that the industry had been resisting for more than a year. Article

FEB 22 – FCC Chairman Julius Genachowski unveiled a plan that calls on Internet service providers to take specific steps to combat online threats - specifically, botnets, domain name fraud, and IP hijacking. The chairman's recommendations came from the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), which was tasked with coming up with ways to address critical private-sector Internet

security vulnerabilities. The group's research landed on three particular areas - botnets, Internet route hijacking, and domain name fraud. Article

FEB 21 – The National Institute of Standards and Technology (NIST) announced a new partnership to establish the National Cybersecurity Center of Excellence, a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The State of Maryland and Montgomery County, MD, are co-sponsoring the center with NIST, which will work to strengthen U.S. economic growth by supporting automated and trustworthy e-government and e-commerce. Article

22 –The UN Security Council is to vote to increase the African Union peacekeeping force in Somalia by more than 5,000 soldiers, diplomats have said. The resolution will increase the number of troops in the country to 17,731 from its current level of 12,000. Article

FEB 21 – The director of the National Security Agency has warned that the hacking group Anonymous could have the ability within the next year or two to bring about a limited power outage through a cyber attack. Gen. Keith Alexander provided his assessment in meetings at the White House and in other private sessions. While he hasn't publicly expressed his concerns about the potential for Anonymous to disrupt power supplies, he has warned publicly about an emerging ability by cyber attackers to disable or even damage computer networks. Article

FEB 18 – The National Security Council is moving to exert greater federal control over scientific studies of highly lethal diseases and toxins in the face of mounting fears that the research could be used by terrorists and rogue states, according to people with knowledge of the process. Article

FEB 17 – The hacking group known as Anonymous has claimed a new series of hacks against the U.S. Federal Trade Commission and consumer rights websites. The loosely organized collection of cyber rebels said it attacked the FTC's consumer protection business center and the National Consumer Protection Week websites. Article

FEB 16 – The Obama administration is slapping sanctions on Iran's ministry of intelligence and security, asserting that it supports global terrorism, commits human rights abuses against Iranians and participates in ongoing repression in Syria. Article

WHITE HOUSE:

FEB 21 –President Obama delivered remarks on Congress' passing of the Payroll Tax Cut which included an initiative that will expand wireless broadband and ensure that first responders have access to the latest lifesaving technologies. [See Congressional section for info on the bill]

DHS:

FEB 22 –The DHS Secretary Janet Napolitano and Dutch Minister of Security and Justice Ivo Opstelten signed a Letter of Intent to build upon cooperative cybersecurity initiatives to promote a safe, secure and resilient cyber environment. The Letter of Intent signed recognizes expanded coordination between the United States and the Netherlands, and outlines several areas to further collaborate on cybersecurity including incident management and response activities, control systems security, and cybersecurity exercises. Press Release

FEB 21 –The DHS Secretary Janet Napolitano traveled to McAllen, Texas and joined CBP Acting Commissioner David Aguilar to see CBP operations at the Southwest border, discuss the Department's efforts

to secure the border while facilitating lawful travel and trade, and meet with state and local law enforcement officials. Press Release

FEB 17 – The DHS Secretary Janet Napolitano announced the release of FY 2012 grant guidance and application kits for seven DHS preparedness grant programs totaling over $1.3 billion to assist states, urban areas, tribal and territorial governments, non-profit agencies, and the private sector in strengthening our nation's ability to prevent, protect, respond to, and recover from terrorist attacks, major disasters and other emergencies in support of the National Preparedness Goal. In FY 2012, DHS preparedness grants were reduced by nearly $1 billion from the FY 2011 enacted level and $1.5 billion below the President's FY 2012 request. Press Release

Bennie Thompson (D-MS), Ranking Member of the Senate Homeland Security and Governmental Affairs, protested the shortsighted and rash cuts. Press Release

FEB 17 –Written testimony of Chief Information Officer Richard Spires for a House Committee on Oversight and Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and Procurement Reform hearing entitled "How Much is Too Much? Examining Duplicative IT Investments at DOD and DOE."

FEB 17 – Mark Weatherford, Deputy Under Secretary for Cybersecurity discusses the recently-introduced Cybersecurity Act of 2012 and the ways it will help keep the American public safe from theft, fraud and loss of personal and financial data, while simultaneously addressing one of DHS' core cybersecurity missions – securing the federal executive branch networks. Blog

FEB 16 – The DHS Secretary Janet Napolitano testified before the Senate Committee on Homeland Security and Governmental Affairs on, "Securing America's Future: The Cybersecurity Act of 2012" [See Congressional section for more information]

FEB 16 –Joint testimony of Chief Privacy Officer Mary Ellen Callahan, and Operations Coordination and Planning Director Richard Chávez for a House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence hearing on DHS monitoring of social networking and media.

FEB 16 – Testimony of Robert Bray, TSA Assistant Administrator for the Office of Law Enforcement and the Federal Air Marshal Service before the House Committee on Homeland Security, Subcommittee on Transportation Security for a hearing addressing the Federal Air Marshal Service.

FEB 15 –Testimony of USCIS Director Alejandro Mayorkas before the House Committee on the Judiciary, Subcommittee on Immigration Policy and Enforcement for a hearing entitled "Safeguarding the Integrity of the Immigration Benefits Adjudication Process."

ICE:

FEB 21 –ICE's Homeland Security Investigations-led National Intellectual Property Rights Coordination Center and the World Customs Organization recently concluded Operation Global Hoax II, seizing tens of thousands of counterfeit and pirated goods at international mail facilities and express courier depots worldwide during a two-month operation that began in November 2011. The 43 countries participating in the Operation shared information and intelligence using CENcomm, the WCO's secure communication tool, with the aim of stemming the growing flow of illicit counterfeit and pirated products being delivered to consumers via mail or by express courier services. Press Release

TSA:

FEB 21 – TSA announced the appointment of Carter Morris and Bill Cason to be the respective Chairman and Vice-Chairman of the Aviation Security Advisory Committee (ASAC). ASAC is TSA's sole federal advisory committee that gives the agency recommendations for improving civil aviation security methods, equipment and procedures.

FBI:

FEB 17 –Director Mueller named John Boles special agent in charge of the FBI's Norfolk Division. Mr. Boles most recently served as a special assistant to the National Security Branch (NSB) executive assistant director, and as section chief of the NSB Executive Staff Section. Press Release

DOJ:

FEB 23 – Attorney General Eric Holder delivered remarks at Columbia University Law School on preventing and combating financial fraud.

FEB 22 – Attorney General Eric Holder delivered remarks at the Department of Justice African-American History Month Celebration.

FEB 17 – Amine El Khalifi, an immigrant from Morocco who is illegally present in the United States, was arrested for allegedly attempting to detonate a bomb in a suicide attack on the U.S. Capitol Building as part of what he intended to be a terrorist operation. Press Release

FEB 16 – Umar Farouk Abdulmutallab, the so-called "underwear bomber," was sentenced to life in prison as a result of his guilty plea to all eight counts of a federal indictment charging him for his role in the attempted Christmas Day 2009 bombing of Northwest Airlines flight 253. Press Release

ODNI

FEB 22: Frank Montoya, Jr. has joined the Office of the Director of National Intelligence as the national counterintelligence executive. Press Release

AFGHANISTAN/PAKISTAN WAR:

FEB 22 –Afghan President Hamid Karzai appealed for calm on after officials said six people were shot dead and dozens wounded in protests over the burning of copies of the Koran, Islam's holy book, at NATO's main base in the country. Article

FEB 18 –Afghan President Hamid Karzai met with a Pakistani cleric linked to Taliban insurgents, a meeting that marked the first public contact between an Afghan official and members of the Afghan Taliban's support network in Pakistan in Afghanistan's bid to bring the militant movement to the negotiating table. The meeting between Karzai and the cleric was held in Islamabad said the cleric and Afghan officials, and shows how far the Afghan president is willing to go to open contact with the insurgent leaders. Article

FEB 16 –In an effort to rid their army of Taliban infiltrators, Afghan officials have begun ordering soldiers with families in Pakistan to either move their relatives to Afghanistan or leave the military. Article

GAO:

FEB 22 –Emergency Communications
Various Challenges Likely to Slow Implementation of a Public Safety Broadband Network
GAO-12-343

CONGRESS:

FEB 16 – Lawmakers keen on dedicating a parcel of radio spectrum for emergency responder communications have acknowledged that their proposal stood little chance of enactment before moving forward this week on the coattails of a payroll tax cut offset. For years legislators have worked to turn a piece of the 700 MHz radio spectrum known as the "D block" over to emergency responders for the creation of a next-generation communication system. But with several leading House Republicans insisting on selling the D block to raise revenue, legislation to create the public safety communications network was going nowhere.[See attached for CQ article]

FEB 16 –The Senate Homeland Security & Governmental Affairs Committee (HSGAC) held its first public hearing on The Cybersecurity Act of 2012 (S. 2105). The bipartisan Act, sponsored by HSGAC 's Chairman Joe Lieberman (I-CT), Ranking Member Susan Collins (R-ME), Commerce Committee Chairman Jay Rockefeller (D-WV), Select Intelligence Committee Chairman Dianne Feinstein (D-CA) and Sen. Sheldon Whitehouse (D-RI) is a product of three years of hearings, consultations, negotiations and failed attempts to pass comprehensive cyber legislation through the Congress in years past. While the Act did have its supporters, it also had its critics. The Act was supported by the White House, the Department of Homeland Security (DHS), the Department of Defense (DoD) and security experts. Critics of the bill, including the U.S. Chamber of Commerce, found fault with imposing undue regulatory and cost burdens on companies, stifling innovation and duplicating DHS's and DoD's cyber efforts in conjunction with the NSA. UPCOMING HEARINGS:

FEB 28 @ 10:00am – The House Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence will hold a hearing on, "Federal Government Intelligence Sharing with State, Local and Tribal Law Enforcement: An Assessment Ten years After 9/11." 311 Cannon Bldg

FEB 28 @ 2:00pm – The Senate Foreign Relations Committee will hold a hearing titled, "National Security & Foreign Policy Priorities in the FY2013 International Affairs Budget." Sec. of State Clinton will testify. 216 Hart Bldg

FEB 29 @ 10:00am – The House Committee on the Judiciary will hold a hearing on, "The U.S. Department of Justice Community Oriented Policing Services Office." 2141 Rayburn Bldg

FEB 29 @ 10:00am – The House Homeland Security Committee, Subcommittee on Emergency Preparedness, Response and Communications will hold a hearing on, "The President's FY2013 Budget Request for the FEMA." 311 Cannon Bldg

MAR 1 @ 10:00am – The House Homeland Security Committee, Subcommittee on Oversight, Investigations and Management will hold a hearing on, "Building One DHS: Why Can't Management Information be Integrated?" 311 Cannon Bldg

THINK TANKS:

FEB 23 – Senior Fellow Aaron Weisburd at the HSPI provides an assessment of Hizballah and Iran's Islamic Revolutionary Guard Corps.

FEB 20 –Americans most frequently mention Iran when asked to name the country they consider to be the United States' greatest enemy, and the 32% who do so is up from 25% in 2011. China is second on the list, with significantly fewer Americans mentioning North Korea, Afghanistan, and Iraq -- the countries that round out the top five. Gallup Poll

FEB 17 – James Carafano, Paul Rosenzweig and Jessica Zuckerman from The Heritage Foundation argue that C-TPAT needs to be restructured because the program lacks adequate initiatives to ensure the robust enduring cooperation of the private sector. Better incentives are also needed to keep the partnership moving forward. Issue Brief

FEB 17 – Washington, D.C., has climbed to the top of the list of cities with the highest risk of cybercrime, according to a new report by Symantec's Norton Internet Security and Sperling's BestPlaces. Seattle, San Francisco, Atlanta and Boston round out the top five in the second cyber risk study by the two organizations. ... The per-capita risk rankings factored in consumer behaviors including prevalence of PCs and smart phones, use of e commerce applications, social networking and the availability of potentially unsecured Wi-Fi hotspots.

FEB 16 - Americans are feeling more favorably toward several of the United States' major allies in 2012 than they have in the past. This year's ratings for Canada (96%), Australia (93%), Germany (86%), Japan (83%), and India (75%) are all record highs for those countries in Gallup trends that stretch back at least a decade. Gallup Poll

UPCOMING EVENTS:

MAR 13 from 7:30-9:30 am – INSA and The Government Executive Media Group will sponsor an event on, "Advancing the Intelligence Community: Harnessing the Power of Cloud Computing." Location: National Press Club, 529 14th St., NW RSVP

ARTICLES/ REPORTS OF INTEREST:

FEB 22 – Security Test Staged in London Subway. ESPN. Article

FEB 22 – Kevin Rudd Resigns as Australia's Foreign Minister. The New York Times. Article

FEB 21 – GPS Attacks Risk Maritime Disaster, Trading Chaos. Reuters. Article

FEB 21 – UN Estimates Cocaine Trafficking in West, Central Africa Generate $900 Million Annually. The Washington Post. Article

FEB 21 – Does 'Secure the Border' Mean "Keep America White"? CNN. Opinion

FEB 20 –U.S. in Accord with Mexico on Drilling. The New York Times. Article

FEB 17 – Drones Set Sights on U.S. Skies. The New York Times. Article

FEB 15 – Canada and the U.S. No Longer Separated by Border Horrors. The Huffington Post. Article

Kathleen Tolan
Counsellor
Public Safety and Border Security
Public Safety Canada
501 Pennsylvania Avenue, N.W.
Washington, D.C. 20001-2114
Tel: (202) 448-6338 Cell: [redacted]
Fax: (202) 682-7792
Email: katie.tolan@international.gc.ca

s.19(1)

Dvorkin, Corey

From: Scrivens, Mark <Mark.Scrivens@justice.gc.ca>
Sent: February-23-12 3:57 PM
To: Pilon, Claude; [redacted] Dick, Robert; Dvorkin, Corey; Hatfield, Adam
Subject: How Anonymous is currently regarded by the U.S. Intelligence leadership

One perspective:

http://www.theatlantic.com/technology/archive/2012/02/who-do-you-trust-less-the-nsa-or-anonymous/253399/

Mark Scrivens
Senior Counsel | Avocat-conseil
Office of the Assistant Deputy Attorney General | Bureau du Sous-Procureur Général Adjoint
Public Safety, Defence, and Immigration Portfolio | Portefeuille de la Sécurité Publique, de la Défense, et de l'Immigration et Sécurité Publique

Justice Canada
Jean Edmonds, Tower South | Tour Sud
365 Laurier Avenue West | 365 Avenue Laurier Ouest 15th Floor | 15e étage, OTTAWA, ON
K1A 1L1
mailto:mscriven@justice.gc.ca
Telephone | Téléphone (613) 954-1248
Facsimile | Télécopieur (613) 957-7840

Page 2108

is a duplicate

est un duplicata

Page 2109

is a duplicate

est un duplicata

Page 2110

is a duplicate

est un duplicata

Page 2111

is a duplicate

est un duplicata

Page 2112

is a duplicate

est un duplicata

Page 2113

is a duplicate

est un duplicata

CYBERDO

From: CYBERDO
Sent: February-20-12 12:12 PM
To: Beaudoin, Luc; 'Gurb Singh (Gurbinder.Singh@rcmp-grc.gc.ca)';
Cc: CYBERDO; 'Lee Shields (Lee.Shields@rcmp-grc.gc.ca)'; Bergeron, Dominic; Anderson, Windy; Bendelier, Kenneth
Subject: RE: Anonymous and Minister of PS
Attachments:

s.15(1) - Subv
s.16(2)(c)

As you might be aware of it there is a pastebin link to the event:

http://pastebin.com

Cyber Duty Officer
Public Safety Canada
CCIRC
www.publicsafety.gc.ca

-----Original Message-----
From: Beaudoin, Luc
Sent: February-20-12 10:41 AM
To: Gurb Singh (Gurbinder.Singh@rcmp-grc.gc.ca);
Cc: CYBERDO; Lee Shields (Lee.Shields@rcmp-grc.gc.ca); Bergeron, Dominic; Anderson, Windy; Bendelier, Kenneth
Subject: Anonymous and Minister of PS

Something to monitor. I would expect that the Minister may be personally targeted (web mail, past public records, facebook, etc) rather than a DDOS or attack on PS network , but Anonymous has successfully infiltrated organisations before (ex: HBGary).

http://www.theglobeandmail.com/news/politics/anonymous-targets-toews-over-lawful-access-bill/article2343432/

``

Public opposition to the federal government's "lawful access" bill continued to grow over the weekend, as hacker group Anonymous stepped into the fray with a threat to reveal more personal information about Public Safety Minister Vic Toews if the legislation isn't scrapped.

....

On Saturday, someone claiming to represent Anonymous posted a YouTube video demanding that Mr. Toews step down and threatening to release personal information about him if Bill C-10 goes forward.

More than 100,000 people have signed an Openmedia.ca petition opposing the bill, and online comment boards are packed with users expressing concern about its privacy implications. But pollster Darrell Bricker said it's unlikely that most people in the broader public would have paid attention to the issue had it not been for some polarizing comments Mr. Toews made last week.

....

``

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

CYBERDO

From: [redacted] s.15(1) - Subv
Sent: February-20-12 11:58 AM
To: Beaudoin, Luc
Cc: CTEC
Subject: RE: Anonymous and Minister of PS

Classification: UNCLASSIFIED

Hi Luc,

We'll keep our eyes peeled.

Thanks,

[redacted]
GC-CTEC - Cyber Duty Officer
--
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point or the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems. To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca Need to report an incident? Find the Incident Report Form here: http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf

-----Original Message-----
From: Beaudoin, Luc [mailto:LucS.Beaudoin@ps-sp.gc.ca]
Sent: February 20, 2012 10:41 AM
To: Gurb Singh (Gurbinder.Singh@rcmp-grc.gc.ca); CTEC
Cc: CYBERDO; Lee Shields (Lee.Shields@rcmp-grc.gc.ca); Bergeron, Dominic; Anderson, Windy; Bendelier, Kenneth
Subject: Anonymous and Minister of PS

Something to monitor. I would expect that the Minister may be personally targeted (web mail, past public records, facebook, etc) rather than a DDOS or attack on PS network , but Anonymous has successfully infiltrated organisations before (ex: HBGary).

http://www.theglobeandmail.com/news/politics/anonymous-targets-toews-over-lawful-access-bill/article2343432/

''

Public opposition to the federal government's "lawful access" bill continued to grow over the weekend, as hacker group Anonymous stepped into the fray with a threat to reveal more personal information about Public Safety Minister Vic Toews if the legislation isn't scrapped.

....

On Saturday, someone claiming to represent Anonymous posted a YouTube video demanding that Mr. Toews step down and threatening to release personal information about him if Bill C-10 goes forward.

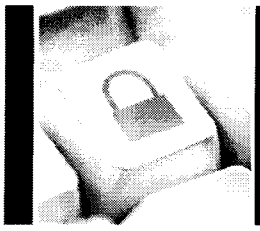
More than 100,000 people have signed an Openmedia.ca petition opposing the bill, and online comment boards are packed with users expressing concern about its privacy implications. But pollster Darrell Bricker said it's unlikely that most people in the broader public would have paid attention to the issue had it not been for some polarizing comments Mr. Toews made last week.

....

``

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Feb 17 2012



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

ANONYMOUS

EXECUTIVE SUMMARY

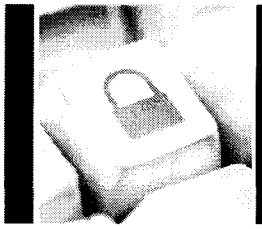
This report provides an overview of the hacktivist group, "Anonymous" and contains: information on its organizational structure, tradecraft, and targets; the threat to GC systems; and, CTEC's prevention and mitigation advice. "Anonymous" targets governments, private firms and individuals whose activities or purposes appear to be in conflict with principles espoused by the group. These principles mainly focus on: civil rights (e.g. oppressive government regimes); and, information accessibility (e.g. perceived government-mandated Internet censorship).

Based on a view of previous targeting by "Anonymous", Government of Canada systems could be targeted due to: government legislative initiatives (e.g. Copyright Modernization Act); and, political initiatives that may result in activist opposition (e.g. environmental or social issues). Specific targets are chosen in a variety of ways, including: through online polls following discussions in Internet Relay Chats (IRC[1]); opposition to "Anonymous'" campaigns, such as the ongoing "Operation Anti-Security"; as a response to provocations made by companies, governments or other hacking groups; and, as targets of opportunity, following searches for vulnerable systems.

"Anonymous" uses a number of capabilities against its targets. These include, but may not be limited to Distributed Denial of Service (DDoS[2]), password cracking, SQL injections[3], and malware (virus) deployments. Canadian organizations have been both direct and indirect targets of "Anonymous" activity, for example: the Toronto Police Service website was hacked in 2011, likely in response to "Occupy Toronto" camp evictions; Canadian corporations involved with the Alberta Tar Sands have been targeted, in particular to protest against the Keystone XL pipeline; and Subsequent to a late-2011 breach of STRATFOR, a US corporation with links to intelligence and law enforcement organizations, credentials used by Canadian federal departments to access STRATFOR databases were published. Although "Anonymous" leverages a variety of tradecraft to achieve its aims, strong IT security practices will help to defend against "Anonymous" exploits. The majority of these exploits are not "zero-day[4]". Please refer to the "Mitigation" section and Annex 1 for details.

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their own agendas. Most notably, "Anonymous" is a term that refers to a group of activist hackers, or "hacktivists," who pose a wide range of cyber threats to government and commercial organizations around the world. Anonymous' agenda has included initiating cyber threat activities in protest of perceived government-mandated Internet censorship, and in support of worldwide activist movements.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

STRUCTURE

Anonymous is loosely composed of sub-groups (e.g.: Anon-ops[5], LulzSec[6]) and often conducts joint campaigns with other hacktivist groups in support of the same agenda. For example, "TeaMp0isoN" and "People's Liberation Front" are separate hacktivist groups with the freedom to opt-in or opt-out of projects conducted jointly with Anonymous. In addition, the Anonymous movement has inspired copycat actions from other hacktivist groups, such as LulzRaft[7].

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several "unofficial" spokespeople[8], Anonymous does not officially have a specific spokesperson. The only requirement for members of Anonymous (known as "Anons") is that they must always remain anonymous while participating in cyber campaigns supporting Anonymous' efforts.

In many cases, Anons voluntarily join a botnet by downloading and installing the Low Orbit Ion Cannon (LOIC)[9] onto their computers. (Comment: The absence of a defined leadership structure is possibly why some threats associated with Anonymous are carried out, whereas others become empty threats if general consensus of a target was not agreed upon by the group at large.)

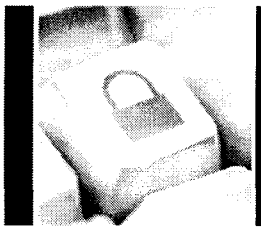
CHOOSING TARGETS

Since Anonymous is decentralized, new targets are determined in a variety of ways. Some of the most commonly utilized and documented methods of selecting targets are: through consensus among Anons using online polls (following a discussion on an Internet Relay Chat (IRC), an online poll will be conducted to determine the target(s) of DoS/DDoS attacks. Although it appears to be a democratic process, elite Anons who are IRC channel operators are the ones who make the final decision about where to direct the LOIC attacks); as a response to perceptions of direct or indirect provocation by governments, by other hacking groups or companies (e.g. HBGary[10]), against the group as a whole, or against the principles to which Anonymous adheres; and, to "expose" poor security practices: for instance, Anonymous members may use "Google Hacking" to identify vulnerable targets of opportunity.

These targeting practices are generally implemented in support of a specific Anonymous objective or campaign. For instance, one key Anonymous raison-d'être is to promote the ongoing "Operation Anti-Security" (also known as "AntiSec"); which is a declaration of cyber warfare on governments and corporations in response to perceived corruption and Internet censorship. As part of this campaign, Anonymous members are encouraged to locate and leak classified government information and to target banks or other high-profile establishments.

PAST TARGETS/BEHAVIOUR

Anonymous has initiated cyber threat activities in protest of government decisions and in support of their own principles. Its hacktivism efforts have recently been concentrated on the various Occupy[11] movements, on protesting Internet censorship and Internet filtering, on protesting against oppressive regimes, and on supporting WikiLeaks. These campaigns include:



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

2008:

PROJECT CHANOLOGY (worldwide):

Action: DDoS attacks were launched against the Church of Scientology websites and non-violent protests worldwide.

Reason: The Church of Scientology was attempting to restrict access to information which it found embarrassing and was readily available on the Internet.

2009:

ANONYMOUS IRAN (Iran):

Action: Creation of an Iranian Green Party Support site, Anonymous Iran, to provide covert resources and event updates to Iranian protestors during government-imposed Internet information censorship.

Reason: To provide support to Iranian protestors against a regime perceived to be corrupt.

OPERATION DIDGERIDIE (Australia):

Action: a DDoS attack was launched against the Australian Prime Minister's website.

Reason: To protest against proposed government policy and legislation related to the implementation of ISP-level blacklists.

2010:

OPERATION TITSTORM (Australia):

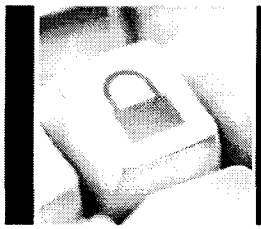
Action: DDoS attack against the Australian Parliament's website and web defacement of the Prime Minister's website.

Reason: To protest against the implementation of an Internet filter that would block websites containing child abuse material and certain types of pornography.

OPERATION PAYBACK/OPERATION SONY (worldwide):

Action: DDoS attacks against Sony PlayStation websites.

Reason: To support online file-sharing and to retaliate against Sony for seeking legal action against two individuals who successfully hacked the PlayStation3 system to allow users to run generic applications[12].



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

OPERATION AVENGE ASSANGE (USA):

Action: DDoS attacks against the Amazon, Paypal, Mastercard and Visa websites.

Reason: To show support for WikiLeaks and to protest against its founder's arrest.

OPERATION ZIMBABWE (Zimbabwe):

Action: DDoS attacks against the Government of the Republic of Zimbabwe's websites.

Reason: To protest against censorship of WikiLeaks documents.

2011:

OPERATION TUNISIA (Tunisia):

Action: DDoS attack on the Government of Tunisia's websites.

Reason: To protest against Internet censorship; and to support the Arab Spring[13].

OPERATION SYRIA (Syria):

Action: Web defacement of Syrian Defence Ministry website.

Reason: To support the Arab Spring (Syrian uprising).

OPERATION EGYPT (Egypt):

Action: DDoS attack against the Government of Egypt's website and the website of the National Democratic Party. Also released the names and passwords of email addresses of government officials.

Reason: To support the Arab Spring (Egyptian revolution).

HBGARY FEDERAL (USA):

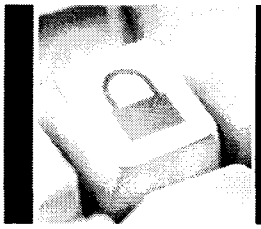
Action: The defacement of HBGary's website, the deletion of company files and the publication of 68,000 employee emails.

Reason: HBGary official provoked Anonymous by threatening to expose information about the group.

BANK OF AMERICA (USA):

Action: The release of sensitive Bank of America documents online which allegedly prove cases of corruption and fraud at the bank.

Reason: To protest in support of allegations of corruption and fraud within the US banking system.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

OPERATION MALAYSIA (Malaysia):

Action: DDoS attacks on 91 Government of Malaysia's websites.

Reason: In response to the Malaysian government's censorship of sites like the Pirate Bay[14] and WikiLeaks.

OCCUPY WALL STREET (USA):

Action: DDoS attacks on the Oakland Police Department website and the St. Louis mayor's website.

Reason: To protest evictions of protestors from Occupy sites; in support of the worldwide Occupy movement.

OPERATION MAYHEM (USA):

Action: The release of Guy Fawkes virus on Facebook.

Reason: To protest the Stop Online Piracy Act[15], perceptions of police violence towards protestors in Occupy movements, and any opposition to Anonymous activities.

COX COMMUNICATIONS (USA):

Action: Domain name system (DNS) servers taken offline, removing Internet access for clientele in most of southwest America.

Reason: To protest Cox Communications' attempted regulation of customer's data usage quota.

OPERATION BLACKOUT (USA):

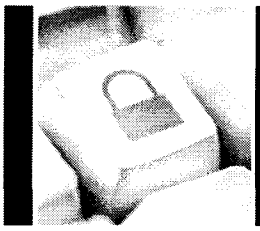
Action: In November, Anonymous threatened action against the US government.

Reason: To protest against the Stop Online Piracy Act.

STRATFOR (worldwide):

Action: STRATFOR is a US company that provides services to intelligence and law enforcement agencies, among others. 200 gigabytes of data were stolen from STRATFOR's web servers and subsequently published. The stolen information included active credit cards, e-mail addresses, phone numbers, encrypted passwords and sensitive information from clients (including governments and military departments). Anonymous planned to donate to charities using the stolen credit card information.

Reason: Following the HB Gary incident, Anonymous began to investigate what it refers to as a "state-corporate alliance against the free information movement." Due to STRATFOR's ties with the intelligence and military contracting sectors and government agencies, Anonymous believed that



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

targeting STRATFOR would "improve [their] ability to continue this investigation and thereby bring to light other instances of [perceived] corruption, crime and deception on the part of certain powerful actors based in the U.S. and elsewhere.[16]"

Ongoing:

OPERATION ANTISEC (NATO, Tunisia, Brazil, Australia, USA, Turkey, UK, and other countries):

Action: In USA: DDoS attacks against the Central Intelligence Agency's (CIA) website; the US Senate website was hacked, and information about its internal server structure was released. In UK: DDoS attacks against the Serious Organised Crime Agency's (SOCA) website.

Reason: The declaration of cyber warfare on governments and corporations worldwide in response to perceived corruption and government censorship.

CANADA

Anonymous has directly and indirectly targeted the Government of Canada, Canada's municipal governments and Canadian private corporations.

Government of Canada:

STRATFOR (December 2011):

The federal government has been an indirect target of anonymous activity in connection with STRATFOR. STRATFOR is a resource used by various federal departments. When usernames and passwords were released by Anonymous, some of them included those of federal employees[17].

Municipal Governments:

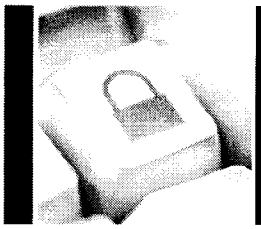
TORONTO (November 2011):

Anonymous threatened to take down the City of Toronto's website if officials evicted protestors from the Occupy Toronto camp. Although no known activity was conducted against the City of Toronto's website, the Toronto Police Service website was hacked and several usernames and passwords were stolen, possibly in retaliation to the continued efforts to evict the Occupy camp.

Private Corporations:

OPERATION GREEN RIGHTS/ PROJECT TARMAGGEDON:

In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline, and the Alberta Tar Sands project. Those targeted have included Canadian Oil Sands Ltd, Imperial Oil, Syncrude, and Suncor.



Future Activity

Although it is impossible to fully predict Anonymous' behaviour, based on prior targeting, there are a few government bills that would direct Anonymous' attention towards the Government of Canada. Copyright Modernization Act: As a part of this bill, ISPs would be responsible for sending notices from copyright holders to Internet users alleged to have participated in illicit downloading and file-sharing online. The ISPs would also be required to retain records which establish the identity of the subscriber and disclose it in court if necessary. (Comment: This could be seen by Anonymous as an attempt to limit consumer rights. Previous protests against government-issued copyright laws in Australia and the USA resulted in Anonymous launching DDoS attacks on Australian government websites and the US Copyright Office.)

Lawful Access Package:

The government's announcement to reintroduce Lawful Access legislation[18] that would require telecommunications companies, including ISPs to ensure intercept capabilities on their network. ISPs would also be required to disclose certain information on persons of interest to law enforcement authorities without a warrant under specific circumstances. (Comment: This could be seen by Anonymous as a violation of privacy. Similar perceptions have prompted Anonymous to take action against Facebook[19].)

TRADECRAFT

Anonymous has traditionally used basic, open-source-available cyber threat tradecraft against their targets. However, beginning in mid-2011, Anons have begun developing their own malware. (Comment: The exploits below do not represent a conclusive list because Anonymous includes a large number of members and all of their activities cannot be tracked and attributed to Anonymous.)

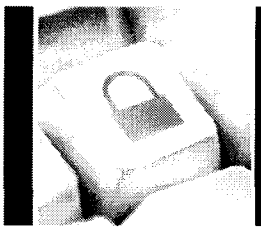
Open Source resources:

DoS/DDoS:

Anonymous' usual method of choice is to launch DoS/DDoS attacks against a target's website in an effort to bring the network offline and to make the website unavailable to legitimate users. Two commonly used methods include:

1) LOIC:

Anons are encouraged to download and launch the Low Orbit Ion Cannon application enabling them to willingly participate in a botnet. The LOIC is pointed at a target of choice, which would then disrupt the service of the victim's host. However, since LOIC could reveal the IP addresses of its users, it's traceability has prompted Anonymous to find other means of attacks.



2) Apache Killer:

The Apache DoS tool nicknamed the "Apache Killer" exploits a vulnerability which allows remote attackers to send requests to servers via a malformed uniform resource identifier (URI)[20]. It is designed to drain the web server's memory, which would then take the website offline. It also allows a remote attacker to use a single computer to wage DoS attacks against an Apache server.

Anonymous-developed tools:

DoS/DDoS via SQL Injections:

#RefRef:

Anonymous developed and released a Perl DDoS tool in September, #RefRef, that exploits SQL[21] vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline. #RefRef could be used in combination with tools such as Havij, an SQL Injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities. As a result of SQL vulnerability exploitation, database content could be changed, or database information (such as credit card information or passwords) could be stolen.

Guy Fawkes virus:

Malware development is also something that Anonymous members have been focusing on. The Guy Fawkes[22] virus was developed by Anon to take control of a Facebook account and use it to spread malware to other members without the users actually logging onto the site. According to security analysts at the antivirus software company BitDefender, the Guy Fawkes virus (which they have named Backdoor-Bifrose-AAJX) has the ability to inject itself in the Internet Explorer process, providing a remote attacker with unhindered access to the compromised system. It would also record keystrokes and disrupt processes of known antimalware software. (Comment: Although the Guy Fawkes virus was previously believed to be responsible for the massive pornographic spam attack against Facebook in November 2011, this was later refuted by Facebook and BitDefender. Anonymous has stated that it is still working to control the virus to be used at a later date.)

Other:

Other techniques used by Anonymous include using social engineering techniques to gain access to victims' systems (e.g. HB Gary Federal), using web defacement to post embarrassing messages on victims' websites, using password cracking to exfiltrate data from a victim's database, and using a Twitter raiding tool called Universal Rapid Gamma Emitter (URGE) to hijack Twitter trending topics into topics of interest to Anonymous. It also allows Anons to tweet messages within the topics.

MITIGATION

Since Anonymous has a wide range of targets, it is difficult to measure which vulnerabilities are most frequently exploited by the group. However, as noted, the threats leveraged are generally limited to open source or well-known vulnerabilities. As a result, strong IT security practices will go a long way to defending against an Anonymous cyber threat. Implementing CCIRC's mitigation guidelines for advanced persistent threats and DDoS attacks is also recommended[23]. In addition, the following mitigation is available for some of the tradecraft[24] specifically noted above:

1. DoS/DDoS attacks.

a)Use network segmentation and segregation into security zones to protect high value assets using routers to spot and drop DDoS connections.

b)If the DDoS is pointed at a specific IP, the target site could be blackholed. This typically requires working with upstream network providers to forward malicious traffic to a non-existent network interface, where the offending traffic will be dropped.

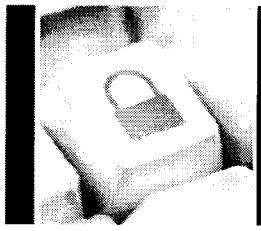
b) In some cases, if a DDoS is anticipated, it may be possible to temporarily have additional bandwidth provisioned to your network. This will lessen the impact on the target for some DDoS incidents.

2. "Apache Killer."

a) Apache has since released patches to fix this vulnerability. All users are recommended to upgrade to Apache 2.2.20 or higher.

3. "#RefRef."

a) Webcode should be hardened[25] against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

1 IRC is a protocol for Internet text messaging and synchronous conferencing. It allows group communications as well as private messaging and file sharing.

2 A denial-of-service (DoS) or a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.

3 SQL injection is often used to attack the security of a website by injecting SQL commands into the database of an application to change the database content or to dump database information to the attacker.

4 Zero-day threats attempt to exploit new computer application vulnerabilities not yet known to the software developer or the general public.

5 Anon-ops provides communications for Anonymous' announcements.

6 LulzSec was a small team that joined forces with Anonymous in the ongoing "Operation Anti-Security" or "AntiSec" campaign, which later disbanded in the summer of 2011.

7 LulzRaft was inspired by LulzSec group and has been responsible for web defacement of the website for the Conservative Party of Canada and for accessing private information about the party's donors. They have also been linked to web defacement of the website of Calgary-based energy company, Husky Energy.

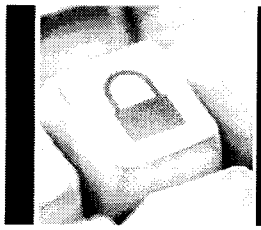
8 Unofficial spokespeople for Anonymous include Jake Davis (also known by his online nickname "Topiary,") Barrett Brown, etc. For more information on Jake Davis, please see http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-ukpolice/. For more information on Barrett Brown, please see http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx.

9 According to open source, LOIC is an open source network stress testing application which performs DoS or DDoS attacks on a target site by flooding the server with TCP or UDP packets to disrupt the service of a host.

10 HBGary Federal is a technology security company who was working with the FBI to unmask members of Anonymous. In February 2011, the CEO Aaron Barr revealed an intention to release information on the identities of Anonymous members. As a result, Anonymous members compromised the HBGary website, stole and publicly released the company's documents and emails.

11 According to open source, the Occupy movement refers to an international protest movement directed against high unemployment, social and economic inequality and perceived corruption in corporations and government.

12 For more information, please refer to http://www.pcmag.com/article2/0,2817,2383018,88.asp.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

13 The Arab Spring refers to revolutionary protests occurring in the Arab world beginning in December 2010. Countries affected include Tunisia, Egypt, Libya, Bahrain, Syria, Yemen, Algeria, Iraq, Jordan, Kuwait, Morocco, Oman, Lebanon and Saudi Arabia.

14 The Pirate Bay is a Swedish website known for facilitating illegal downloads and supporting the international anti-copyright movement.

15 The Stop Online Piracy Act is proposed US legislation to combat against the online distribution of copyrighted intellectual property. This has been viewed by Anonymous as an attempt to censor the Internet.

16 For the full explanation, please refer to Barret Brown's statement at http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-hacked.

17 CTEC has provided mitigation to employees of the affected departments.

18 This legislation will be similar to the previous Bill C-50, Bill C-51 and Bill C-52.

19 Operation Facebook was launched on November 5th, 2011 because Anonymous believes that "Facebook is the opposite of the Antisec cause."

20 For more information, please refer to CVE-2011-3192 at http://nvd.nist.gov/.

21 An SQL server is a relational database server that can store and retrieve data across a network (e.g. the Internet). Queries from client machines are formatted in the SQL language.

22 Guy Fawkes was associated with the Gunpowder Plot, a failed assassination attempt against King James I of England in 1605. The conspirators' plan was to blow up the Houses of Parliament in order to kill the King and the Members of Parliament. Coincidentally, Anons have adopted the easily available and inexpensive Guy Fawkes mask as their symbol.

23 [http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx] + [DDoS hyperlink when finished]

24 Security analysts are still undergoing analysis on the Guy Fawkes virus; as such, we are unable to provide mitigation at this time. In addition, since URGE is not a hacking tool, there does not appear to be any mitigation actions provided at this time.

25 Hardening minimises access between the public facing HTTP server and the SQL database. It also validates requests sent by external clients to the HTTP server.

Page 2129

is a duplicate

est un duplicata

Page 2130

is a duplicate

est un duplicata

Page 2131

is a duplicate

est un duplicata

Mitigation Guidelines for Denial-of-Service Attacks

Number: TR12-001
Date: 22 February 2012

Audience

This Information Report is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries. The recipients of this product may further distribute it to technical stakeholders within their organization.

Purpose

The purpose of this Information Report is to provide IT security personnel with an introduction to distributed denial-of-service (DDoS) attacks, their modus-operandi and the recommended steps to help with the preparation, identification, containment, recovery and continuous improvement efforts required to limit associated organizational risk. This document may be used by system administrators, computer security incident response teams (CSIRTS), IT security operations centres and other related technology groups.

Introduction

Denial of service (DoS) attacks are common malicious network actions aimed at disrupting the availability of computing resources from legitimate users. These types of attacks, especially DDoS attacks have recently gained in popularity due to the availability of DoS rental services from botnet operators, as well as the availability of various free and easy to use hacking tools. The latter have enabled activists using hacking to support their causes (also known as hacktivists) to efficiently recruit large numbers of followers to perpetrate cyber attacks, increasing both their distribution and power. Well known examples of DoS attacks include the use of the Low Orbit Ion Cannon DDoS tool in support of Wikileaks[1] used by hacking group "Anonymous" and attacks against national infrastructures such as Korea[2] , Georgia[3] and Estonia[4].

DoS and DDoS definition

A DoS attack is an attempt to make a computer resource unavailable to its intended users[5]. A DDoS attack occurs when multiple systems simultaneously flood networked computer resources, rendering them inaccessible. A DDoS attack, in contrast with a DoS attack, comes from many sources, often hundreds or even thousands. As a result, mitigation actions against a DDoS attack are more difficult to coordinate and associated traffic is more damaging to the target.

DDoS attacks often use stateless protocols such as UDP and ICMP, but stateful protocols can also be used when the connections are not fully established such as during a TCP SYN flood attack. Both techniques make it easier for the attacker to use spoofed IP addresses and harder to determine the source of the attack.

Five Steps To Defend Against DDOS Attacks

Preparation

Preparation is the most important step in defending against a DDoS attack. Clear and complete procedures and guidelines should be established well before an attack takes place. Any organization can fall victim to DDoS attacks, either directly or indirectly. Having a solid plan in place will help reduce the risk and lessen the impact should an attack occur.

Identification

Indicators that your organization may be under a DDoS attack could include poor network performance, inaccessible services or system crashes. Being able to identify and understand the nature of the attack and its targets will help in the containment and recovery process. For this purpose, organizations require tools that provide visibility over their managed information technology (IT) infrastructure. Often, prior to a DDoS attack, a reconnaissance of the target is performed by the attacker. This may include scanning the target network for known exposed vulnerabilities or sending malformed packets to the target host to analyze changes in response time. This reconnaissance activity may be hard to detect, especially because it may take place well before the attack itself. A knowledgeable attacker will also ensure scan traffic does not meet the threshold required to trigger alarms from network monitoring tools. However, there may be available intelligence indicating an increased likelihood of a DDoS attack against an organization. Good examples are the Anonymous Operations (aka "anonops")[6] , which broadly advertise their motivation and targets.

Containment

Having a pre-determined containment plan before an attack for a number of scenarios will significantly improve response speed and limit damages resulting from a DDoS attack. For example, the containment strategy for a mail server may differ from one for a web server. Underestimating the importance of this phase can result in mistakes and significant collateral damages. Therefore, understanding the nature of DDoS attacks and documenting the associated decision-making process is critical. An organization should clearly identify its network perimeter and exposed assets. Load balancers, modern firewall technologies (Deep Packet Inspection, proxy, application layer filtering), content caching, content hosting geographic diversity, dynamic DNS service and ISP-based DDoS protection services are some of the tools an organization may leverage to contain an ongoing DDoS attack.

Recovery

Depending on the containment strategy employed and the sensitivity to its collateral impact, an organization may be under different pressure to recover from a DDoS attack. Understanding the characteristics of the attack is required for an appropriate recovery. DDoS may exploit limits in the following resources:

- Server queue length
- Server computing resources
- Client tolerance to level of service variability
- Bandwidth

A DDoS attack may exploit any or a combination of these limitations. An organization equipped with a flexible provisioning model for these resources may be able to rapidly adapt and sustain long-term DDoS attacks. However, some attacks may leverage vulnerabilities in protocols or software and achieve unexpected high impact as a result.[7] An organization equipped with packet capture capability may be able to identify the delivery method of the attack and potentially design an accurate Intrusion Prevention System / Firewall signature. Despite mitigation efforts, some

DDoS attacks may be persistent over time. An organization using connection logs and other tools may be able to provide a list of potentially offending IP addresses (if not spoofed) to their upstream ISP, law enforcement and national Computer Emergency Response Team (CERT) to coordinate mitigation/investigation of the offending sources.

Lessons Learned

Lessons learned is a very important step that is often overlooked. Lessons learned activities should take place as soon as possible following an incident. All decisions and steps taken throughout the incident handling cycle should be reviewed. All procedures should be reviewed to see where improvements may be made.

Perhaps the most challenging part of performing a Lessons Learned review involves documenting the impact and cost the incident caused to the organization. Although time consuming, this step is essential to allow organizations to properly justify security resources and assess their return on investment. Damages to an organization include tangible metrics, such as loss in sales and productivity, as well as intangible metrics, such as reputation and brand.

By performing this review after each incident, organizations will enable continuous improvement and potentially significant reduction in the impact of incidents.

Checklist

The following checklist is intended to help organizations during the various mitigation phases of DDoS attacks. Many of these mitigations are applicable to other types of cyber attacks as well and should be considered accordingly.

Checklist for mitigation phases of DDoS attacks

#	Item	In progress	Completed
	Preparation		
1.	Identify your most critical assets and the services they provide. ■ Are they up to date with the latest patches? ■ Do they run any unnecessary services such as Telnet or FTP?		
2.	Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.		
3.	Establish 24/7 contact information for your ISP and alternate methods for communications.		
4.	Deny all obviously spoofed traffic (e.g., internal IP addresses that should not be coming in or going out of your network). Implement a bogon block list (unallocated address space) at the network boundary.		
5.	Establish procedures on how to segregate your networks in the event of a DDoS attack. Use existing network devices, such as routers and managed switches, to defend against DDoS attacks. Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls.		
6.	Disable all unnecessary services and restrict access to and from all previously identified critical hosts based on DDoS traffic characteristics.		
7.	Create a whitelist of the source IPs you must allow if you need to prioritize traffic during an attack.		
8.	Document your network topology including all IP addresses. Keep it up to date.		

9.	Review your Business Continuity Plan (BCP) and ensure senior management and legal team understand the significance of a DDoS attack, including their roles.		
10.	Understand "normal." Establish a baseline of network traffic, CPU usage, connection and memory utilization of critical hosts under normal conditions so that network monitoring tools will trigger on abnormal changes.		
11.	Acknowledge that your organization may be attacked. Organizations should consider the development and implementation of policies, plans and procedures to defend against DDoS attacks. Identify and planfor resources to implement these plans.		
12.	Assign roles and responsibilities. Identify who plays a role in defending against a DDoS attack and ensure they are aware of this responsibility. This should include personnel from critical business functions, IT operations, network and IT security teams, legal advisors, and media relations staff. Ensure an up-to-date point-of-contact list with primary and alternate personnel is maintained. As the network may be unavailable, including mobile devices, ensure alternate communications mechanisms are in place.		
13.	Conduct exercises. The worst time to test plans and procedures is during an attack.		
	Identification		
1.	Determine if you are the primary target or a collateral victim. (ex: is your upstream internet provider or content hosting provider the target ?)		
2.	Understand the logical flow of the attack.		
3.	Determine what type of traffic is being used, such as IP addresses, ports and protocols.		
4.	Consider using network analysis tools to determine the type of traffic being used in the attack (e.g., TcpDump, Wireshark, Snort).		
5.	Review any available logs to understand the attack and what is being targeted.		
6.	Notify appropriate personnel. This may include senior management and the legal team.		
	Containment		
1.	Contact your ISP to implement filtering.		
2.	Block the traffic as close to the network cloud as possible (router, firewall, load balancer, etc.).		
3.	Relocate the target to another IP address if a particular host is being targeted. This is a temporary solution.		
4.	If a particular application is being targeted, consider disabling it temporarily.		
5.	Identify and correct the vulnerability or weakness that is being exploited. An example of this may be an unused service that is accidently left enabled on a public facing device or unpatched operating system.		
6.	Implement filtering based on the characteristics of the attack. An example may be blocking IMCP echo packets.		
7.	Implement rate limiting for certain protocols, allowing a certain number of packets per second for a specific protocol or to access a certain host.		
	Recovery		
1.	Confirm that the DDoS attack has finished and services are reachable again.		
2.	Confirm that your networks are back to your baseline performance.		
3.	If necessary, patch and update all affected machines.		

4.	If possible, identify the source of the attack. Enlist the help of your ISP.		
5.	Review logs for signs of reconnaissance. Maintain logs for possible future law enforcement requirements.		
Lessons Learned			
1.	Create or update the following documents: ■ Standard Operating Procedures ■ Emergency Operating Procedures ■ Business Continuity Plans		

Recommendations

CCIRC recommends that organizations assess their risk exposure to Denial of Service attacks which may be caused accidentally or intentionally and consider mitigation advice herein provided and implement them as appropriate for the specific IM/IT environment.

References

1. US-CERT, Understanding Denial-of-Service Attacks
http://www.us-cert.gov/cas/tips/ST04-015.html
2. NIST, Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
3. GovCERT.NL, Factsheet: Protect your online services against dDoS attacks
http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html
4. Societe Generale DDoS Incident Reponse
http://cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf

Reporting

Any Canadian Critical Infrastructure Operator wishing to report incidents may do so using the CCIRC Cyber Duty Officer PGP encryption key, found at:
http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/rprt-eng.aspx

Associated reports should be sent to:
cyber-incident@ps-sp.gc.ca.

Critical Note

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

---

[1] Introduction to LOIC: http://en.wikipedia.org/wiki/LOIC

[2] http://blogs.mcafee.com/mcafee-labs/malware-in-recent-korean-ddos-attacks-destroys-systems

[3] http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/

[4] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[5] Definition: http://en.wikipedia.org/wiki/Denial-of-service_attack

[6] http://anonops.blogspot.com/2011/09/tar-sands-action-september-3-press_04.html

[7] http://www.theregister.co.uk/2011/08/24/devastating_apache_vuln/

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) operates within Public Safety Canada, and works with partners inside and outside Canada to mitigate cyber threats to vital networks outside the federal government. These include systems that keep Canada's critical infrastructure functioning properly, such as the electrical grid and financial networks, or contain valuable commercial information that underpins our economic prosperity. CCIRC supports the owners and operators of systems of national importance, including critical infrastructure, and is responsible for coordinating the national response to any serious cyber security incident.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

Date Modified: 2012-12-20

CYBERDO

From: Williston, Sandra
Sent: February-17-12 1:27 PM
To: CYBERDO; Anderson, Windy
Cc: Beaudoin, Luc
Subject: RE: [redacted]

s.16(2)(c)
s.20(1)(c)

Windy;

[redacted]

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: CYBERDO
Sent: February-17-12 1:22 PM
To: Anderson, Windy
Cc: Beaudoin, Luc; CYBERDO
Subject: [redacted]
Importance: High

Windy;

CCIRC contacted CTEC immediately upon receipt of the below email.

CTEC was aware since this morning and have been in contact with [redacted] they do not require any assistance at this time.

No participation by CCIRC at this time.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

s.16(1)(b) s.16(2)

From:
Sent: February-17-12 1:10 PM
To: stephan.aube@parl.gc.ca; Beaudoin, Luc; CYBERDO
Subject: RE:
Importance: High

Hi All,

As you may be aware, see below.

Stef is the IT director and I think he can benefit from your assistance

He can share with you current activities that took place.

Stéphan Aubé
Dir. Opérations des TI, Chambre des communes
Dir. IT Operations, House of Commons
181, Queen, bureau-room 6-028, Ottawa, Ontario, Canada K1A 0A6
Tel.: (613)992-7449 - Fax: 613-947-6292 – E-Mail : aubes@parl.gc.ca

Regards,

From:
Sent: February-17-12 11:58 AM
To: 'saube@parl.gc.ca'
Subject: STEF:
Importance: High

Poste aujourdhui.

s.16(1)(b)

s.16(2)(c)

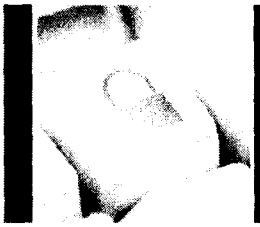
[redacted]

From: stephan.aube@parl.gc.ca [mailto:stephan.aube@parl.gc.ca]
Sent: February-17-12 1:07 PM
To: [redacted]
Subject: DDOS

Tel que discute !

Stéphan Aubé
Dir. Opérations des TI, Chambre des communes
Dir. IT Operations, House of Commons

181, Queen, bureau-room 6-028, Ottawa, Ontario, Canada K1A 0A6
Tel.: (613)992-7449 - Fax: 613-947-6292 – E-Mail : aubes@parl.gc.ca



CCIRC
Canadian Cyber Incident Response Centre

FIN12-502

BUILDING A **SAFE** AND **RESILIENT CANADA**

ANONYMOUS

created Feb 17, 2012

Consult CSEC ?

EXECUTIVE SUMMARY

This report provides an overview of the h
organizational structure, tradecraft, and targets; the threat to GC system
mitigation advice. "Anonymous" targets governments, private firms and
purposes appear to be in conflict with principles espoused by the group. These principles mainly focus on: civil rights (e.g. oppressive government regimes); and, information accessibility (e.g. perceived government-mandated Internet censorship).

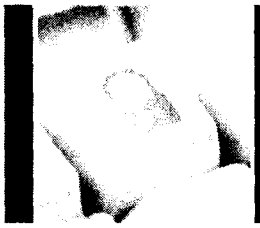
Based on a view of previous targeting by "Anonymous", Government of Canada systems could be targeted due to: government legislative initiatives (e.g. Copyright Modernization Act); and, political initiatives that may result in activist opposition (e.g. environmental or social issues). Specific targets are chosen in a variety of ways, including: through online polls following discussions in Internet Relay Chats (IRC[1]); opposition to "Anonymous'" campaigns, such as the ongoing "Operation Anti-Security"; as a response to provocations made by companies, governments or other hacking groups; and, as targets of opportunity, following searches for vulnerable systems.

"Anonymous" uses a number of capabilities against its targets. These include, but may not be limited to Distributed Denial of Service (DDoS[2]), password cracking, SQL injections[3], and malware (virus) deployments. Canadian organizations have been both direct and indirect targets of "Anonymous" activity, for example: the Toronto Police Service website was hacked in 2011, likely in response to "Occupy Toronto" camp evictions; Canadian corporations involved with the Alberta Tar Sands have been targeted, in particular to protest against the Keystone XL pipeline; and Subsequent to a late-2011 breach of STRATFOR, a US corporation with links to intelligence and law enforcement organizations, credentials used by Canadian federal departments to access STRATFOR databases were published. Although "Anonymous" leverages a variety of tradecraft to achieve its aims, strong IT security practices will help to defend against "Anonymous" exploits. The majority of these exploits are not "zero-day[4]". Please refer to the "Mitigation" section and Annex 1 for details.

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their own agendas. Most notably, "Anonymous" is a term that refers to a group of activist hackers, or "hacktivists," who pose a wide range of cyber threats to government and commercial organizations around the world. Anonymous' agenda has included initiating cyber threat activities in protest of perceived government-mandated Internet censorship, and in support of worldwide activist movements.

Luc's group has provided the "final" version of this note for this specific ATIP - I recommend throwing this version



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

STRUCTURE

Anonymous is loosely composed of sub-groups (e.g.: Anon-ops[5], LulzSec[6]) and often conducts joint campaigns with other hacktivist groups in support of the same agenda. For example, "TeaMp0isoN" and "People's Liberation Front" are separate hacktivist groups with the freedom to opt-in or opt-out of projects conducted jointly with Anonymous. In addition, the Anonymous movement has inspired copycat actions from other hacktivist groups, such as LulzRaft[7].

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several "unofficial" spokespeople[8], Anonymous does not officially have a specific spokesperson. The only requirement for members of Anonymous (known as "Anons") is that they must always remain anonymous while participating in cyber campaigns supporting Anonymous' efforts.

In many cases, Anons voluntarily join a botnet by downloading and installing the Low Orbit Ion Cannon (LOIC)[9] onto their computers. (Comment: The absence of a defined leadership structure is possibly why some threats associated with Anonymous are carried out, whereas others become empty threats if general consensus of a target was not agreed upon by the group at large.)

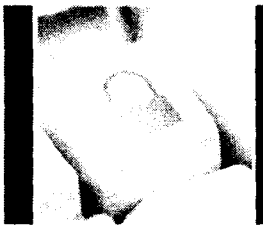
CHOOSING TARGETS

Since Anonymous is decentralized, new targets are determined in a variety of ways. Some of the most commonly utilized and documented methods of selecting targets are: through consensus among Anons using online polls (following a discussion on an Internet Relay Chat (IRC), an online poll will be conducted to determine the target(s) of DoS/DDoS attacks. Although it appears to be a democratic process, elite Anons who are IRC channel operators are the ones who make the final decision about where to direct the LOIC attacks); as a response to perceptions of direct or indirect provocation by governments, by other hacking groups or companies (e.g. HBGary[10]), against the group as a whole, or against the principles to which Anonymous adheres; and, to "expose" poor security practices: for instance, Anonymous members may use "Google Hacking" to identify vulnerable targets of opportunity.

These targeting practices are generally implemented in support of a specific Anonymous objective or campaign. For instance, one key Anonymous raison-d'être is to promote the ongoing "Operation Anti-Security" (also known as "AntiSec"); which is a declaration of cyber warfare on governments and corporations in response to perceived corruption and Internet censorship. As part of this campaign, Anonymous members are encouraged to locate and leak classified government information and to target banks or other high-profile establishments.

PAST TARGETS/BEHAVIOUR

Anonymous has initiated cyber threat activities in protest of government decisions and in support of their own principles. Its hacktivism efforts have recently been concentrated on the various Occupy[11] movements, on protesting Internet censorship and Internet filtering, on protesting against oppressive regimes, and on supporting WikiLeaks. These campaigns include:



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

2008:

PROJECT CHANOLOGY (worldwide):

Action: DDoS attacks were launched against the Church of Scientology websites and non-violent protests worldwide.

Reason: The Church of Scientology was attempting to restrict access to information which it found embarrassing and was readily available on the Internet.

2009:

ANONYMOUS IRAN (Iran):

Action: Creation of an Iranian Green Party Support site, Anonymous Iran, to provide covert resources and event updates to Iranian protestors during government-imposed Internet information censorship.

Reason: To provide support to Iranian protestors against a regime perceived to be corrupt.

OPERATION DIDGERIDIE (Australia):

Action: a DDoS attack was launched against the Australian Prime Minister's website.

Reason: To protest against proposed government policy and legislation related to the implementation of ISP-level blacklists.

2010:

OPERATION TITSTORM (Australia):

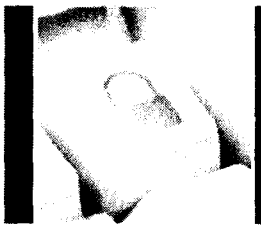
Action: DDoS attack against the Australian Parliament's website and web defacement of the Prime Minister's website.

Reason: To protest against the implementation of an Internet filter that would block websites containing child abuse material and certain types of pornography.

OPERATION PAYBACK/OPERATION SONY (worldwide):

Action: DDoS attacks against Sony PlayStation websites.

Reason: To support online file-sharing and to retaliate against Sony for seeking legal action against two individuals who successfully hacked the PlayStation3 system to allow users to run generic applications[12].



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

OPERATION AVENGE ASSANGE (USA):

Action: DDoS attacks against the Amazon, Paypal, Mastercard and Visa websites.

Reason: To show support for WikiLeaks and to protest against its founder's arrest.

OPERATION ZIMBABWE (Zimbabwe):

Action: DDoS attacks against the Government of the Republic of Zimbabwe's websites.

Reason: To protest against censorship of WikiLeaks documents.

2011:

OPERATION TUNISIA (Tunisia):

Action: DDoS attack on the Government of Tunisia's websites.

Reason: To protest against Internet censorship; and to support the Arab Spring[13].

OPERATION SYRIA (Syria):

Action: Web defacement of Syrian Defence Ministry website.

Reason: To support the Arab Spring (Syrian uprising).

OPERATION EGYPT (Egypt):

Action: DDoS attack against the Government of Egypt's website and the website of the National Democratic Party. Also released the names and passwords of email addresses of government officials.

Reason: To support the Arab Spring (Egyptian revolution).

HBGARY FEDERAL (USA):

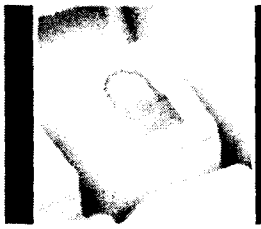
Action: The defacement of HBGary's website, the deletion of company files and the publication of 68,000 employee emails.

Reason: HBGary official provoked Anonymous by threatening to expose information about the group.

BANK OF AMERICA (USA):

Action: The release of sensitive Bank of America documents online which allegedly prove cases of corruption and fraud at the bank.

Reason: To protest in support of allegations of corruption and fraud within the US banking system.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

OPERATION MALAYSIA (Malaysia):

Action: DDoS attacks on 91 Government of Malaysia's websites.

Reason: In response to the Malaysian government's censorship of sites like the Pirate Bay[14] and WikiLeaks.

OCCUPY WALL STREET (USA):

Action: DDoS attacks on the Oakland Police Department website and the St. Louis mayor's website.

Reason: To protest evictions of protestors from Occupy sites; in support of the worldwide Occupy movement.

OPERATION MAYHEM (USA):

Action: The release of Guy Fawkes virus on Facebook.

Reason: To protest the Stop Online Piracy Act[15], perceptions of police violence towards protestors in Occupy movements, and any opposition to Anonymous activities.

COX COMMUNICATIONS (USA):

Action: Domain name system (DNS) servers taken offline, removing Internet access for clientele in most of southwest America.

Reason: To protest Cox Communications' attempted regulation of customer's data usage quota.

OPERATION BLACKOUT (USA):

Action: In November, Anonymous threatened action against the US government.

Reason: To protest against the Stop Online Piracy Act.

STRATFOR (worldwide):

Action: STRATFOR is a US company that provides services to intelligence and law enforcement agencies, among others. 200 gigabytes of data were stolen from STRATFOR's web servers and subsequently published. The stolen information included active credit cards, e-mail addresses, phone numbers, encrypted passwords and sensitive information from clients (including governments and military departments). Anonymous planned to donate to charities using the stolen credit card information.

Reason: Following the HB Gary incident, Anonymous began to investigate what it refers to as a "state-corporate alliance against the free information movement." Due to STRATFOR's ties with the intelligence and military contracting sectors and government agencies, Anonymous believed that

targeting STRATFOR would "improve [their] ability to continue this investigation and thereby bring to light other instances of [perceived] corruption, crime and deception on the part of certain powerful actors based in the U.S. and elsewhere.[16]"

Ongoing:

OPERATION ANTISEC (NATO, Tunisia, Brazil, Australia, USA, Turkey, UK, and other countries):

Action: In USA: DDoS attacks against the Central Intelligence Agency's (CIA) website; the US Senate website was hacked, and information about its internal server structure was released. In UK: DDoS attacks against the Serious Organised Crime Agency's (SOCA) website.

Reason: The declaration of cyber warfare on governments and corporations worldwide in response to perceived corruption and government censorship.

CANADA

Anonymous has directly and indirectly targeted the Government of Canada, Canada's municipal governments and Canadian private corporations.

Government of Canada:

STRATFOR (December 2011):

The federal government has been an indirect target of anonymous activity in connection with STRATFOR. STRATFOR is a resource used by various federal departments. When usernames and passwords were released by Anonymous, some of them included those of federal employees[17].

Municipal Governments:

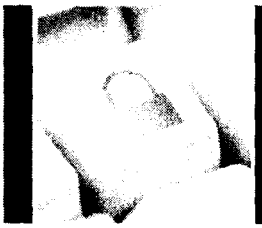
TORONTO (November 2011):

Anonymous threatened to take down the City of Toronto's website if officials evicted protestors from the Occupy Toronto camp. Although no known activity was conducted against the City of Toronto's website, the Toronto Police Service website was hacked and several usernames and passwords were stolen, possibly in retaliation to the continued efforts to evict the Occupy camp.

Private Corporations:

OPERATION GREEN RIGHTS/ PROJECT TARMAGGEDON:

In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline, and the Alberta Tar Sands project. Those targeted have included Canadian Oil Sands Ltd, Imperial Oil, Syncrude, and Suncor.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Future Activity

Although it is impossible to fully predict Anonymous' behaviour, based on prior targeting, there are a few government bills that would direct Anonymous' attention towards the Government of Canada. Copyright Modernization Act: As a part of this bill, ISPs would be responsible for sending notices from copyright holders to Internet users alleged to have participated in illicit downloading and file-sharing online. The ISPs would also be required to retain records which establish the identity of the subscriber and disclose it in court if necessary. (Comment: This could be seen by Anonymous as an attempt to limit consumer rights. Previous protests against government-issued copyright laws in Australia and the USA resulted in Anonymous launching DDoS attacks on Australian government websites and the US Copyright Office.)

Lawful Access Package:

The government's announcement to reintroduce Lawful Access legislation[18] that would require telecommunications companies, including ISPs to ensure intercept capabilities on their network. ISPs would also be required to disclose certain information on persons of interest to law enforcement authorities without a warrant under specific circumstances. (Comment: This could be seen by Anonymous as a violation of privacy. Similar perceptions have prompted Anonymous to take action against Facebook[19].)

TRADECRAFT

Anonymous has traditionally used basic, open-source-available cyber threat tradecraft against their targets. However, beginning in mid-2011, Anons have begun developing their own malware. (Comment: The exploits below do not represent a conclusive list because Anonymous includes a large number of members and all of their activities cannot be tracked and attributed to Anonymous.)

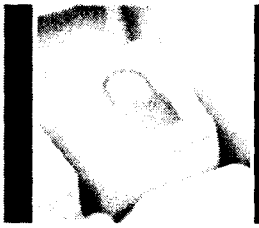
Open Source resources:

DoS/DDoS:

Anonymous' usual method of choice is to launch DoS/DDoS attacks against a target's website in an effort to bring the network offline and to make the website unavailable to legitimate users. Two commonly used methods include:

1) LOIC:

Anons are encouraged to download and launch the Low Orbit Ion Cannon application enabling them to willingly participate in a botnet. The LOIC is pointed at a target of choice, which would then disrupt the service of the victim's host. However, since LOIC could reveal the IP addresses of its users, it's traceability has prompted Anonymous to find other means of attacks.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

2) Apache Killer:

The Apache DoS tool nicknamed the "Apache Killer" exploits a vulnerability which allows remote attackers to send requests to servers via a malformed uniform resource identifier (URI)[20]. It is designed to drain the web server's memory, which would then take the website offline. It also allows a remote attacker to use a single computer to wage DoS attacks against an Apache server.

Anonymous-developed tools:

DoS/DDoS via SQL Injections:

#RefRef:

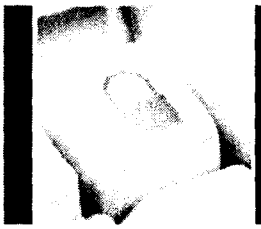
Anonymous developed and released a Perl DDoS tool in September, #RefRef, that exploits SQL[21] vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline. #RefRef could be used in combination with tools such as Havij, an SQL Injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities. As a result of SQL vulnerability exploitation, database content could be changed, or database information (such as credit card information or passwords) could be stolen.

Guy Fawkes virus:

Malware development is also something that Anonymous members have been focusing on. The Guy Fawkes[22] virus was developed by Anon to take control of a Facebook account and use it to spread malware to other members without the users actually logging onto the site. According to security analysts at the antivirus software company BitDefender, the Guy Fawkes virus (which they have named Backdoor-Bifrose-AAJX) has the ability to inject itself in the Internet Explorer process, providing a remote attacker with unhindered access to the compromised system. It would also record keystrokes and disrupt processes of known antimalware software. (Comment: Although the Guy Fawkes virus was previously believed to be responsible for the massive pornographic spam attack against Facebook in November 2011, this was later refuted by Facebook and BitDefender. Anonymous has stated that it is still working to control the virus to be used at a later date.)

Other:

Other techniques used by Anonymous include using social engineering techniques to gain access to victims' systems (e.g. HB Gary Federal), using web defacement to post embarrassing messages on victims' websites, using password cracking to exfiltrate data from a victim's database, and using a Twitter raiding tool called Universal Rapid Gamma Emitter (URGE) to hijack Twitter trending topics into topics of interest to Anonymous. It also allows Anons to tweet messages within the topics.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

MITIGATION

Since Anonymous has a wide range of targets, it is difficult to measure which vulnerabilities are most frequently exploited by the group. However, as noted, the threats leveraged are generally limited to open source or well-known vulnerabilities. As a result, strong IT security practices will go a long way to defending against an Anonymous cyber threat. Implementing CCIRC's mitigation guidelines for advanced persistent threats and DDoS attacks is also recommended[23]. In addition, the following mitigation is available for some of the tradecraft[24] specifically noted above:

1. DoS/DDoS attacks.

a)Use network segmentation and segregation into security zones to protect high value assets using routers to spot and drop DDoS connections.

b)If the DDoS is pointed at a specific IP, the target site could be blackholed. This typically requires working with upstream network providers to forward malicious traffic to a non-existent network interface, where the offending traffic will be dropped.

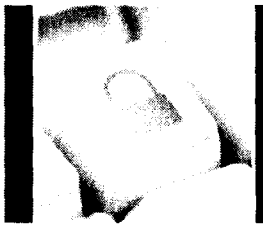
b) In some cases, if a DDoS is anticipated, it may be possible to temporarily have additional bandwidth provisioned to your network. This will lessen the impact on the target for some DDoS incidents.

2. "Apache Killer."

a) Apache has since released patches to fix this vulnerability. All users are recommended to upgrade to Apache 2.2.20 or higher.

3. "#RefRef."

a) Webcode should be hardened[25] against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

1 IRC is a protocol for Internet text messaging and synchronous conferencing. It allows group communications as well as private messaging and file sharing.

2 A denial-of-service (DoS) or a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.

3 SQL injection is often used to attack the security of a website by injecting SQL commands into the database of an application to change the database content or to dump database information to the attacker.

4 Zero-day threats attempt to exploit new computer application vulnerabilities not yet known to the software developer or the general public.

5 Anon-ops provides communications for Anonymous' announcements.

6 LulzSec was a small team that joined forces with Anonymous in the ongoing "Operation Anti-Security" or "AntiSec" campaign, which later disbanded in the summer of 2011.

7 LulzRaft was inspired by LulzSec group and has been responsible for web defacement of the website for the Conservative Party of Canada and for accessing private information about the party's donors. They have also been linked to web defacement of the website of Calgary-based energy company, Husky Energy.

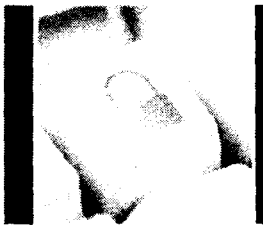
8 Unofficial spokespeople for Anonymous include Jake Davis (also known by his online nickname "Topiary,") Barrett Brown, etc. For more information on Jake Davis, please see http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-ukpolice/. For more information on Barrett Brown, please see http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx.

9 According to open source, LOIC is an open source network stress testing application which performs DoS or DDoS attacks on a target site by flooding the server with TCP or UDP packets to disrupt the service of a host.

10 HBGary Federal is a technology security company who was working with the FBI to unmask members of Anonymous. In February 2011, the CEO Aaron Barr revealed an intention to release information on the identities of Anonymous members. As a result, Anonymous members compromised the HBGary website, stole and publicly released the company's documents and emails.

11 According to open source, the Occupy movement refers to an international protest movement directed against high unemployment, social and economic inequality and perceived corruption in corporations and government.

12 For more information, please refer to http://www.pcmag.com/article2/0,2817,2383018,88.asp.



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

13 The Arab Spring refers to revolutionary protests occurring in the Arab world beginning in December 2010. Countries affected include Tunisia, Egypt, Libya, Bahrain, Syria, Yemen, Algeria, Iraq, Jordan, Kuwait, Morocco, Oman, Lebanon and Saudi Arabia.

14 The Pirate Bay is a Swedish website known for facilitating illegal downloads and supporting the international anti-copyright movement.

15 The Stop Online Piracy Act is proposed US legislation to combat against the online distribution of copyrighted intellectual property. This has been viewed by Anonymous as an attempt to censor the Internet.

16 For the full explanation, please refer to Barret Brown's statement at http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-hacked.

17 CTEC has provided mitigation to employees of the affected departments.

18 This legislation will be similar to the previous Bill C-50, Bill C-51 and Bill C-52.

19 Operation Facebook was launched on November 5th, 2011 because Anonymous believes that "Facebook is the opposite of the Antisec cause."

20 For more information, please refer to CVE-2011-3192 at http://nvd.nist.gov/.

21 An SQL server is a relational database server that can store and retrieve data across a network (e.g. the Internet). Queries from client machines are formatted in the SQL language.

22 Guy Fawkes was associated with the Gunpowder Plot, a failed assassination attempt against King James I of England in 1605. The conspirators' plan was to blow up the Houses of Parliament in order to kill the King and the Members of Parliament. Coincidentally, Anons have adopted the easily available and inexpensive Guy Fawkes mask as their symbol.

23 [http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx] + [DDoS hyperlink when finished]

24 Security analysts are still undergoing analysis on the Guy Fawkes virus; as such, we are unable to provide mitigation at this time. In addition, since URGE is not a hacking tool, there does not appear to be any mitigation actions provided at this time.

25 Hardening minimises access between the public facing HTTP server and the SQL database. It also validates requests sent by external clients to the HTTP server.

CYBERDO

From: "Aubé, Stéphan" <stephan.aube@parl.gc.ca>
Sent: February-17-12 1:25 PM
To: CYBERDO; Beaudoin, Luc
Subject: Re: [Activity 3497] RE: DDOS s.16(1)(b) s.16(2)(c)

Thank you Bruce !

Stephan

----- Original Message -----
From: CYBERDO [mailto
Sent: Friday, February 17, 2012 01:20 PM
To: Aubé, Stéphan; Beaudoin, Luc <LucS.Beaudoin@ps-sp.gc.ca>
Cc: CYBERDO
Subject: [Activity 3497] RE: DDOS

Good Afternoon

We have forwarded your report to CTEC, who is the Federal CIRT. There are aware of this activity and assisting in a coordinated response.

Thanks for providing this information to CCIRC.

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

-----Original Message-----
From: [mailto
Sent: February-17-12 1:10 PM
To: stephan.aube@parl.gc.ca; Beaudoin, Luc; CYBERDO
Subject: RE: DDOS
Importance: High

Hi All,

As you may be aware, is currently under an Anonymous DDoS attack, see below.

Stef is the IT director and I think he can benefit from your assistance in mitigating this DDoS attack.

He can share with you current activities that took place.

Good luck!

Stéphan Aubé
Dir. Opérations des TI, Chambre des communes Dir. IT Operations, House of Commons 181, Queen, bureau-room 6-028, Ottawa, Ontario, Canada K1A 0A6
Tel.: (613)992-7449 - Fax: 613-947-6292 - E-Mail : aubes@parl.gc.ca

Regards,

[redacted]

s.16(1)(b)

[redacted]

From: [redacted]
Sent: February-17-12 11:58 AM
To: 'saube@parl.gc.ca'
Subject: STEF: Anonymous - attack to site (je pense)
Importance: High

To site est down, probablement a cause de Anonymous, un DDoS (Distributed denial service attack)

Poste aujourdhui.

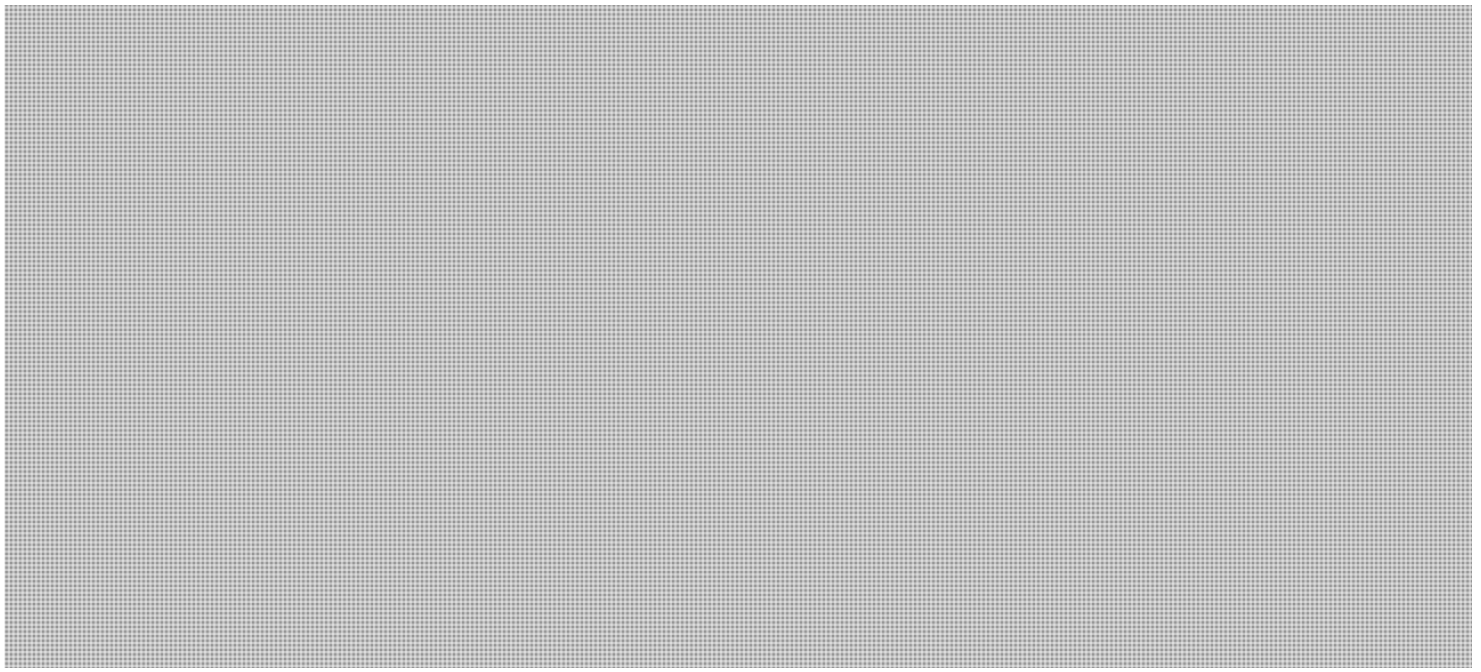
s.16(1)(b)
s.16(2)(c)

Le booster est [redacted]

[redacted]

[redacted]

[redacted]



s.16(1)(b)
s.16(2)(c)

From: stephan.aube@parl.gc.ca [mailto:stephan.aube@parl.gc.ca]
Sent: February-17-12 1:07 PM
To:
Subject: DDOS

Tel que discute !

Stéphan Aubé
Dir. Opérations des TI, Chambre des communes Dir. IT Operations, House of Commons 181, Queen, bureau-room 6-028, Ottawa, Ontario, Canada K1A 0A6
Tel.: (613)992-7449 - Fax: 613-947-6292 - E-Mail : aubes@parl.gc.ca

Page 2157

is a duplicate

est un duplicata

Page 2158

is a duplicate

est un duplicata

Page 2159

is a duplicate

est un duplicata

Page 2160

is a duplicate

est un duplicata

CYBERDO

From: Beaudoin, Luc
Sent: February-15-12 8:03 PM
To: CYBERDO
Subject: Anon threat to dns root 31-3

s.16(2)(c)

More on Anon threat to dns root 31-3

http://www.circleid.com/posts/20120215_anonymous_plans_to_go_after_dns_root_servers/

http://pastebin.com/

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

Dvorkin, Corey

From: Barr, Corri <Corri.Barr@tbs-sct.gc.ca>
Sent: February-15-12 4:04 PM
To: Dvorkin, Corey
Subject: Tweet from @HannahThibedeau

@HannahThibedeau: VicToews attacked by anonymous Twitter account http://soc.li/8m6BUYE #cdnpoli

CYBERDO

From: Dick, Robert
Sent: February-15-12 8:00 PM
To: Anderson, Windy; Moore, Bruce
Subject: Fw: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Further to previous email.

From: Swift, Andrew
Sent: Wednesday, February 15, 2012 07:58 PM
To: Durand, Stéphanie; Dick, Robert
Subject: Re: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Thanks Stephanie. FYI:

-AANDC contacted CSE late this afternoon about a call from Aboriginal Peoples Television Network about whether AANDC is prepared for cyber attacks now that ANONYMOUS has expressed interest in aboriginal issues (according to the reporter)

-AANDC had prepared media lines that heavily referenced CSE and were not consistent w/ previous messages on threats to GC (see below)

-I spoke to MO and PCO who agreed that standard lines about not speaking to threats, cyber strategy in place, pillar of securing govt systems, etc should be provided to AANDC for them to use

-Felt it was better for AANDC to answer instead of redirecting to another dept to speak about a hypothetical threat

-I passed along the lines to AANDC and our PCO analyst was going to confirm w/ AANDC's to make sure all were clear

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

From: Durand, Stéphanie
Sent: Wednesday, February 15, 2012 07:49 PM
To: Dick, Robert; Swift, Andrew
Subject: Re: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Thanks.
Andrew: see below.

From: Dick, Robert
Sent: Wednesday, February 15, 2012 07:16 PM
To: Durand, Stéphanie

Subject: Fw: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Info

From: CYBERDO
Sent: Wednesday, February 15, 2012 06:35 PM
To: Anderson, Windy; Dick, Robert
Cc: GOC-COG; CYBERDO; Beaudoin, Luc; Champoux, Martin
Subject: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Windy/Robert for your situational awareness;

At 17:15 EST 15 Feb 2012, the GOC received a call from AADNC, Senior Communications Officer, Isabelle Duguay (819-997-3544) with the following queries:

AADNC has been receiving calls from a Journalist for information on potential hacking of AADNC by the group Anonymous.

A response was provided to AADNC a short time ago by Andrew Swift (Public Safety Affairs). (I'm not sure what the response was however apparently AADNC is satisfied.)

See additional comments below from AADNC Senior Communications Officer:

CONTEXT: We have developed the response in collaboration with our departmental CIO and called to give a heads-up to CSEC that we were directing potential media questions to them.
CSEC told us that sometimes, in such cases, Public Safety would take the lead.
journalist's deadline is today.

Here is the question AADNC received:
Jorge Barrera, Web Journalist, APTN - Hacking group Anonymous is picking up the indigenous cause... Is the Dept prepared to deal with hacking attacks? Are we aware of potential threats?

and here's AADNC proposed response:

- AANDC is aware of the current threat concerning the Anonymous group.
- AANDC manages the risk of security breaches through a layered perimeter defense implementation and through coordinated communications with the Communication Security Establishment Canada (CSEC).
- CSEC is the technical lead for information technology security to safeguard Government of Canada electronic information.
- For more information on technology security at the Government of Canada, please contact CSEC Media Relations Office at 613-991-7248.

Thank you!

Bruce Moore
Public Safety Canada
CCIRC
Cyber Duty Officer

s.16(2)(c)

CYBERDO

From: Dick, Robert
Sent: February-15-12 7:53 PM
To: Anderson, Windy
Cc: Moore, Bruce
Subject: Fw: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Just so you know I've passed it along to ensure all loops closed. Thanks for this.

From: Durand, Stéphanie
Sent: Wednesday, February 15, 2012 07:49 PM
To: Dick, Robert; Swift, Andrew
Subject: Re: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Thanks.
Andrew: see below.

From: Dick, Robert
Sent: Wednesday, February 15, 2012 07:16 PM
To: Durand, Stéphanie
Subject: Fw: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Info

From: CYBERDO
Sent: Wednesday, February 15, 2012 06:35 PM
To: Anderson, Windy; Dick, Robert
Cc: GOC-COG; CYBERDO; Beaudoin, Luc; Champoux, Martin
Subject: [CCIRC Activity 3490] RE: Questions from AADNC re Media Inquiry Anonymous

Windy/Robert for your situational awareness;

At 17:15 EST 15 Feb 2012, the GOC received a call from AADNC, Senior Communications Officer, Isabelle Duguay (819-997-3544) with the following queries:

AADNC has been receiving calls from a Journalist for information on potential hacking of AADNC by the group Anonymous.

A response was provided to AADNC a short time ago by Andrew Swift (Public Safety Affairs). (I'm not sure what the response was however apparently AADNC is satisfied.)

See additional comments below from AADNC Senior Communications Officer:

CONTEXT: We have developed the response in collaboration with our departmental CIO and called to give a heads-up to CSEC that we were directing potential media questions to them.
CSEC told us that sometimes, in such cases, Public Safety would take the lead.
journalist's deadline is today.

Here is the question AADNC received:
Jorge Barrera, Web Journalist, APTN - Hacking group Anonymous is picking up the indigenous cause... Is the Dept prepared to deal with hacking attacks? Are we aware of potential threats?

and here's AADNC proposed response:

- AANDC is aware of the current threat concerning the Anonymous group.
- AANDC manages the risk of security breaches through a layered perimeter defense implementation and through coordinated communications with the Communication Security Establishment Canada (CSEC).
- CSEC is the technical lead for information technology security to safeguard Government of Canada electronic information.
- For more information on technology security at the Government of Canada, please contact CSEC Media Relations Office at 613-991-7248.

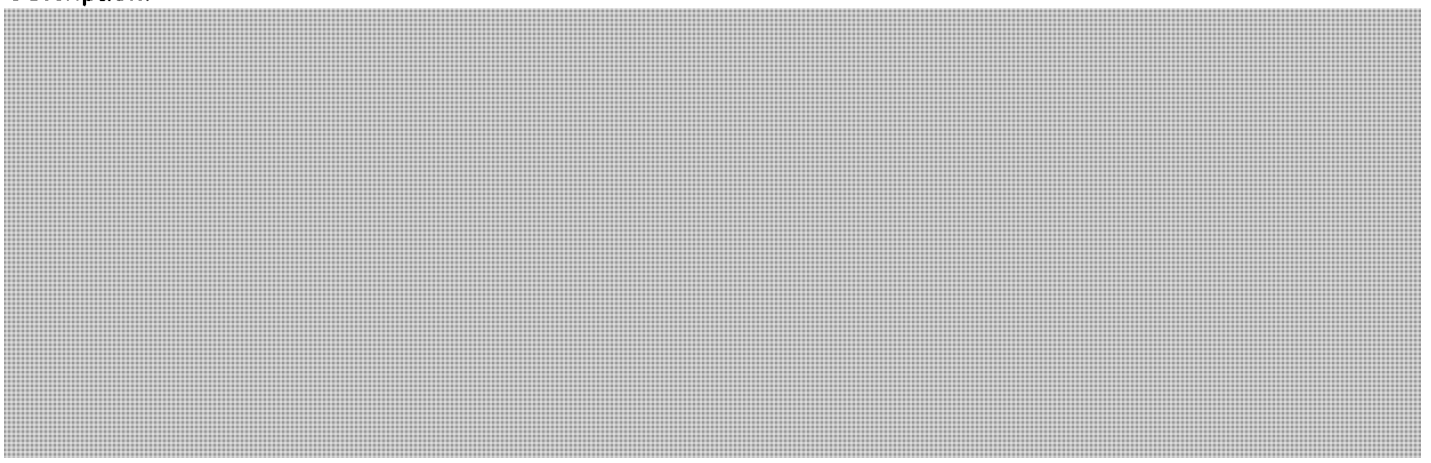
Thank you!

Bruce Moore
Public Safety Canada
CCIRC
Cyber Duty Officer s.16(2)(c)

CYBERDO

From: Bendelier, Kenneth
Sent: February-15-12 7:08 AM
To: CYBERDO; 'DARREN.GAUTHIER@forces.gc.ca'; ANDREW.CHERNYSH@forces.gc.ca
Cc: Beaudoin, Luc
Subject: This may be of interest

Description:



s.15(1) - Int'l
s.16(2)(c)

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-993-5042
Facsimile | Télécopieur +1 613-954-3097
Kenneth.Bendelier@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

CYBERDO

From: [redacted] on behalf of [redacted]cymru.com>
Sent: February-15-12 4:21 AM
To: [redacted]
Subject: [redacted] [DNB] Anonymous Takes Down NASDAQ Site with DDOS Attack

Title: Anonymous Takes Down NASDAQ Site with DDOS Attack
Author: Eduard Kovacs
Source: Softpedia
Date Published: 15th February 2012

Excerpt:

'....A group of Anonymous hackers launched a distributed denial of service (DDOS) attack against the official website of the NASDAQ stock market as a form of support for the "99 percent.".....'

To read the complete article see:
http://news.softpedia.com/news/Anonymous-Takes-Down-NASDAQ-Site-with-DDOS-Attack-252858.shtml

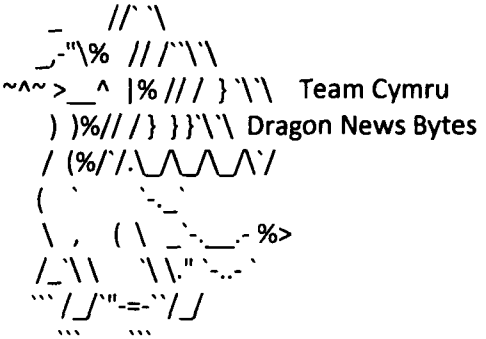
The opinions expressed in the posted news items do not necessarily reflect the views of Team Cymru.

The appearance of hyperlinks does not constitute endorsement by Team Cymru of an external Web site, or any commercial company, information, products or services contained therein.

Dragon News Bytes is a Private and Restricted mailing list.

The information transmitted is intended only for the person or entity to which it is addressed and any retransmission or dissemination outside of your company is prohibited.

To subscribe to this mailing list, please signup at:
https://lists.cymru.com/mailman/listinfo/ians_dragon_newsbytes
and then send an email to: outreach@cymru.com providing some personal background and two references.



For more Security News see:
www.team-cymru.org/News
www.team-cymru.org/News/secnews.rss
http://twitter.com/teamcymru

There are many way to keep up with what Team Cymru are doing:
* Join our announce list via cymru-announce-subscribe@cymru.com
* Join our printed newsletter list via quarterly@cymru.com
* See what we see, www.team-cymru.org/Monitoring/Graphs
* Cool stuff you can use: www.team-cymru.org/Services/
* Team Cymru's YouTube Channel: www.youtube.com/teamcymru

s.19(1)
s.20(1)(c)

[redacted]
Security Evangelist
Team Cymru
http://www.team-cymru.org/About/contact.html

'To communicate simply you must understand profoundly'

[redacted]

[redacted]

Dvorkin, Corey

From: Bradley, Kees
Sent: February-17-12 8:42 AM
To: Dvorkin, Corey
Subject: FW: RFI - CCIRC Activity 3484: Inquiry - "Operation Global Blackout"

From: Schramm, Kent
Sent: February-15-12 2:44 PM
To: Bradley, Kees
Subject: FW: RFI - CCIRC Activity 3484: Inquiry - "Operation Global Blackout"

K.K. (Kent) Schramm, CD
Manager Operational Concepts / Gestionnaire, Concepts Opérationnel
National Cyber Security Directorate / Direction générale de la cybersécurité nationale
Public Safety Canada / Sécurité Publique Canada
340 Laurier Avenue West / 340, avenue Laurier Ouest
Ottawa, Ontario, K1A OP8
Tel: (613) 949-7377

From: DARREN.GAUTHIER@forces.gc.ca [mailto:DARREN.GAUTHIER@forces.gc.ca]
Sent: February-15-12 2:04 PM
To: Schramm, Kent
Subject: FW: RFI - CCIRC Activity 3484: Inquiry - "Operation Global Blackout"

Darren T. Gauthier
A/Team Lead
Computer Network Intelligence
Chief Defence Intelligence | Chef du Renseignement de la défense
National Defence Headquarters | Quartier général de la Défense nationale
101 Colonel By Drive | 101 promenade Colonel By
Ottawa, ON, Canada K1A 0K2
Darren.Gauthier@forces.gc.ca
Telephone | Téléphone 613-945-5012
Facsimile | Télécopieur 613-945-7180
Government of Canada | Gouvernement du Canada

From: Scheurkogel NR@CDI DGIP@Ottawa-Hull
Sent: Wednesday, 15, February, 2012 12:59 PM
To: Hodgson PO1 ER@CDI DGIP@Ottawa-Hull

Cc: Gauthier DT@CDI DGIP@Ottawa-Hull
Subject: Fw: RFI - CCIRC Activity 3484: Inquiry - "Operation Global Blackout"

Interesting chatter from the telcos.

Sent from my wireless handheld device / Transmis de mon appareil portable

---

From: Bob.Leafloor@ic.gc.ca <Bob.Leafloor@ic.gc.ca>
To: [redacted]; Alain.Labossiere@ic.gc.ca <Alain.Labossiere@ic.gc.ca>; [redacted]@ic.gc.ca <[redacted]@ic.gc.ca>
Sent: Tue Feb 14 15:09:27 2012
Subject: RE: RFI - CCIRC Activity 3484: Inquiry - "Operation Global Blackout"

Interesting. The 13 servers are any-casted to probably 200 plus, CIRA would know the number, so it would need the mother of all bots, and no caching to be black, you would think>

Bob Leafloor
Mgr. Emergency Communications Technologies
Regulatory Policy and Planning
Radiocommunications and Broadcasting Regulatory Branch
Industry Canada 300 Slater St. Ottawa, Ontario K1A 0C8

Off. 613 990 4236 Cell [redacted] mailto:leafloor.bob@ic.gc.ca

-----Original Message-----
From: [redacted]
Sent: Tue 2012-02-14 2:54 PM
To: Labossière, Alain: DGEPS-DGGPN; Canadian TCP
Subject: RE: RFI - CCIRC Activity 3484: Inquiry - "Operation Global Blackout"

Fyi to you all that there is a web page called [redacted] that has been up for a while on this.

[redacted]

-----Original Message-----
From: Alain.Labossiere@ic.gc.ca [mailto:Alain.Labossiere@ic.gc.ca]
Sent: February 14, 2012 2:11 PM
To: [redacted]@ic.gc.ca
Subject: RFI - CCIRC Activity 3484: Inquiry - "Operation Global Blackout"
Importance: High

Bonjour / Good afternoon

CCIRC just sent this Request For Information (RFI) see below.

Please provide any evaluation/comment directly to this mailing list for discussion benefit.

If you believe a joint (Industry/Gov) conference call is necessary, we could set one up or we can have some discussion at the weekly CTCP call.

I have pasted a portion of the text below and here is the link:

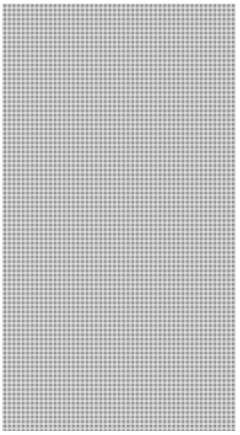
http://pastebin.com/[redacted]

Merci / Thank you !

al

****

To protest SOPA, Wallstreet, our irresponsible leaders and the beloved bankers who are starving the world for their own selfish needs out of sheer sadistic fun, On March 31, the Internet will go Black.
In order to shut the Internet down, one thing is to be done. Down the 13 root DNS servers of the Internet. Those servers are as follow:



s.16(2)(c)

-----Original Message-----

From: CYBERDO [mailto:
Sent: Tuesday, February 14, 2012 1:50 PM
To: Labossière, Alain: DGEPS-DGGPN
Cc: Beaudoin, Luc; CYBERDO
Subject: CCIRC Activity 3484: Inquiry - "Operation Global Blackout"
Importance: High

Good Afternoon Alain;

CCIRC noted a posting on pastebin purporting to be a call to arms from Anonymous to coordinate a reflective DOS attack against global DNS Root Severs on 31 March 2012.

Request CTCP members evaluate and provide comments back to IC and CCIRC.

Pastebin URL: http://pastebin.com/

Thanks

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

CYBERDO

From: Beaudoin, Luc
Sent: February-14-12 4:35 PM
To: CYBERDO
Subject: Re: CCIRC Activity 3484: Inquiry - "Operation Global Blackout"

Good call

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----
From: CYBERDO
Sent: Tuesday, February 14, 2012 01:50 PM
To: 'Alain.Labossiere@ic.gc.ca' <Alain.Labossiere@ic.gc.ca>
Cc: Beaudoin, Luc; CYBERDO
Subject: CCIRC Activity 3484: Inquiry - "Operation Global Blackout"

Good Afternoon Alain;

CCIRC noted a posting on pastebin purporting to be a call to arms from Anonymous to coordinate a reflective DOS attack against global DNS Root Severs on 31 March 2012.

Request [redacted] members evaluate and provide comments back to IC and CCIRC.

Pastebin URL: http://pastebin.com/[redacted] s.16(2)(c)

Thanks

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

CYBERDO

From: Alain.Labossiere@ic.gc.ca
Sent: February-14-12 2:11 PM
To: [redacted]@ic.gc.ca
Subject: RFI - CCIRC Activity 3484: Inquiry - "Operation Global Blackout"

Importance: High

Bonjour / Good afternoon

CCIRC just sent this Request For Information (RFI) see below.

Please provide any evaluation/comment directly to this mailing list for discussion benefit.

If you believe a joint (Industry/Gov) conference call is necessary, we could set one up or we can have some discussion at the weekly CTCP call.

I have pasted a portion of the text below and here is the link:

http://pastebin.com/[redacted]

Merci / Thank you !

al

s.16(2)(c)

****

To protest SOPA, Wallstreet, our irresponsible leaders and the beloved bankers who are starving the world for their own selfish needs out of sheer sadistic fun, On March 31, the Internet will go Black.
In order to shut the Internet down, one thing is to be done. Down the 13 root DNS servers of the Internet. Those servers are as follow:

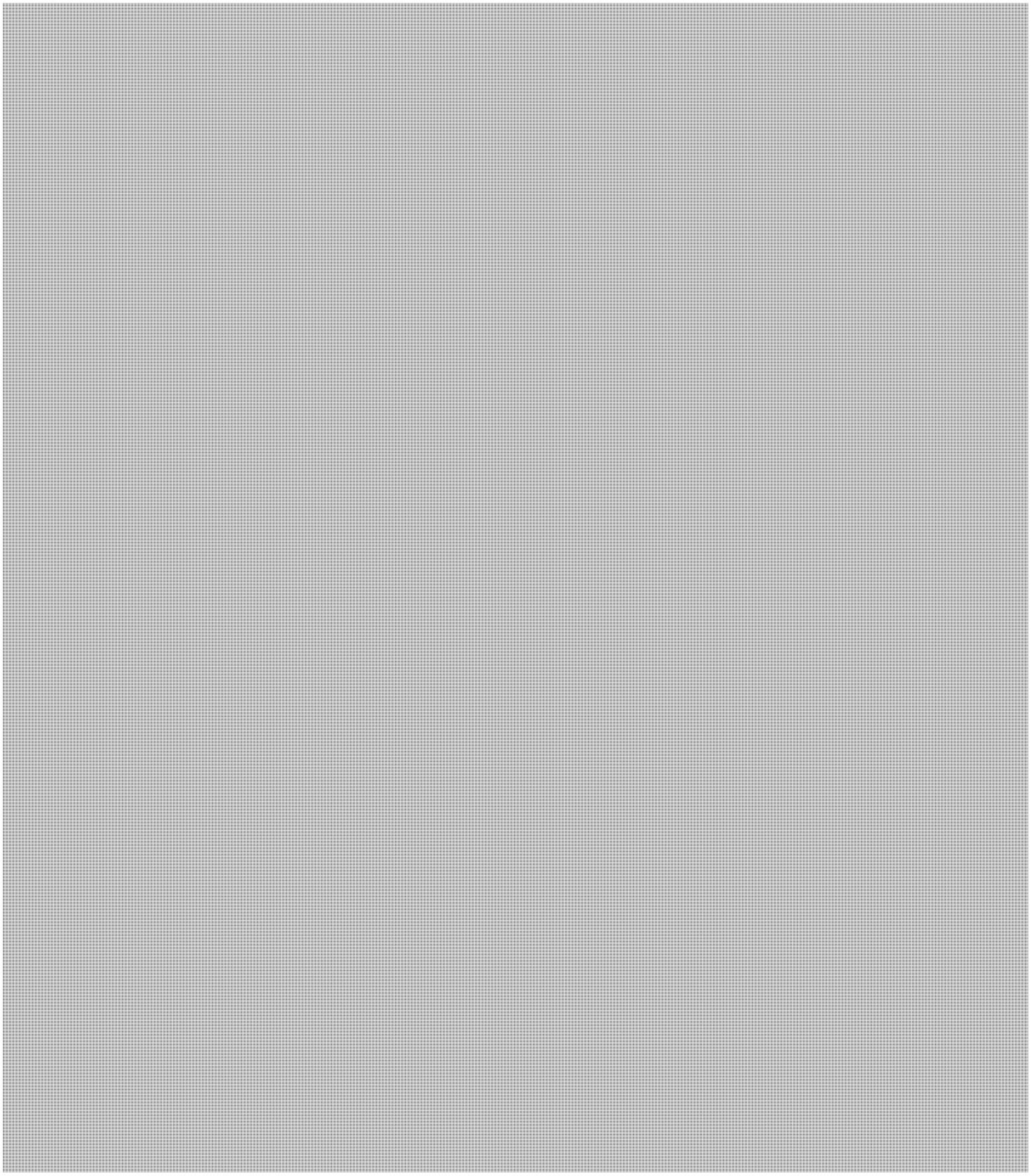
[redacted]

Proulx, Véronique

From: Pilon, Claude
Sent: March-27-12 4:24 PM
To: Proulx, Véronique
Cc: Bradley, Kees
Subject: RE: Another tasking from Robert with respect to his Parliament Meeting

Veronique, s.23

Voici une opinion préliminaire étant donné l'urgence de la requête. Si tu as des questions, n'hésite pas à me contacter.



Merci

s.23

Claude

Claude Pilon, B.Sc., LL.L, LL.B

Counsel / Avocat
Public Safety Canada Legal Services / Services juridiques de Sécurité publique Canada
(613) 991-4364 / claude.pilon@ps-sp.gc.ca
PROTECTED: SOLICITOR-CLIENT PRIVILEGE/PROTÉGÉ: PRIVILÉGE DU SECRET PROFESSIONNEL DE L'AVOCAT

Please feel free to reply in the official language of your choice/ N'hésitez pas à me répondre dans la langue officielle de votre choix

From: Proulx, Véronique
Sent: March-26-12 3:17 PM
To: Pilon, Claude
Subject: RE: Another tasking from Robert with respect to his Parliament Meeting

s.23

Bonjour Claude,

[redacted]

Un gros merci,
Véronique

Véronique Proulx
Canadian Cyber Incident Response Centre
Public Safety Canada
(613) 990-7102

From: Pilon, Claude
Sent: March-26-12 3:06 PM
To: Bradley, Kees; Proulx, Véronique
Cc: Dvorkin, Corey
Subject: RE: Another tasking from Robert with respect to his Parliament Meeting

Veronique,

[redacted]

Thanks

Claude

Claude Pilon, B.Sc., LL.L, LL.B
Counsel / Avocat
Public Safety Canada Legal Services / Services juridiques de Sécurité publique Canada
(613) 991-4364 / claude.pilon@ps-sp.gc.ca
PROTECTED: SOLICITOR-CLIENT PRIVILEGE/PROTÉGÉ: PRIVILÉGE DU SECRET PROFESSIONNEL DE L'AVOCAT

Please feel free to reply in the official language of your choice/ N'hésitez pas à me répondre dans la langue officielle de votre choix

From: Bradley, Kees
Sent: March-26-12 2:49 PM
To: Proulx, Véronique; Pilon, Claude
Cc: Dvorkin, Corey
Subject: RE: Another tasking from Robert with respect to his Parliament Meeting

[redacted]

Cheers,
Kees

From: Dvorkin, Corey
Sent: March-26-12 2:43 PM
To: Proulx, Véronique
Cc: Bradley, Kees
Subject: RE: Another tasking from Robert with respect to his Parliament Meeting

[redacted]

And I would like to see what is being prepped, and might be able to help shape it for Robert. So happy to help.

s.23

Corey Michael Dvorkin
Senior Strategist / Conseiller principale
Cyber Policy / Politiques cyber
National Cyber Security Directorate / Direction générale de la cybersécurité nationale
Public Safety Canada / Sécurité Publique Canada
340 Laurier Avenue West / 340, avenue Laurier Ouest
Ottawa, Ontario, K1A OP8
Tel: (613) 990-9608
corey.dvorkin@ps-sp.gc.ca

From: Proulx, Véronique
Sent: March-26-12 2:40 PM
To: Dvorkin, Corey
Subject: FW: Another tasking from Robert with respect to his Parliament Meeting

Hi Corey,

[redacted]

Any input you might have would be appreciated. I'm also happy to send you other documents I've been preparing that will be inserted into the briefing binder for Robert's Parliamentary Committee appearance.

Cheers,
Veronique

Véronique Proulx

Canadian Cyber Incident Response Centre
Public Safety Canada
(613) 990-7102

s.23

From: Proulx, Véronique
Sent: March-26-12 1:05 PM
To: Bendelier, Kenneth; Anderson, Windy
Cc: Klassen, Nathan
Subject: RE: Another tasking from Robert with respect to his Parliament Meeting

[redacted] I am reviewing it right now, and will circulate it for input, along with a number of other documents that will be inserted into the briefing binder. I'll make sure to include Corey when I send this out.

Thanks!
V.

From: Anderson, Windy
Sent: Monday, March 26, 2012 12:57 PM
To: Proulx, Véronique
Cc: Bendelier, Kenneth; Klassen, Nathan
Subject: Another tasking from Robert with respect to his Parliament Meeting

He wants Veronique to contact Corey (in Mark's group) and together they find out by talking to Justice/RCMP/whomever to find out what a DDOS attack is considered in the criminal code. What is the penalty. Is it there, etc.

Thanks.

Have a great day,

Windy

Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Dvorkin, Corey

From: Heather.Dryden@ic.gc.ca
Sent: March-28-12 7:10 PM
To: DGTPUsers@ic.gc.ca; David.Gibson@ic.gc.ca; Maggie.Smith@ic.gc.ca; Bob.Leafloor@ic.gc.ca; Colman.Ho@ic.gc.ca; Alain.Labossiere@ic.gc.ca
Cc: Grigsby, Alexandre; Dvorkin, Corey; Kathryn.Reynolds@ic.gc.ca
Subject: Root Server System Security / Anonymous
Attachments: 20120102 GAC RAB Root Server System.doc

Following media coverage of the "Anonymous" threats <http://www.bbc.co.uk/news/technology-17472447> , you might be interested in some information from an ICANN perspective (attached).
ICANN, as the global coordinator for Internet names and numbers tends to garner an undue amount of the focus when it comes to the Domain Name System (DNS). In this case, ICANN has a direct but narrow role stemming from its operation of the "L" root server. ICANN is in fact one of a decentralized range of operational Internet and private sector organizations (which includes the independent root server operators, where it does not have authority).

The Internet Corporation for Assigned Names and Numbers

2 March 2012

To: Heather Dryden
Chair, Governmental Advisory Council

From: Rod Beckstrom
President and Chief Executive Officer

Re: Root Server System Security

Dear Heather:

You may be aware that there has been a recent threat of a future attack against the root-server system purporting to originate from the group Anonymous.

ICANN takes all threats against DNS infrastructure seriously, as is consistent with our technical coordination role, our role as operator of the L Root server, and our mission to maintain the stable and secure operation of the Internet's unique identifier systems.

We are tracking the threat and collaborating with others in the industry and greater community to ensure we are prepared. These efforts are being led by Jeff Moss, ICANN"s Chief Security Officer.

We are writing to ask you, in your role as Chair of the GAC, if there is any advice or information that you or your members wish to share on this specific threat. If you have information concerning the threat, or if you have any questions, please contact Jeff Moss at jeffrey.moss@icann.org.

We will update you with relevant information as we receive it.

Sincerely,

Rod

cc: Jamie Hedlund, Vice President, Government Affairs

CYBERDO

From: CYBERDO
Sent: March-27-12 9:44 AM
To: [redacted]
Cc: CYBERDO; [redacted]
Subject: FW: CCIRC CE12-2682 [DDoS website hosted in Sweden]

s.15(1) - Int'l
s.16(2)(c)

Hello [redacted]

The Canadian Cyber Incident Response Centre (CCIRC) is requesting your assistance regarding the following website:

[redacted] (link broken to prevent accidental clicking)

As requested in the below email, dated 13 March, CCIRC sent a request to have the website removed. This website is being used to launch DDoS attacks against various websites, one of which was a Canadian website on 12 March 2012.

Any assistance your team is able to provide would be greatly appreciated.

Cyber Duty Officer / Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: [redacted] Fax: (613)991-3574
www.PublicSafety.gc.ca

From: CYBERDO
Sent: March-13-12 2:29 PM
To: [redacted]
Cc: [redacted] CYBERDO
Subject: CCIRC CE12-2682 [DDoS website hosted in Sweden]

Hello;

The Canadian Cyber Incident Response Centre (CCIRC) monitors the cyber threat environment around the clock and is responsible for coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents.

CCIRC has received a report regarding a website hosted in [redacted] which is connected with a Distributed Denial of Servivce (DDoS) campaign by the hacktivist group Anonymous.

Details:
[redacted] (link broken to prevent accidental clicking)

Currently, there is a link on [redacted] that has a link called [redacted] When this link is clicked on, it directs users to the [redacted]

Analysis of this webpage reveals [redacted]. When this [redacted] based page is opened, there is a default domain that has been chosen by Anonymous to be the target domain of the DDOS. The user is presented with the option of changing the target by entering any domain they choose. They can also specify the "Requests Per Second" (number of http requests it will DDOS the target domain with). The default requests per second is set to 1000.

This website was the launch point for a DDoS attack against a Canadian website on 12 March 2012.

CCIRC requests your assistance with having this website removed.

We have assigned event number CE12-2682 to this event, please use this number on any correspondence associated with this activity.

Please advise when corrective action has been taken. Thank you.

s.16(2)(c)

Cyber Duty Officer / Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: [redacted] Fax: (613)991-3574
www.PublicSafety.gc.ca

Dvorkin, Corey

From: Matz, Mark
Sent: March-23-12 8:39 PM
To: Grigsby, Alexandre; Dvorkin, Corey; Labelle, Alana; Mohammed, Melanie
Subject: Re: OPC request for a meeting

Alana, please coordinate with Alex schedule a time for us to meet with Chris Prince and also include Mel in the meeting.

Thanks! Mark

----- Original Message -----
From: Grigsby, Alexandre
Sent: Friday, March 23, 2012 02:05 PM
To: Dvorkin, Corey
Cc: Matz, Mark
Subject: OPC request for a meeting

I've run into Chris Prince from the Office of the Privacy Commissioner a few times at events in Ottawa and had a chat with him at the Cyber Dialogue. He also helped out in pulling together the privacy-related material for the London Conference briefs.

Apparently they've been doing some research cyber security-related stuff and want to have a general discussion. I don't really have any insights into what they want to talk about, but it might not hurt just to chat.

You free anytime between April 10 and 13?

Alexandre Grigsby
613.949.4243

-----Original Message-----
From: Christopher Prince [mailto:Christopher.Prince@priv.gc.ca]
Sent: March-21-12 11:13 AM
To: Grigsby, Alexandre
Cc: Nicholas Koutros
Subject: follow-up

Great to see you the other day, Alex. s.19(1)

Here's a link to an interview on CBC Spark with the McGill professor I mentioned - http://www.cbc.ca/spark/2012/03/spark-176-march-18-21-2012/ (with Gabriella Coleman, the Wolfe Chair in Scientific and Technological Literacy at McGill and a leading authority on the anthropology of digital media, hackers and the law. She's currently working on a book on Anonymous and digital activism. (Runs 18:47)

And here's Coleman's best work on the issue - http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action / http://canopycanopycanopy.com/15/our_weirdness_is_free.

[redacted] Anyway, do you think you and some folks over there might want to

come over for the talk and to have a general discussion? Just at the working level I mean (like up and a couple of your peers in Policy). We met with Robert Gordon and Robert Dick about a year ago on the cyber strategy and we did say we'd try to share ideas where it made sense - this to me seems like one of those issues ...

Anyway, let me know if there's any interest. The best time for us would be April 10-13. As I was mentioning in TO, we're working on a lot of Parliamentary issues between now and then but the MPs are off for Easter Break mid-April.

Chris

Chris Prince
Strategic Policy Analyst
Office of the Privacy Commissioner of Canada
112 Kent Street, 3rd Floor
Ottawa, Ontario
K1A 1H3
(613) 947-7005

Dvorkin, Corey

From: Bonvie, Jeff
Sent: March-22-12 11:16 AM
To: Bradley, Kees; Grigsby, Alexandre; Dvorkin, Corey
Subject: If you didn't see it yesterday...

http://arstechnica.com/tech-policy/news/2012/03/anonymous-reincarnates-the-lulzsec-name-for-new-campaign-of-hacks-and-attacks.ars

CYBERDO

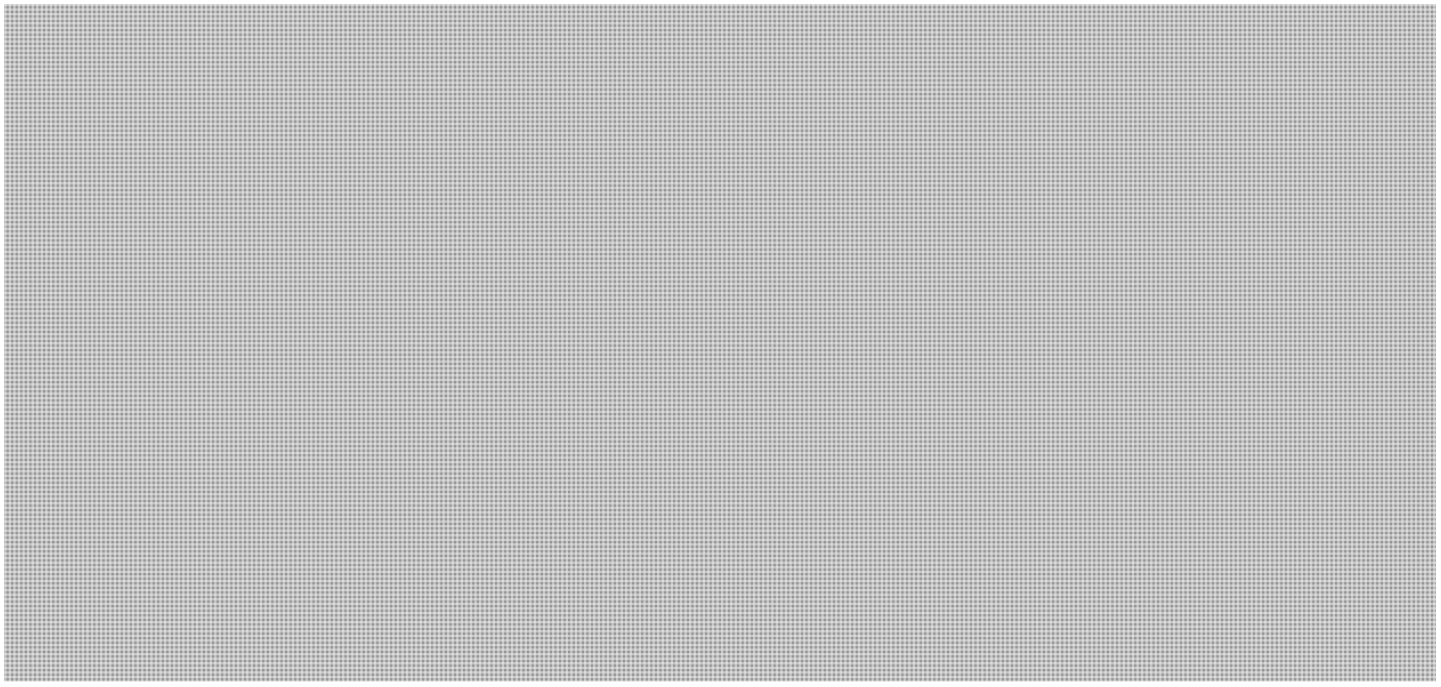
From: Bendelier, Kenneth
Sent: March-23-12 3:11 PM
To: Beaudoin, Luc
Cc: CYBERDO
Subject: Fw: Critical: Northrop Grumman (SSES) contract dump

Importance: High

DND might be interested.....

----- Original Message -----
From: E-Secure-IT [mailto:alert@e-secure-it.com]
Sent: Friday, March 23, 2012 03:10 PM
To: Bendelier, Kenneth
Subject: Critical: Northrop Grumman (SSES) contract dump

Generated by your Alert Subscription on Folder:
- Government US
- Major Site Security Breaches - Hack / DDos Attacks
- Anonymous
Source: pastebin
Complete item: http://pastebin.com/CZ4iLzH2



E-Secure-IT
https://www.e-secure-it.com

s.19(1)

Pages 2188 to / à 2190

are withheld pursuant to section

sont retenues en vertu de l'article

21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

CYBERDO

From: Matsuno, Akira
Sent: March-13-12 2:21 PM
To: CYBERDO
Cc: Clow, Patrick
Subject: CE12-2682

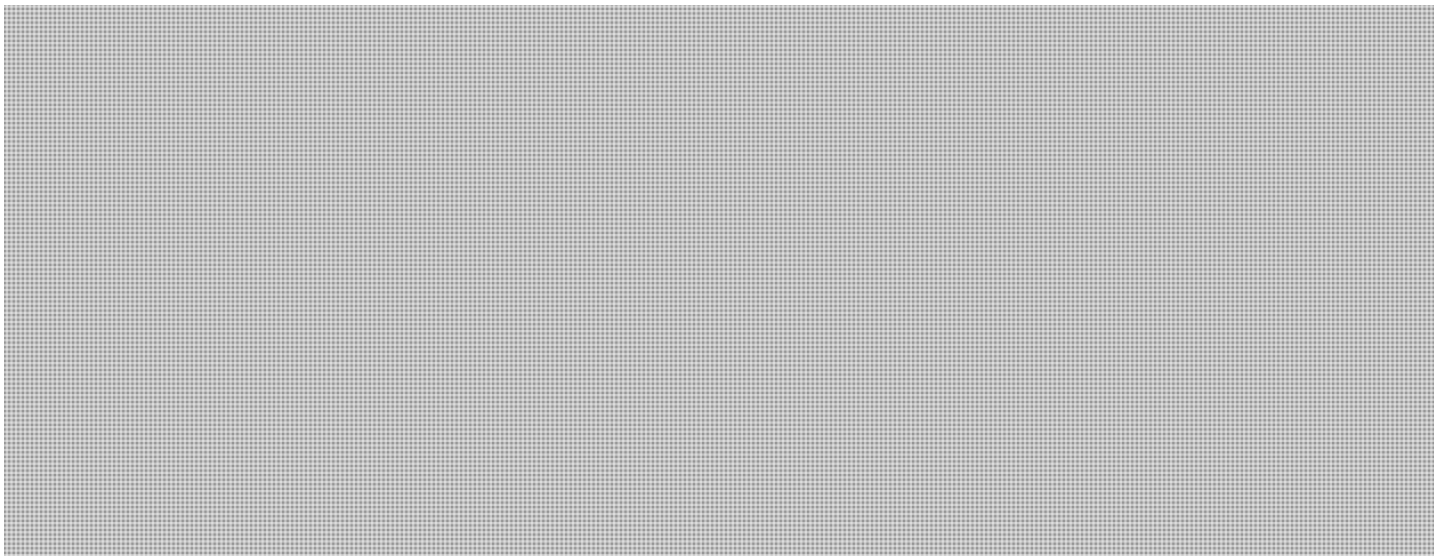
s.16(2)(c)

Hi Sandra,

I've done the analysis on the website. I'll submit these notes into the TAR as well:

The link [redacted] is a site controlled by the Hacktivist group, Anonymous. Currently, there is a link on [redacted] that has a link called "Join The Attack". When this link is clicked on, it directs users to the pastehtml(dot)com/view/bqossnqhx.html webpage.

Analysis of this webpage reveals [redacted]. See attached rtf file for complete code dump. When this [redacted] based page is opened, there is a default domain that has been chosen by Anonymous to be the target domain of the DDOS. The user is presented with the option of changing the target by entering any domain they wish. They can also specify the "Requests Per Second" (number of http requests it will DDOS the target domain with). The default requests per second is set to 1000.



This code is very portable, and could show up in other domains as well in the future, meaning that Anonymous could easily just host this script on another domain under their control.

Let me know if you require anything else.

Thanks!
Akira

Akira Matsuno, CISSP, GREM
Technical Analyst

Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613) 991-7783 Fax: (613) 991-3574
Cell: (613) [redacted]
Akira.Matsuno@ps-sp.gc.ca
publicsafety.gc.ca
Government of Canada

s.19(1)

IN12-501-Overview of the Hacktivist Group Anonymous
La version française suit

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
INFORMATION NOTE
****

Number: IN12-501
Date: 1 March 2012

****
Overview of the Hacktivist Group "Anonymous"
****

PURPOSE

The purpose of this report is to provide an overview of the hacktivist group "Anonymous." It contains information on its organizational structure, tradecraft and targets; the threat to Canadian Critical Infrastructure systems; and recommended mitigation.

ASSESSMENT

EXECUTIVE SUMMARY

Anonymous targets governments, private firms and individuals whose activities or purposes appear to be in conflict with principles espoused by the group. These principles mainly focus on: civil rights (e.g. oppressive regimes); information accessibility (e.g. Internet censorship); and other causes associated with perceived social injustice.

Based on a view of previous targeting by Anonymous, Canadian critical infrastructure systems could be targeted due to government legislative and regulatory initiatives (e.g. the Copyright Modernization Act) and initiatives that may result in activist opposition (e.g. environmental or social issues).

Anonymous uses a number of capabilities against its targets. These include, but are not limited to, distributed denial-of-service attacks (DDoS)(2), password cracking, SQL injections(3) and malware (virus) deployments. Canadian organizations have been both direct and indirect targets of Anonymous activity. For example, the Toronto Police Service website was hacked in 2011, likely in response to the "Occupy Toronto" camp evictions; Canadian corporations involved with the Alberta Tar Sands have been targeted, in particular to protest against the Keystone XL pipeline; and subsequent to a late-2011 breach of STRATFOR, a US corporation with links to intelligence and law enforcement organizations, credentials used by Canadian organizations to access STRATFOR databases were published. Although Anonymous leverages a variety of tradecraft to achieve its aims, strong IT security practices will help to defend against Anonymous exploits. The majority of these exploits are not leveraging zero-day(4).

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their agendas. Most notably, "Anonymous" is a term that refers to a group of

activist hackers, or hacktivists, that poses a wide range of cyber threats to government and commercial organizations around the world. Anonymous' agenda has included initiating cyber threat activities in protest of perceived government-mandated Internet censorship and in support of worldwide activist movements.

STRUCTURE

Anonymous is loosely composed of sub-groups (e.g. Anon-ops5, LulzSec6) and often conducts joint campaigns with other hacktivist groups in support of the same agenda. For example, TeaMpOisoN and People's Liberation Front are separate hacktivist groups with the freedom to opt-in or opt-out of projects conducted jointly with Anonymous. The Anonymous movement has also inspired copycat actions from other hacktivist groups, such as LulzRaft7.

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several unofficial spokespeople(8), Anonymous does not officially have a specific spokesperson. The only requirement for members of Anonymous (known as "Anons") is that they must always remain anonymous while participating in cyber campaigns supporting Anonymous' efforts. In many cases, Anons voluntarily join a botnet by downloading and installing the Low Orbit Ion Cannon (LOIC)(9) onto their computers. (Comment: The absence of a defined leadership structure is possibly why some threats associated with Anonymous are carried out, whereas others become empty threats if general consensus of a target was not agreed upon by the group at large.)

CHOOSING TARGETS

Since Anonymous is decentralized, new targets are determined in a variety of ways. Some of the most commonly used and documented methods of selecting targets are listed below.

- Through consensus among Anons using online polls. Following a discussion on an IRC, an online poll will be conducted to determine the target(s) of DoS/DDoS attacks. Although it appears to be a democratic process, elite Anons who are IRC channel operators are the ones who make the final decision about where to direct the LOIC attacks.
- As a response to perceptions of direct or indirect provocation by governments, by other hacking groups or companies (e.g. HBGary(10)), against the group as a whole, or against the principles to which Anonymous adheres.
- By exposing poor security practices. For instance, Anonymous members may use "Google Hacking" to identify vulnerable targets of opportunity. Results of such reconnaissance activities are often posted ans shared using sites such as pastebin.com .

These targeting practices are generally implemented in support of a specific Anonymous objective or campaign. For instance, one key Anonymous raison-d'être is to promote the ongoing "Operation Anti-Security" (also known as "AntiSec"), which is a declaration of cyber warfare on governments and corporations in response to perceived corruption and Internet censorship. As part of this campaign, Anonymous members are encouraged to locate and leak classified government information and to target banks or other high-profile establishments.

PAST TARGETS/BEHAVIOUR

Anonymous has initiated cyber threat activities in protest of government decisions and in support of their own principles. Recently, its hacktivism efforts have been concentrated on the various Occupy(11) movements, protesting Internet censorship and Internet filtering, protesting against oppressive regimes, and supporting WikiLeaks.

These campaigns include:

2008:
Project Chanology (worldwide)
Action: DDoS attacks were launched against the Church of Scientology websites and non-violent protests worldwide.
Reason: The Church of Scientology was attempting to restrict access to information that it found embarrassing and was readily available on the Internet.

2009:
Anonymous Iran (Iran)
Action: An Iranian Green Party Support site, Anonymous Iran, was created to provide covert resources and event updates for Iranian protestors during government-imposed Internet information censorship.
Reason: To provide support to Iranian protestors against a regime perceived to be corrupt.

Operation Didgeridie (Australia)
Action: A DDoS attack was launched against the Australian prime minister's website.
Reason: To protest against proposed government policy and legislation related to the implementation of ISP-level blacklists.

2010:
Operation Titstorm (Australia)
Action: A DDoS attack was launched against the Australian parliament's website and the prime minister's website was defaced.
Reason: To protest against the implementation of an Internet filter that would block websites containing child abuse material and certain types of pornography.

Operation Payback / Operation Sony (worldwide)
Action: DDoS attacks were launched against Sony PlayStation websites.
Reason: To support online file-sharing and to retaliate against Sony for seeking legal action against two individuals who successfully hacked the PlayStation3 system to allow users to run generic applications(12).

Operation Avenge Assange (US)
Action: DDoS attacks were launched against Amazon, PayPal, MasterCard and Visa websites.
Reason: To show support for WikiLeaks and to protest against its founder's arrest.

Operation Zimbabwe (Zimbabwe)
Action: DDoS attacks were launched against the Government of the Republic of Zimbabwe's websites.
Reason: To protest against censorship of WikiLeaks documents.

2011:
Operation Tunisia (Tunisia)
Action: DDoS attacks were launched on the Government of Tunisia's websites.
Reason: To protest against Internet censorship and to support the Arab Spring(13).

Operation Syria (Syria)
Action: Website of the Syrian Defence Ministry website was defaced.
Reason: To support the Arab Spring (Syrian uprising).

Operation Egypt (Egypt)
Action: A DDoS attack was launched against the Government of Egypt's website and the National Democratic Party's website. Also, the names and passwords of email addresses of government officials were released.
Reason: To support the Arab Spring (Egyptian revolution).

HBGary Federal (US)
Action: HBGary's website was defaced, company files were deleted and 68,000 employee emails were published.

Reason: An HBGary official provoked Anonymous by threatening to expose information about the group.

Bank Of America (US)
Action: Sensitive Bank of America documents were released online, which allegedly proved cases of corruption and fraud at the bank.
Reason: To protest in support of allegations of corruption and fraud within the US banking system.

Operation Malaysia (Malaysia)
Action: DDoS attacks were launched on 91 Government of Malaysia's websites.
Reason: In response to the Malaysian government's censorship of sites such as Pirate Bay(14) and WikiLeaks.

Occupy Wall Street (US)
Action: DDoS attacks were launched on the Oakland Police Department website and the St. Louis mayor's website.
Reason: To protest evictions of protestors from Occupy sites, in support of the worldwide Occupy movement.

Operation Mayhem (US)
Action: Guy Fawkes virus was released on Facebook.
Reason: To protest the Stop Online Piracy Act(15), perceptions of police violence towards protestors in Occupy movements and any opposition to Anonymous activities.

Cox Communications (US)
Action: Domain Name System (DNS) servers were taken offline, removing Internet access for clientele in most of southwest America.
Reason: To protest Cox Communications' attempted regulation of customers' data usage quota.

Operation Blackout (US)
Action: In November, Anonymous threatened action against the US government.
Reason: To protest against the Stop Online Piracy Act.

STRATFOR (worldwide)
Action: STRATFOR is a US company that provides services to intelligence and law enforcement agencies, among others. Two hundred gigabytes of data was stolen from STRATFOR's web servers and subsequently published. The stolen information included active credit cards, e-mail addresses, phone numbers, encrypted passwords and sensitive information from clients (including government and military departments). Anonymous planned to donate to charities using the stolen credit card information.
Reason: Following the HBGary incident, Anonymous began to investigate what it refers to as a "state-corporate alliance against the free information movement." Due to STRATFOR's ties with the intelligence and military contracting sectors and government agencies, Anonymous believed that targeting STRATFOR would "improve [their] ability to continue this investigation and thereby bring to light other instances of [perceived] corruption, crime and deception on the part of certain powerful actors based in the US and elsewhere(16)."

Ongoing:
Operation Antisec (NATO, Tunisia, Brazil, Australia, US, Turkey, UK, and other countries)
Action: In the US, DDoS attacks were launched against the Central Intelligence Agency's (CIA) website, the US Senate website was hacked and information about its internal server structure was released. In the UK, DDoS attacks were launched against the Serious Organised Crime Agency's (SOCA) website.
Reason: The declaration of cyber warfare on governments and corporations worldwide in response to perceived corruption and government censorship.

CANADA:
Anonymous has directly and indirectly targeted the Government of Canada, Canada's municipal governments and Canadian private corporations. Examples include:

Government of Canada:
STRATFOR (December 2011)
The federal government has been an indirect target of Anonymous activity in connection with STRATFOR. STRATFOR is a resource used by various federal departments. When usernames and passwords were released by Anonymous, some of them included those of federal employees(17).

Bill C-11, ACTA and Bill C-30 (February 2012):
The federal government was directly targeted by Anonymous in relation to the Bill-C-11 (Copyright Modernization Act), ACTA and C-30 (Lawful Access Package) through denial of service attacks and threats against the Public Safety Minister extensively covered in the media.

Municipal Governments:
Toronto (November 2011)
Anonymous threatened to take down the City of Toronto's website if officials evicted protestors from the Occupy Toronto camp. Although no known activity was conducted against the City of Toronto's website, the Toronto Police Service website was hacked and several usernames and passwords were stolen, possibly in retaliation to the continued efforts to evict the Occupy camp.

Private Corporations:
Operation Green Rights/ Project Tarmaggedon (July 2011)
In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline and the Alberta Tar Sands project.

TRADECRAFT

Anonymous has traditionally used basic, open-source-available cyber threat tradecraft against their targets. However, beginning in mid-2011, Anons have begun developing their own malware. (Comment: The exploits below do not represent a conclusive list because Anonymous has a large number of members and all of their activities cannot be tracked and attributed to Anonymous.)

DoS/DDoS:
Anonymous' usual method of choice is to launch DoS/DDoS attacks against a target's website in an effort to bring the network offline and to make the website unavailable to legitimate users. Two commonly used methods include:

- LOIC/HOIC/JS LOIC/BOIC:
Anons are encouraged to download and launch the Low Orbit Ion Cannon application enabling them to willingly participate in a botnet. The LOIC is pointed at a target of choice, which then disrupts the service of the victim's host. However, since LOIC can reveal the IP addresses of its users, its traceability has prompted Anonymous to find other means of attacks such as encouraging the use of anonymization proxy like TOR (The onion router). Other versions of the tool include a Javascript version, JS LOIC, and most recently, a Bookmark-based version coined BOIC. These versions require little more than one mouse-click to flood a target with GET and POST packets aimed at creating a denial of service condition.

- Apache Killer:
The Apache DoS tool nicknamed the "Apache Killer" exploits a vulnerability that allows remote attackers to send requests to servers via a malformed uniform resource identifier (URI)(20). It is designed to drain the web server's memory, which would then take the website offline. It also allows a remote attacker to use a single computer to wage DoS attacks against an Apache server.

DoS/DDoS via SQL Injections:
- #RefRef:

Anonymous developed and released a Perl DDoS tool in September 2011, #RefRef, that exploits SQL(21) vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline. #RefRef could be used in combination with tools such as Havij, an SQL Injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities. As a result of SQL vulnerability exploitation, database content could be changed, or database information (such as credit card information or passwords) could be stolen.

Guy Fawkes Virus:
Malware development is also something that Anonymous members have been focusing on. The Guy Fawkes(22) virus was developed by Anon to take control of a Facebook account and use it to spread malware to other members without the users actually logging onto the site. According to security analysts at the antivirus software company BitDefender, the Guy Fawkes virus (which they have named Backdoor-Bifrose-AAJX) has the ability to inject itself in the Internet Explorer process, providing a remote attacker with unhindered access to the compromised system. It would also record keystrokes and disrupt processes of known antimalware software. (Comment: Although the Guy Fawkes virus was previously believed to be responsible for the massive pornographic spam attack against Facebook in November 2011, this was later refuted by Facebook and BitDefender. Anonymous has stated that it is still working to control the virus to be used at a later date.)

Other:
Other techniques used by Anonymous include using social engineering techniques to gain access to victims' systems (e.g. HBGary Federal), using web defacement to post embarrassing messages on victims' websites, using password cracking to exfiltrate data from a victim's database, and using a Twitter raiding tool called Universal Rapid Gamma Emitter (URGE) to hijack Twitter trending topics into topics of interest to Anonymous. It also allows Anons to tweet messages within the topics.

MITIGATION

Strong IT security practices will go a long way to defending against threats such as the Anonymous hacktivist collective. Anonymous generally leverages open source or well-known vulnerabilities. The nature of the targets is also generally advertised in open forums such as Twitter and Pastebin, as well as main stream media.
Organizations are encouraged to consult CCIRC's mitigation guidelines for advanced persistent threats and DDoS attacks found here:
- http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx
- http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

In addition, the following mitigation is available for some of the tradecraft specifically noted above:

Apache Killer
- Apache has since released patches to fix this vulnerability. All users are recommended to upgrade to Apache 2.2.20 or higher.

#RefRef
- Webcode should be hardened against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users. Consult best practices references such as the Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)

ENDNOTES

(1) IRC is a protocol for Internet text messaging and synchronous conferencing. It allows group communications as well as private messaging and file sharing.

(2) A distributed denial-of-service (DDoS) attack is one in which a multitude of systems attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.

(3) SQL injection is often used to attack the security of a website by injecting SQL commands into the database of an application.

(4) Zero-day threats attempt to exploit new computer application vulnerabilities not yet known to the software developer or the general public.

(5) Anon-ops provides communications for Anonymous' announcements.

(6) LulzSec was a small team that joined forces with Anonymous in the ongoing "Operation Anti-Security" or "AntiSec" campaign, which later disbanded in the summer of 2011.

(7) LulzRaft was inspired by LulzSec group and has been responsible for web defacement of the Conservative Party of Canada's website and for accessing private information about the party's donors. They have also been linked to web defacement of Calgary-based energy company Husky Energy's website.

(8) Unofficial spokespeople for Anonymous include Jake Davis (also known by his online nickname "Topiary") and Barrett Brown. For more information on Jake Davis, please see http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-ukpolice/. For more information on Barrett Brown, please see http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx.

(9) According to open source, LOIC is an open source network stress testing application that performs DoS or DDoS attacks on a target site by flooding the server with TCP or UDP packets to disrupt the service of a host.

(10) HBGary Federal is a technology security company that was working with the FBI to unmask members of Anonymous. In February 2011, the CEO, Aaron Barr, revealed an intention to release information on the identities of Anonymous members. As a result, Anonymous members compromised the HBGary website and stole and publicly released the company's documents and emails.

(11) According to open source, the Occupy movement refers to an international protest movement directed against high unemployment, social and economic inequality and perceived corruption in corporations and government.

(12) For more information, please refer to http://www.pcmag.com/article2/0,2817,2383018,88.asp.

(13) The Arab Spring refers to revolutionary protests occurring in the Arab world beginning in December 2010. Countries affected include Tunisia, Egypt, Libya, Bahrain, Syria, Yemen, Algeria, Iraq, Jordan, Kuwait, Morocco, Oman, Lebanon and Saudi Arabia.

(14) The Pirate Bay is a Swedish website known for facilitating illegal downloads and supporting the international anti-copyright movement.

(15) The Stop Online Piracy Act is proposed US legislation to combat against the online distribution of copyrighted intellectual property. This has been viewed by Anonymous as an attempt to censor the Internet.

(16) For the full explanation, please refer to Barrett Brown's statement at http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-

hacked.

(17) CCIRC notified affected organizations accordingly.

(18) This legislation will be similar to previous bills: Bill C-50, Bill C-51 and Bill C-52.

(19) Operation Facebook was launched on November 5, 2011, because Anonymous believes that "Facebook is the opposite of the Antisec cause."

(20) For more information, please refer to CVE-2011-3192 at http://nvd.nist.gov/.

(21) An SQL server is a relational database server that can store and retrieve data across a network (e.g. the Internet). Queries from client machines are formatted in the SQL language.

(22) Guy Fawkes was associated with the Gunpowder Plot, a failed assassination attempt against King James I of England in 1605. The conspirators' plan was to blow up the Houses of Parliament in order to kill the King and the Members of Parliament. Coincidentally, Anons have adopted the easily available and inexpensive Guy Fawkes mask as their symbol.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589

SÉCURITÉ PUBLIQUE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

****
NOTE D'INFORMATION
****

Numéro : IN12-501
Date : 1 mars 2012

****
Aperçu du collectif d'hacktivistes Anonymous
****

OBJECTIF
========

Le présent rapport donne un aperçu du groupe d'hacktivistes Anonymous. Il présente

des renseignements sur sa structure organisationnelle, ses techniques et ses cibles, sur la menace qu'il pose pour les systèmes d'infrastructures essentielles du Canada et sur les mesures d'atténuation recommandées.

ÉVALUATION

SOMMAIRE

Anonymous cible les gouvernements, les entreprises privées et les particuliers dont les activités ou les buts semblent être en conflit avec les principes énoncés par le groupe. Ces principes sont axés sur les droits civils (p. ex., régimes oppressifs), l'accès à l'information (p. ex., censure sur Internet) et d'autres causes liées aux injustices sociales perçues.

Compte tenu des cibles précédentes d'Anonymous, les systèmes des infrastructures essentielles du Canada pourraient être ciblés en raison des initiatives législatives et réglementaires du gouvernement (p. ex., Loi sur la modernisation du droit d'auteur) et d'initiatives qui pourraient provoquer une opposition militante (p. ex, enjeux sociaux ou environnementaux).

Anonymous utilise diverses capacités contre ses cibles : attaques distribuées par déni de service (DDoS) (2), craquage de mots de passe, injections SQL (3), déploiements de maliciels (virus), etc. Des organisations canadiennes ont été ciblées directement et indirectement par des activités d'Anonymous. Par exemple, le site Web du service de police de Toronto a été piraté en 2011, probablement en réponse aux expulsions du camp Occupons Toronto; des entreprises canadiennes qui participent à l'exploitation des sables bitumineux en Alberta ont été ciblées, en particulier pour manifester contre le pipeline Keystone XL; et, à la suite de l'attaque à la fin 2011 contre STRATFOR, une entreprise des É.-U. avec des liens avec les organismes de renseignement et d'application de la loi, les justificatifs utilisés par des entreprises canadiennes pour accéder aux bases de données de STRATFOR ont été publiés. Anonymous utilise diverses techniques pour réaliser ses objectifs, mais des pratiques solides en matière de sécurité de la TI aident à se protéger contre ces attaques. La majorité des attaques ne tirent pas profit de vulnérabilités du jour zéro (4).

APERÇU

Les pirates militants poursuivent de plus en plus des activités de menaces cybernétiques pour atteindre leurs objectifs. En particulier, le terme « Anonymous » fait référence à un groupe de pirates militants (hacktivistes) qui font peser un large éventail de cybermenaces sur les gouvernements et les organisations commerciales partout au monde. Le programme d'Anonymous a compris l'utilisation de cybermenaces pour manifester contre la censure gouvernementale perçue sur Internet et appuyer des mouvements militants internationaux.

STRUCTURE

Anonymous comprend un ensemble hétérogène de sous-groupes (p. ex., Anon-ops5, LulzSec6) et mène souvent des campagnes en collaboration avec d'autres groupes hacktivistes qui partagent les mêmes objectifs. Par exemple, TeaMpOisoN et le People's Liberation Front sont des groupes hacktivistes distincts qui sont libres de participer ou non à des projets conjoints avec Anonymous. Le mouvement Anonymous a aussi été imité par d'autres groupes hacktivistes, par exemple, LulzRaft7.

Anonymous n'est pas organisé hiérarchiquement et n'a pas de chefs définis. De plus, Anonymous n'a pas de porte-parole officiel, même s'il y a plusieurs porte-paroles officieux (8). La seule exigence que les membres d'Anonymous (les « Anons ») doivent respecter est de garder l'anonymat lorsqu'ils participent à des campagnes

cybernétiques pour appuyer les efforts du groupe. Dans de nombreux cas, les Anons se joignent volontairement à un réseau zombie en téléchargeant et en installant l'application LOIC (Low Orbit Ion Cannon) (9) sur leur ordinateur. (Remarque : L'absence d'une structure de direction définie peut expliquer pourquoi certaines menaces associées à Anonymous sont mises à exécution, alors que d'autres n'aboutissent pas si un consensus au sujet d'une cible ne se dégage pas parmi les membres.)

SÉLECTION DE CIBLES

Puisqu'Anonymous est décentralisé, les nouvelles cibles sont fixées de diverses façons. Voici certaines méthodes souvent utilisées et bien documentées de sélection de cibles :

- Consensus des membres dégagé au moyen de sondages en ligne. Après une période de discussion par l'intermédiaire du service de clavardage IRC, un sondage en ligne est réalisé pour fixer les cibles d'attaques de déni de service (DoS) ou de DDoS. Le processus peut sembler démocratique, mais ce sont les Anons d'élite qui exploitent les canaux IRC qui prennent la décision définitive sur la cible des attaques effectuées au moyen de LOIC.
- En réponse à une provocation directe ou indirecte perçue de la part de gouvernements, d'autres groupes pirates ou d'entreprises (p. ex., HBGary (10)) contre le groupe Anonymous ou ses principes.
- Pour exposer de mauvaises pratiques en matière de sécurité. Par exemple, les membres d'Anonymous peuvent utiliser la technique « Google hacking » pour détecter des cibles intéressantes. Les résultats de ces activités de reconnaissance sont souvent publiés sur des sites tels que pastebin.com.

Ces pratiques de ciblage sont généralement mises en œuvre pour appuyer un objectif ou une campagne en particulier d'Anonymous. Par exemple, une raison d'être importante d'Anonymous est de promouvoir l'opération « Anti-Security » (ou AntiSec), une déclaration de cyberguerre contre les gouvernements et les entreprises en réponse à une corruption ou à une censure Internet perçues. Dans le cadre de cette campagne, Anonymous encourage ses membres à trouver et à divulguer des renseignements gouvernementaux confidentiels et de cibler des banques et d'autres établissements bien en vue.

CIBLES ET COMPORTEMENTS DANS LE PASSÉ

Anonymous a lancé des activités de cybermenaces pour manifester contre des décisions gouvernementales et pour appuyer ses propres principes. Plus récemment, ces efforts hacktivistes appuyaient les divers mouvements Occupons (11) et WikiLeaks et s'opposaient à la censure et au filtrage d'Internet ainsi qu'aux régimes oppressifs. Voici un aperçu de certaines de certaines campagnes :

2008 :
Projet Chanalogy (à l'échelle mondiale)
Démarche : Attaques DDoS lancées contre les sites Web de l'église de Scientologie et manifestations non violentes à l'échelle mondiale.
Raison : L'Église de Scientologie essayait de limiter l'accès à des informations disponible sur Internet qu'elle jugeait embarrassantes.

2009 :
Anonymous Iran (Iran)
Démarche : Création d'Anonymous Iran, un site d'appui du Parti vert d'Iran, pour fournir des ressources clandestines et des renseignements sur les événements aux manifestants iraniens dans le cadre de la censure des renseignements Internet imposée par le gouvernement.
Raison : Appuyer les manifestants iraniens contre un régime perçu comme corrompu.

Opération Didgeridie (Australie)
Démarche : Attaque DDoS lancée contre le site Web du premier ministre australien.
Raison : Manifester contre la politique et les lois proposées relatives à la mise en œuvre de listes noires au niveau des FSI.

2010 :
Opération Titstorm (Autralie)
Démarche : Attaque DDoS lancée contre les sites Web du Parlement australien et altération du site Web du premier ministre australien.
Raison : Manifester contre la mise en œuvre d'un filtre Internet qui bloquerait les sites Web présentant de mauvais traitements d'enfants et certains types de pornographie.

Opérations Payback et Sony (à l'échelle mondiale)
Démarche : Attaques DDoS lancées contre les sites Web de Sony PlayStation.
Raison : Appuyer le partage de fichiers en ligne et exercer des représailles sur Sony pour avoir intenté des poursuites contre deux personnes qui avaient réussi à débrider le système PlayStation 3 pour permettre aux utilisateurs d'exécuter des applications génériques (12).

Opération Riposte Assange (« Avenge Assange ») (É.-U.)
Démarche : Attaques DDoS lancées contre les sites Web d'Amazon, de PayPal, de MasterCard et de Visa.
Raison : Manifester du soutien à l'égard de WikiLeaks et manifester contre l'arrestation de son fondateur.

Opération Zimbabwe (Zimbabwe)
Démarche : Attaques DDoS lancées contre les sites Web de la République du Zimbabwe.
Raison : Manifester contre la censure des documents de WikiLeaks.

2011 :
Opération Tunisie (Tunisie)
Démarche : Attaques DDoS lancées contre les sites Web du gouvernement de la Tunisie.
Raison : Manifester contre la censure d'Internet et appuyer le printemps arabe (13).

Opération Syrie (Syrie)
Démarche : Site Web du ministère de la Défense syrien altéré.
Raison : Appuyer le Printemps arabe (soulèvement en Syrie).

Opération Égypte (Égypte)
Démarche : Attaque DDoS lancée contre les sites Web du gouvernement égyptien et du Parti national démocratique. De plus, publication des noms et des mots de passe des comptes de courriel de hauts fonctionnaires du gouvernement.
Raison : Appuyer le Printemps arabe (soulèvement en Égypte).

HBGary Federal (É.-U.)
Démarche : Altération du site Web de HBGary, suppression de fichiers de l'entreprise, publication de 68 000 courriels d'employés.
Raison : Un représentant de HBGary a provoqué Anonymous en menaçant de divulguer des renseignements sur le groupe.

Banque d'Amérique (É.-U.)
Démarche : Des documents de nature sensible de la Banque d'Amérique, qui sont censés prouver des cas de corruption et de fraude à la banque, sont publiés en ligne.
Raison : Appuyer des allégations de corruption et de fraude au sein du système bancaire aux É.-U.

Opération Malaisie (Malaisie)
Démarche : Attaques DDoS lancées contre 91 sites Web du gouvernement de la Malaisie.
Raison : Répondre à la censure par le gouvernement de la Malaisie de sites tels que Pirate Bay (14) et WikiLeaks.

Occupons Wall Street (É.-U.)
Démarche : Attaques DDoS lancées contre les sites Web du service de police d'Oakland et de maire de St. Louis.
Raison : Manifester contre l'expulsion des manifestants des sites Occupons et appuyer le mouvement Occupons international.

Opération Mayhem (É.-U.)
Démarche : Virus Guy Fawkes diffusé sur Facebook.
Raison : Manifester contre le projet de loi Stop Online Piracy Act (15), la perception de violence policière dans le cadre des mouvements Occupons et toute forme d'opposition aux activités d'Anonymous.

Cox Communications (É.-U.)
Démarche : Serveurs DNS (Domain Name System) mis hors ligne, bloquant l'accès Internet de la plupart des clients dans le sud-ouest des É.-U.
Raison : Manifester contre la restriction par Cox Communications des quotas d'utilisation de données des clients.

Opération Blackout (É.-U.)
Démarche : En novembre, menaces proférées par Anonymous contre le gouvernement des É.-U.
Raison : Manifester contre le projet de loi Stop Online Piracy Act.

STRATFOR (à l'échelle mondiale)
Démarche : STRATFOR est une entreprise des É.-U. qui fournit des services aux organismes du renseignement et d'application de la loi et à d'autres clients. 200 Go de données sont volés sur les serveurs Web de STRATFOR et ensuite publiés. L'information volée comprend des numéros de cartes de crédit actives, des adresses de courriel, des numéros de téléphone, des mots de passe chiffrés et des renseignements de nature sensible des clients (y compris des ministères gouvernementaux et des services militaires). Anonymous compte faire des dons à des organismes de bienfaisance en utilisant les renseignements volés sur les cartes de crédit.
Raison : À la suite de l'incident HBGary, Anonyme a lancé une enquête sur ce qu'elle nomme une alliance entre l'État et le secteur privé contre le mouvement de l'information libre. En raison des liaisons de STRATFOR avec les secteurs de marchés militaires et du renseignement et les organismes gouvernementaux, Anonymous croit qu'en ciblant STRATFOR, il pourra améliorer sa capacité de poursuivre cette enquête et, ainsi, de divulguer d'autres cas de corruption, de crime et de pratiques trompeuses [soi-disant] de la part d'acteurs puissants situés aux É.-U. et ailleurs (16).

En cours :
Opération AntiSec (OTAN, Tunisie, Brésil, Australie, É.-U., Turquie, Royaume-Uni et autres pays)
Démarche : Aux É.-U., attaques DDoS contre le site Web de la CIA. Piratage du site Web du Sénat des É.-U. et publication de renseignements sur sa structure interne de serveurs. Au Royaume-Uni, attaques DDoS contre le site Web du Serious Organised Crime Agency (SOCA).
Raison : Déclaration de guerre cybernétique à l'échelle mondiale contre des gouvernements et des entreprises en réponse à la corruption et à la censure par le gouvernement perçues.

CANADA :
Anonymous a ciblé, directement et indirectement, le gouvernement, des administrations municipales et des entreprises privées du Canada. En voici des exemples :

Gouvernement du Canada :
STRATFOR (décembre 2011)
Le gouvernement fédéral est une cible indirecte des activités d'Anonymous relatives à STRATFOR. Divers ministères fédéraux consultent les ressources de STRATFOR. Des noms de compte et des mots de passe d'employés fédéraux figurent parmi les

renseignements publiés par Anonymous (17).

Projet de loi C-11, Accord commercial relatif à la contrefaçon (ACRC) et Projet de loi C-30 (février 2012)
Le gouvernement fédéral a été ciblé directement par Anonymous, au moyen d'attaques DoS et de menaces fortement médiatisées contre le ministre de la Sécurité publique, en réponse au projet de loi C-11 (Loi sur la modernisation du droit d'auteur), à l'ACRC et au projet de loi C-30 (accès licite).

Administrations municipales :
Toronto (novembre 2011)
Anonymous a menacé de mettre hors ligne le site Web de la Ville de Toronto si les fonctionnaires expulsent les manifestants du camp Occupons Toronto. Aucune activité n'a été effectuée contre le site Web de la Ville de Toronto, mais le site Web du service de police de Toronto a été piraté et des noms de compte et des mots de passe ont été volés, possiblement en guise de représailles aux efforts continus pour expulser les manifestants du camp Occupons.

Entreprises privées :
Opération Green Rights et projet Tarmaggedon (juillet 2011)
En réponse à des préoccupations environnementales, Anonymous a ciblé des entreprises associées au pipeline Keystone XL et au projet de sables bitumineux en Alberta.

TECHNIQUES

Anonymous a traditionnellement utilisé des techniques de cybermenaces de base disponibles de sources ouvertes contre ses cibles. Par contre, à compter de la mi-2011, des Anons ont commencé à développer leurs propres maliciels. (Remarque : La liste d'attaques ci-dessous n'est pas exhaustive, puisqu'Anonymous compte un grand nombre de membres et que leurs activités ne peuvent pas toutes être tracées et attribuées à Anonymous.)

DoS et DDoS :
La méthode privilégiée d'Anonymous est de lancer des attaques DoS ou DDoS contre le site Web de la cible pour essayer de mettre son réseau hors ligne et d'empêcher l'accès au site par les utilisateurs légitimes. Voici les méthodes le plus souvent utilisées :

- /HOIC/JS LOIC/BOIC :
On encourage les Anons à télécharger et à lancer l'application Low Orbit Ion Cannon (LOIC) pour leur permettre de participer volontairement au réseau zombie. Le LOIC est pointé vers la cible choisie pour perturber le service de l'hôte. Toutefois, puisque le LOIC peut révéler les adresses IP de ses utilisateurs, Anonymous a cherché d'autres modes d'attaque, par exemple l'utilisation d'un mandataire d'anonymisation tel que TOR (The Onion Router). D'autres versions de l'application comprennent une version JavaScript, JS LOIC, et, plus récemment, une version fondée sur les favoris (nommée BOIC). Ces versions ne demandent guère plus qu'un clic pour inonder la cible avec un grand nombre de paquets GET et POST afin de créer un déni de service.

- Apache Killer :
L'outil de DoS Apache, surnommé Apache Killer, exploite une vulnérabilité qui permet aux attaquants à distance d'envoyer des requêtes à des serveurs au moyen d'un identificateur de ressource uniforme (URI) mal formé (20. Il est conçu pour surcharger la mémoire du serveur Web et, ainsi, mettre le site Web hors ligne. Il permet aussi à un attaquant à distance de mener une attaque DoS contre un serveur Apache à partir d'un seul ordinateur.

Attaques DoS et DDoS au moyen d'injections SQL :
- #RefRef :
Anonymous a développé et publié, en septembre 2011, un outil de DDoS en Perl,

#RefRef, qui exploite des vulnérabilités de SQL (21). L'outil envoie des requêtes SQL mal formées, conçues pour surcharger les ressources du serveur, à un portail Web hébergé sur un serveur SQL. Par conséquent, le site Web est mis hors ligne. #RefRef peut être utilisé avec d'autres outils, par exemple, Havij, un outil d'injection SQL qui aide les vérificateurs de pénétration à trouver et à exploiter des vulnérabilités d'injection SQL. Ces attaques contre des vulnérabilités de SQL peuvent modifier le contenu de bases de données ou voler des données de bases de données (p. ex., renseignements sur les cartes de crédit ou mots de passe).

Virus Guy Fawkes :
Les membres d'Anonymous se sont aussi axés sur le développement de maliciels. Le virus Guy Fawkes (22) a été développé par des Anons pour prendre le contrôle d'un compte Facebook et s'en servir pour distribuer des maliciels à d'autres membres sans connexion réelle de l'utilisateur au site. Selon des analystes de la sécurité de l'entreprise de logiciels antivirus BitDefender, le virus Guy Fawkes (qu'ils nomment Backdoor-Bifrose-AAJX) peut s'injecter dans le processus d'Internet Explorer, donnant ainsi un accès sans entrave au système compromis. Il peut aussi enregistrer les frappes et perturber les opérations de logiciels antimaliciels connus. (Remarque : On croyait que le virus Guy Fawkes était responsable de l'attaque pornographique massive contre Facebook en novembre 2011, mais Facebook et BitDefender ont par la suite réfuté cette hypothèse. Anonymous affirme qu'il travaille encore à contrôler le virus en vue d'une utilisation ultérieure.)

Autre :
Anonymous utilise aussi d'autres techniques : ingénierie sociale pour obtenir l'accès aux systèmes des victimes (p. ex., HBGary Federal), altération de sites Web ciblés pour afficher des messages embarrassants, craquage de mots de passe pour extraire des renseignements de bases de données, utilisation d'un outil de détournement Twitter nommé Universal Rapid Gamma Emitter (URGE) pour détourner les sujets d'actualité sur Twitter vers des sujets d'intérêt à Anonymous, etc. L'outil URGE permet aussi aux Anons de poster des gazouillis sur ces sujets.

ATTÉNUATION

Des pratiques solides en matière de sécurité de la TI aident à se protéger contre des menaces telles que celles présentées par le collectif hacktiviste Anonymous. Anonymous met généralement à profit des techniques en source ouverte ou des vulnérabilités bien connues. Les cibles sont généralement annoncées dans des forums ouverts (p. ex., Twitter, Pastebin) et dans les médias.
Nous encourageons les organisations à consulter les principes de prévention contre les menaces sophistiquées et persistantes et contre les attaques par déni de service du CCRIC aux adresses suivantes :
- http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-fra.aspx
- http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

De plus, les mesures d'atténuation suivantes sont disponibles pour se protéger contre certaines des techniques susmentionnées :

Apache Killer :
- Apache a publié des correctifs pour cette vulnérabilité. Nous recommandons à tous les utilisateurs de mettre leur système à niveau à la version 2.2.20 (ou plus récente) d'Apache.

#RefRef :
- Le code Web devrait être renforcé contre les injections SQL pour empêcher le serveur d'exécuter des requêtes SQL arbitraires provenant d'utilisateurs inconnus. Consultez les références sur les pratiques exemplaires, p. ex. l'Open Web Application Security Project (OWASP) - https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet (en anglais seulement).

NOTES DE FIN

(1) IRC est un protocole de communication textuelle et de conférences en temps réel sur Internet. Il assure les communications de groupe ainsi que la messagerie privée et le partage de fichiers.

(2) Dans une attaque distribuée par déni de service (DDoS), de multiples systèmes attaquent une seule cible. Le déluge de messages entrants vers le système ciblé force sa fermeture et empêche la prestation de services aux utilisateurs légitimes.

(3) L'injection SQL est souvent utilisée pour attaquer la sécurité d'un site Web en injectant des commandes SQL dans la base de données d'une application.

(4) Les attaques du jour zéro essaient d'exploiter des vulnérabilités logicielles qui ne sont pas encore connues des développeurs du logiciel ou du grand public.

(5) Anon-ops assure la communication des annonces d'Anonymous.

(6) LulzSec était une petite équipe qui s'est associée à Anonynmous dans le cadre de la campagne à long terme Anti-Security (ou AntiSec). LulzSec a mis fin à ses activités à l'été 2011.

(7) LulzRaft a été inspiré par le groupe LulzSec et est responsable de l'altération du site Web du Parti conservateur du Canada et de l'accès aux renseignements privés sur les donateurs du parti. Ils ont aussi été liés à l'altération du site Web de l'entreprise d'énergie Husky Energy, établie à Calgary.

(8) Les porte-paroles officieux d'Anonymous comprennent Jake Davis (aussi connu sous son pseudonyme en ligne, « Topiary ») et Barrett Brown. Pour en savoir plus sur Jake Davis, consultez http://www.lefigaro.fr/hightech/2011/08/01/01007-20110801ARTFIG00418-piratage-des-lulzsec-un-anglais-de-18-ans-au-tribunal.php. Pour en savoir plus sur Barrett Brown, consultez http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx (en anglais).

(9) Selon des sources d'information ouvertes, LOIC est une application d'essais sous contrainte de réseau en source libre qui permet d'effectuer des attaques DoS ou DDoS contre un site cible en l'inondant de paquets TCP ou UDP pour perturber ses services.

(10) HBGary Federal est une entreprise de sécurité de la technologie qui collaborait avec le FBI pour démasquer les membres d'Anonymous. En février 2011, le PDG, Aaron Barr, a révélé leur intention de publier des renseignements sur l'identité des membres d'Anonymous. Par conséquent, des membres d'Anonymous ont compromis le site Web de HBGary et ont volé et publié des documents et des courriels de l'entreprise.

(11) Selon des sources d'information ouvertes, le mouvement Occupons désigne un mouvement international de manifestation contre les taux de chômage élevés, l'inégalité sociale et économique et la corruption perçue au sein des entreprises et des gouvernements.

(12) Pour en savoir plus, consultez http://www.branchez-vous.com/techno/actualite/2011/04/anonymous-sony-playstation-3-piratage-geohot-cyberattaque.html.

(13) Le terme printemps arabe désigne des manifestations révolutionnaires dans le monde arabe à partir de décembre 2010. Les pays touchés comprennent la Tunisie, l'Égypte, la Lybie, Bahreïn, la Syrie, le Yémen, l'Algérie, l'Iraq, la Jordanie, le Koweït, le Maroc, Oman, le Liban et l'Arabie saoudite.

(14) The Pirate Bay est un site Web suédois notoire qui facilite les téléchargements illégaux et appuie le mouvement international contre le droit d'auteur.

(15) Stop Online Piracy Act (SOPA) est un projet de loi des É.-U. pour combattre la distribution en ligne de propriété intellectuelle protégée par le droit d'auteur. Anonymous le considère comme une tentative de censure d'Internet.

(16) Pour obtenir l'explication complète d'Anonymous, consultez la déclaration de Barrett Brown à http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-hacked.

(17) Le Centre d'évaluation des cybermenaces (CECM) a fourni des mesures d'atténuation aux employés des ministères touchés.

(18) Ce projet de soi est semblable aux projets de loi C-50, C-51 et C-52 précédents.

(19) L'opération Facebook a été lancée le 5 novembre 2011 parce qu'Anonymous croit que « Facebook est à l'opposé des valeurs d'AntiSec ».

(20) Pour en savoir plus, consultez le bulletin CVE-2011-3192 à http://nvd.nist.gov/ (en anglais).

(21) Un serveur SQL est un serveur de base de données relationnelle qui peut stocker et récupérer des données sur un réseau (p. ex., Internet). Les requêtes provenant des ordinateurs clients sont formatées dans le langage SQL.

(22) Guy Fawkes était associé à la Conspiration des poudres (« Gunpowder Plot »), une tentative infructueuse d'assassinat du roi James I d'Angleterre en 1605. Le projet des conspirateurs était de faire sauter le Parlement pour tuer le roi et les membres du Parlement. Les Anons ont d'ailleurs adopté comme symbole le masque de Guy Fawkes, facilement accessible et bon marché.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118
Télécopieur : 613-998-9589
Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Cybertech

s.16(2)(c)

From: CYBERDO
Sent: March-15-12 7:29 AM
To: [redacted]
Subject: FW: Important: Anonymous-OS 0.1 : Anonymous Hackers released their own Operating System

Fyi..

Sheldon Billard

Canadian Cyber Incident Response Centre | canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Ottawa, Ontario, Canada K1A 0P8 Telephone | Téléphone 613-991-7056

-----Original Message-----
From: Bendelier, Kenneth
Sent: March-14-12 4:41 PM
To: CYBERDO; Beaudoin, Luc
Cc: Proulx, Véronique
Subject: Fw: Important: Anonymous-OS 0.1 : Anonymous Hackers released their own Operating System

----- Original Message -----
From: E-Secure-IT [mailto:alert@e-secure-it.com]
Sent: Wednesday, March 14, 2012 04:39 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous-OS 0.1 : Anonymous Hackers released their own Operating System

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Hacker News
Complete item: http://thehackernews.com/2012/03/anonymous-os-01-anonymous-hackers.html

Description:
Yes! Its true, Anonymous Hackers released their own Operating System with name "Anonymous-OS", is Live is an ubuntu-based distribution and created under Ubuntu 11.10 and uses Mate desktop. You can create the LiveUSB with Unetbootin.

E-Secure-IT
https://www.e-secure-it.com

This exact email was held under cyber as well

Dvorkin, Corey

From: Dincoy, Rana
Sent: March-07-12 10:05 AM
To: Dvorkin, Corey; Klassen, Nathan; Proulx, Véronique
Subject: Emailing: Big Brother's nasty cousin

Published | PubliÃ©: 2012-03-07
Received | ReÃ§u: 2012-03-07 3:20 AM

THE GLOBE AND MAIL

GLOBE AND MAIL (METRO)
EDITORIAL, Page: A16

Big Brother's nasty cousin

The hackers group Anonymous is trying to hijack the democratic process, and House of Commons Speaker Andrew Scheer is right to treat it as a threat.

It claims to be fighting for freedom of speech in challenging the Canadian government's Bill C-30, which would give police extra powers to oversee Internet users and watch out for child predators, without having to ask for a judge's permission first. In fact, Anonymous is using a personal threat to try to muzzle an elected member of Parliament and cabinet minister. The Parliamentary privilege that Mr. Scheer accuses Anonymous of breaching is the most basic one of being able to represent constituents and defend bills without fear of personal reprisal. The anonymous, digital voices used by the hackers group do add a satirical counterpoint to Bill C-30, with its overtones of Orwell's Big Brother watching over people's shoulders. As the state's anonymous minions keep an eye on the people, Anonymous seems to say that the people are now keeping an eye on the state. If it had stopped there, it would have been fair comment - even with its crudities about the personal life of Public Safety Minister Vic Toews, irrelevant to the question of whether the bill is appropriate or not.

But the real reason for the anonymity is not to create satire but to shield the group from being accountable for its actions and to enable its attempts at intimidation, now and in the future. "We know all about you, Mr. Toews," it said, and threatened to "release what we have unless you scrap this bill." If such a threat were allowed to succeed, Anonymous might as well run Parliament.

Mr. Toews, in introducing the bill, attempted a kind of moral bullying when he said that anyone opposed is on the side of child pornographers. And the government, which opposes the long-gun registry and the long-form census as intrusions on Canadians' privacy, is at best being inconsistent in proposing a highly intrusive law to police the Internet.

But making a personal threat and attempting to coerce a Member of Parliament, and by extension, Parliament itself, add up to a more serious mistake. Fighting for freedom from the state by denying freedom of speech to elected representatives is a perverse and dangerous way to make a point.

Dvorkin, Corey

From: Dave Black <Dave.Black@rcmp-grc.gc.ca>
Sent: March-06-12 11:22 AM
To: John Cau; Lee Shields; Robyn O'Meara; Sophie Sirois; Terry Hart
Cc: Dvorkin, Corey; Jeff Beaulac; Spendlove, Jim; Marc Ottawa - Tech Crime Moreau
Subject: Remember Lulzsec's boast last year that Law Enforcement couldn't touch them?

Breaking news from FOX News:

EXCLUSIVE: Inside LulzSec, a mastermind turns on his minions

Read more: http://www.foxnews.com/scitech/2012/03/06/exclusive-inside-lulzsec-mastermind-turns-on-his-minions/#ixzz1oM1OjYsb

EXCLUSIVE: For the last eight months, the self-styled "hacktivists" who make up LulzSec and the international hacker community beyond have been led by a turncoat.

Like a Mafia don who wears a wire to ensnare his own soldiers, Hector Xavier Monsegur, aka "Sabu," has been helping the FBI track down and gather evidence against his associates, tweeting out misinformation and even protecting the CIA among other government and financial institutions from hacks, according to sources close to the LulzSec leader and law enforcement officials in charge of the months-long international hacking probe capped by international arrests of the remaining LulzSec leaders on Tuesday morning.

Flipping Monsegur wasn't easy. But with a charge of aggravated identity theft and a two-year prison sentence to hang over his head, the FBI forced Monsegur to weigh the political beliefs that drove him and his allegiance to cohorts around the world against his desire to be with his kids—he is the guardian of two children—and his extended family.

"He didn't go easy," a law enforcement official involved in flipping Sabu told FoxNews.com. "It was because of his kids. He didn't want to go away to prison and leave them. That's how we got him."

"He really cares about these kids," a source said. "They're young [and] he is really worried about what will happen."

On Aug. 15, 2011, Monsegur pleaded guilty to more than ten charges relating to his hacking activity. In the following few weeks, he worked almost daily out of FBI offices, helping the feds identify and ultimately take down the other high-level members of LulzSec and Anonymous, sources said. In time, his handlers allowed him to work from the home from which he previously wrought destruction, using a PC laptop provided by the FBI. His old battered laptop with its missing left Shift, L and 7 keys was turned over to the FBI, along with the encryption keys government sleuths needed to access his records and take them into evidence.

The white pit bull Monsegur bought shortly after his arrest sits at his feet, barking at all strangers who step off the elevator.

Monsegur maintained the same habits and online presence he did prior to his arrest as the young hackers he commanded sat alone in their rooms around the world, searching for vulnerabilities on websites and servers. Their leads were sent to Sabu, like offerings made to a monarch.

"In half the world he was a god," one law enforcement official explained. "If he thought what you did was good, you'd rise up in the [hacker] community—once he blessed you, basically."

"About 90 percent of what you see online is bulls---."

- One of Monsegur's FBI handlers

Sabu was online between 8 and 16 hours a day, often sleeping during the day and working throughout the night, watching YouTube videos as he worked for the FBI. Monitoring software on his government-issued laptop allowed the feds to see what he did in real time. The FBI has had an agent watching his online activity 24 hours a day, officials said.

When Sabu told his handlers of a vulnerability his minions detected in a company or government server, the feds reached out to the targets and tried to prevent damage. Sometimes, it was too late.

Sabu and his FBI handlers also disseminated false information to the public and hacker community—often through Twitter, sometimes through unsuspecting reporters who thought they'd landed an online interview with the notorious hacker. Their correspondence was sometimes directly with agents. More often it was with Sabu acting on strict guidance from the agents sitting with him, reading his every word.

"About 90 percent of what you see online is bulls---," said one of Monsegur's handlers, referring to the Twitter posts from Sabu's account and "interviews" he's given to the press on direction from the FBI as part of their disinformation campaign.

With Sabu's help, the FBI learned the identities of other LulzSec members, gathered evidence and records from private chatrooms used by the elite hackers to plan and discuss their cyber attacks, and found out about planned hacks in time to minimize or prevent damage without blowing their star witness' cover.

In August, 2011, it became known that LulzSec affiliate Anonymous had hacked into 70 law enforcement websites, mostly local sheriffs' websites in Missouri run by the same hosting company. The hacks had actually occurred four weeks prior. Using information passed on by Monsegur, the FBI was able to work with the server company to mitigate the damage.

With Sabu's help, the FBI alerted 300 government, financial and corporate entities in the U.S. and around the globe to potential vulnerabilities in their computer systems, allowing the companies to protect themselves, an FBI supervisory official told FoxNews.com.

Sabu's work as a cooperating witness also included fact-checking allegations from his peers. When members of LulzSec and Anonymous announced publicly that they'd hacked a company to steal information, Sabu would verify or discredit the claims. Most of the time, the hackers just got into computer systems and databases and looked around without taking anything—but even the rumor of a breach can cause a company to spend large amounts of money or spook stockholders.

When the CIA found itself under siege from LulzSec hackers, Sabu stepped in. With his underlings launching so-called DDoS attacks -- denial of service cyberattacks that basically flood a website with traffic to overwhelm it -- the CIA's public website was threatened.

"We told Sabu to tell them to stop," an official said. "'It's embarrassing for the CIA,' we told Sabu, 'Make them stop, now.'"

Sabu sent out the order: "You're knocking over a bee's nest," he warned his associates. "Stop."

They did.

The example showed the power of the alienated young father who used his brilliant mind to wreak economic havoc around the world from the least likely computer command center until the feds unmasked him. Afforded cult-leader status by his fellow hackers, Monsegur evoked both respect and envy.

"He's a rockstar," a New York-based hacker with close ties to WikiLeaks said recently. "All the girls, you buy them a drink, but all they want to talk about is Sabu, Sabu, Sabu.

"And what really sucks is he really is that good."

Today, the hackers who worshipped Sabu are in for a rude awakening.

"When people in the hacking community realize their God has actually been cooperation with the government, it'll be sheer terror," said one senior official.

Another source was even more blunt: "You might be a messiah in the hacking community but you're still a rat," he said.

Read more: http://www.foxnews.com/scitech/2012/03/06/exclusive-inside-lulzsec-mastermind-turns-on-his-minions/#ixzz1oM17k7Jg

Dvorkin, Corey

From: Scrivens, Mark <Mark.Scrivens@justice.gc.ca>
Sent: March-06-12 12:22 PM
To: Dvorkin, Corey; Pilon, Claude; Bruce, John (CSE)
Subject: How to join anonymous (hopefully a malware free website!)

http://www.cyberguerrilla.org/?p=1591

Mark Scrivens
Senior Counsel | Avocat-conseil
Office of the Assistant Deputy Attorney General | Bureau du Sous-Procureur Général Adjoint
Public Safety, Defence, and Immigration Portfolio | Portefeuille de la Sécurité Publique, de la Défense, et de l'Immigration et Sécurité Publique

Justice Canada
Jean Edmonds, Tower South | Tour Sud
365 Laurier Avenue West | 365 Avenue Laurier Ouest 15th Floor | 15e étage, OTTAWA, ON
K1A 1L1
mailto:mscriven@justice.gc.ca
Telephone | Téléphone (613) 954-1248
Facsimile | Télécopieur (613) 957-7840

CYBERDO

From: Beaudoin, Luc
Sent: March-03-12 1:11 PM
To: CYBERDO; [redacted]
Cc: Bendelier, Kenneth
Subject: [redacted] leaked by Anonymous

s.15(1) - Subv
s.16(2)(c)

CTEC,

FYI and something to monitor on your end.

Luc

http://pastebin.com[redacted]

Description:

[redacted]

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

Hayward, Jane

From: CYBERDO
Sent: March-07-13 10:53 AM
To: Proulx, Véronique
Subject: FW: CCIRC Technical Report TR12-001: Mitigation Guidelines for Denial-of-Service Attacks / CCRIC Rapport technique RT12-001: Principes de prévention contre les attaques par déni de service

-----Original Message-----
From: GOC-COG
Sent: February-23-12 12:34 PM
To: _GOC Distribution List / Liste de distribution du COG
Subject: CCIRC Technical Report TR12-001: Mitigation Guidelines for Denial-of-Service Attacks / CCRIC Rapport technique RT12-001: Principes de prévention contre les attaques par déni de service

(La version française suit)

PUBLIC SAFETY CANADA

CANADIAN CYBER INCIDENT RESPONSE CENTRE

****

Technical Report

****

Number: TR12-001

Date: 22 February 2012

****

Mitigation Guidelines for Denial-of-Service Attacks

****

AUDIENCE

This Information Report is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries. The recipients of this product may further distribute it to technical stakeholders within their organization.

PURPOSE

The purpose of this Information Report is to provide IT security personnel with an introduction to distributed denial-of-service (DDoS) attacks, their modus-operandi and the recommended steps to help with the preparation, identification, containment, recovery and continuous improvement efforts required to limit associated organizational risk. This document may be used by system administrators, computer security incident response teams (CSIRTS), IT security operations centres and other related technology groups.

INTRODUCTION

Denial of service (DoS) attacks are common malicious network actions aimed at disrupting the availability of computing resources from legitimate users. These types of attacks, especially DDoS attacks have recently gained in popularity due to the availability of DoS rental services from botnet operators, as well as the availability of various free and easy to use hacking tools. The latter have enabled activists using hacking to support their causes (also known as hacktivists) to efficiently recruit large numbers of followers to perpetrate cyber attacks, increasing both their distribution and power. Well known examples of DoS attacks include the use of the Low Orbit Ion Cannon DDoS tool in support of Wikileaks (Introduction to LOIC: http://en.wikipedia.org/wiki/LOIC) used by hacking group "Anonymous" and attacks against national infrastructures such as Korea (http://blogs.mcafee.com/mcafee-labs/malware-in-recent-korean-ddos-attacks-destroys-systems), Georgia (http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/) and Estonia (http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia).

DOS AND DDOS DEFINITION

A DoS attack is an attempt to make a computer resource unavailable to its intended users (Definition: http://en.wikipedia.org/wiki/Denial-of-service_attack). A DDoS attack occurs when multiple systems simultaneously flood networked computer resources, rendering them inaccessible. A DDoS attack, in contrast with a DoS attack, comes from many sources, often hundreds or even thousands. As a result, mitigation actions against a DDoS attack are more difficult to coordinate and associated traffic is more damaging to the target.

DDoS attacks often use stateless protocols such as UDP and ICMP, but stateful protocols can also be used when the connections are not fully established such as during a TCP SYN flood attack. Both techniques make it easier for the attacker to use spoofed IP addresses and harder to determine the source of the attack.

FIVE STEPS TO DEFEND AGAINST DDOS ATTACKS

Preparation:

Preparation is the most important step in defending against a DDoS attack. Clear and complete procedures and guidelines should be established well before an attack takes place. Any organization can fall victim to DDoS attacks, either directly or indirectly. Having a solid plan in place will help reduce the risk and lessen the impact should an attack occur.

Identification:

Indicators that your organization may be under a DDoS attack could include poor network performance, inaccessible services or system crashes. Being able to identify and understand the nature of the attack and its targets will help in the containment and recovery process. For this purpose, organizations require tools that provide visibility over their managed information technology (IT) infrastructure. Often, prior to a DDoS attack, a reconnaissance of the target is performed by the attacker. This may include scanning the target network for known exposed vulnerabilities or sending malformed packets to the target host to analyze changes in response time. This reconnaissance activity may be hard to detect, especially because it may take place well before the attack itself. A knowledgeable attacker will also ensure scan traffic does not meet the threshold required to trigger alarms from network monitoring tools. However, there may be available intelligence indicating an increased likelihood of a DDoS attack against an organization. Good examples are the Anonymous Operations (aka "anonops" (http://anonops.blogspot.com/2011/09/tar-sands-action-september-3-press_04.html)), which broadly advertise their motivation and targets.

Containment:

Having a pre-determined containment plan before an attack for a number of scenarios will significantly improve response speed and limit damages resulting from a DDoS attack. For example, the containment strategy for a mail server may differ from one for a web server. Underestimating the importance of this phase can result in mistakes and significant collateral damages. Therefore, understanding the nature of DDoS attacks and documenting the associated decision-making process is critical. An organization should clearly identify its network perimeter and exposed assets. Load balancers, modern firewall technologies (Deep Packet Inspection, proxy, application layer filtering), content caching, content hosting geographic diversity, dynamic DNS service and ISP-based DDoS protection services are some of the tools an organization may leverage to contain an ongoing DDoS attack.

Recovery:

Depending on the containment strategy employed and the sensitivity to its collateral impact, an organization may be under different pressure to recover from a DDoS attack. Understanding the characteristics of the attack is required for an appropriate recovery. DDoS may exploit limits in the following resources:

- Server queue length
- Server computing resources
- Client tolerance to level of service variability
- Bandwidth

A DDoS attack may exploit any or a combination of these limitations. An organization equipped with a flexible provisioning model for these resources may be able to rapidly adapt and sustain long-term DDoS attacks. However, some attacks may leverage vulnerabilities in protocols or software and achieve unexpected high impact as a result (http://www.theregister.co.uk/2011/08/24/devastating_apache_vuln/). An organization equipped with packet capture capability may be able to identify the delivery method of the attack and potentially design an accurate Intrusion Prevention System / Firewall signature. Despite mitigation efforts, some DDoS attacks may be persistent over time. An organization using connection logs and other tools may be able to provide a list of potentially offending IP addresses (if not spoofed) to their upstream ISP, law enforcement and national Computer Emergency Response Team (CERT) to coordinate mitigation/investigation of the offending sources.

Lessons Learned:

Lessons learned is a very important step that is often overlooked. Lessons learned activities should take place as soon as possible following an incident. All decisions and steps taken throughout the incident handling cycle should be reviewed. All procedures should be reviewed to see where improvements may be made.

Perhaps the most challenging part of performing a Lessons Learned review involves documenting the impact and cost the incident caused to the organization. Although time consuming, this step is essential to allow organizations to properly justify security resources and assess their return on investment. Damages to an organization include tangible metrics, such as loss in sales and productivity, as well as intangible metrics, such as reputation and brand.

By performing this review after each incident, organizations will enable continuous improvement and potentially significant reduction in the impact of incidents.

CHECKLIST

The following checklist is intended to help organizations during the various mitigation phases of DDoS attacks. Many of these mitigations are applicable to other types of cyber attacks as well and should be considered accordingly.

Preparation:

1. Identify your most critical assets and the services they provide.

- Are they up to date with the latest patches?
- Do they run any unnecessary services such as Telnet or FTP?

2. Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.

3. Establish 24/7 contact information for your ISP and alternate methods for communications.

4. Deny all obviously spoofed traffic (e.g., internal IP addresses that should not be coming in or going out of your network). Implement a bogon block list (unallocated address space) at the network boundary.

5. Establish procedures on how to segregate your networks in the event of a DDoS attack. Use existing network devices, such as routers and managed switches, to defend against DDoS attacks. Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls.

6. Disable all unnecessary services and restrict access to and from all previously identified critical hosts based on DDoS traffic characteristics.

7. Create a whitelist of the source IPs you must allow if you need to prioritize traffic during an attack.

8 Document your network topology including all IP addresses. Keep it up to date.

9. Review your Business Continuity Plan (BCP) and ensure senior management and legal team understand the significance of a DDoS attack, including their roles.

10. Understand "normal." Establish a baseline of network traffic, CPU usage, connection and memory utilization of critical hosts under normal conditions so that network monitoring tools will trigger on abnormal changes.

11. Acknowledge that your organization may be attacked. Organizations should consider the development and implementation of policies, plans and procedures to defend against DDoS attacks. Identify and plan for resources to implement these plans.

12. Assign roles and responsibilities. Identify who plays a role in defending against a DDoS attack and ensure they are aware of this responsibility. This should include personnel from critical business functions, IT operations, network and IT security teams, legal advisors, and media relations staff. Ensure an up-to-date point-of-contact list with primary and alternate personnel is maintained. As the network may be unavailable, including mobile devices, ensure alternate communications mechanisms are in place.

13. Conduct exercises. The worst time to test plans and procedures is during an attack.

Identification:

1. Determine if you are the primary target or a collateral victim. (ex: is your upstream internet provider or content hosting provider the target ?)

2. Understand the logical flow of the attack.

3. Determine what type of traffic is being used, such as IP addresses, ports and protocols.

4. Consider using network analysis tools to determine the type of traffic being used in the attack (e.g., TcpDump, Wireshark, Snort).

5. Review any available logs to understand the attack and what is being targeted.

6. Notify appropriate personnel. This may include senior management and the legal team.

Containment:

1. Contact your ISP to implement filtering.

2. Block the traffic as close to the network cloud as possible (router, firewall, load balancer, etc.).

3. Relocate the target to another IP address if a particular host is being targeted. This is a temporary solution.

4. If a particular application is being targeted, consider disabling it temporarily.

5. Identify and correct the vulnerability or weakness that is being exploited. An example of this may be an unused service that is accidently left enabled on a public facing device or unpatched operating system.

6. Implement filtering based on the characteristics of the attack. An example may be blocking IMCP echo packets.

7. Implement rate limiting for certain protocols, allowing a certain number of packets per second for a specific protocol or to access a certain host.

Recovery:

1. Confirm that the DDoS attack has finished and services are reachable again.

2. Confirm that your networks are back to your baseline performance.

3. If necessary, patch and update all affected machines.

4. If possible, identify the source of the attack. Enlist the help of your ISP.

5. Review logs for signs of reconnaissance. Maintain logs for possible future law enforcement requirements.

Lessons Learned:

1. Create or update the following documents:

- Standard Operating Procedures
- Emergency Operating Procedures
- Business Continuity Plans

RECOMMENDATIONS

CCIRC recommends that organizations assess their risk exposure to Denial of Service attacks which may be caused accidentally or intentionally and consider mitigation advice herein provided and implement them as appropriate for the specific IM/IT environment.

REFERENCES

1. US-CERT, Understanding Denial-of-Service Attacks

http://www.us-cert.gov/cas/tips/ST04-015.html

2. NIST, Computer Security Incident Handling Guide

http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

3. GovCERT.NL, Factsheet: Protect your online services against dDoS attacks

http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html

4. Societe Generale DDoS Incident Reponse

http://cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf

REPORTING

Any Canadian Critical Infrastructure Operator wishing to report incidents may do so using the CCIRC Cyber Duty Officer PGP encryption key, found at:

http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx

Associated reports should be sent to: s.16(2)(c)

cyberdo@ps-sp.gc.ca.

Potentially malicious files/samples may be shared with CCIRC by sending them zipped and protected with the password [redacted] via email to:

[redacted]

CRITICAL NOTE:

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

NOTE TO READERS

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118

Fax: 613-998-9589

Email: communications@ps-sp.gc.ca

For urgent matters please contact the GOC.

SÉCURITÉ PUBLIQUE CANADA

CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

****

Rapport technique

****

Numéro : TR12-001

Date : 22 février 2011

****

Principes de prévention contre les attaques par déni de service

****

PUBLIC CIBLE

Le présent rapport d'information est rédigé à l'intention des professionnels et gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales, ainsi que des industries à infrastructure critique et autres industries connexes. Les personnes ayant obtenu le présent produit peuvent le divulguer aux intervenants techniques dans leur organisme.

OBJECTIF

Ce rapport d'information renseigne le personnel chargé de la sécurité informatique sur les attaques par déni de service distribué (DSD) et leur modus operandi. Il décrit la procédure recommandée pour faciliter les étapes de préparation, d'identification, de confinement et de reprise des services, ainsi que les efforts d'amélioration que l'organisation doit déployer en tout temps pour limiter les risques de s'exposer à telles attaques. Ce document est destiné aux administrateurs de système, aux équipes d'intervention en cas d'incident informatique (EIII), aux Centres des opérations de sécurité informatique et aux autres groupes technologiques concernés.

PRÉSENTATION

Dirigées contre les réseaux, les attaques par déni de service sont des actions malveillantes répandues visant à empêcher les utilisateurs légitimes d'avoir accès à des ressources informatiques. Ces actions, en particulier les attaques par déni de service distribué (DSD), se sont récemment multipliées en raison de la disponibilité des services de déni de service loués par des zombimestres (des opérateurs de réseaux d'ordinateurs zombies) et de l'accès à de nombreux outils de piratage gratuits et faciles à utiliser. Ces outils ont permis aux « hacktivistes », des activistes qui font appel au piratage informatique – le hacking – pour défendre leur cause, de lever efficacement une armée de partisans qui appuient et facilitent leurs cyberattaques, leur permettant ainsi d'étendre leur réseau de distribution et d'accroître leur pouvoir. Parmi les attaques par déni de service les plus connues, on retrouve celle du groupe de pirates informatiques Anonymous avec l'application LOIC (Low Orbit Ion Cannon) pour appuyer Wikileaks (Présentation de l'application LOIC : http://fr.wikipedia.org/wiki/LOIC) et des attaques DSD contre les infrastructures nationales de la Corée (http://blogs.mcafee.com/mcafee-labs/malware-in-recent-korean-ddos-attacks-destroys-systems (en anglais)), de la Géorgie (http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/ (en anglais)) et de l'Estonie (http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia (en anglais).

DÉNI DE SERVICE ET DÉNI DE SERVICE DISTRIBUÉ – DÉFINITIONS

Une attaque par déni de service est une attaque ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser (Définition : http://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service). Une attaque par déni de service distribué (DSD) se produit lorsqu'une multitude de systèmes « inondent » de diverses requêtes simultanées les ressources d'un réseau informatique, rendant ces dernières inaccessibles. Contrairement aux attaques par déni de service, les attaques DSD ne sont pas perpétrées par un seul attaquant, mais bien des centaines, voire des milliers. Il est donc plus difficile de coordonner les mesures d'atténuation pour les contrer, et le trafic qu'elles génèrent endommage encore plus l'infrastructure ciblée.

Les attaques DSD reposent souvent sur l'exploitation de protocoles sans état, tel UDP et ICMP, mais utilisent également des protocoles avec état lorsque les connexions sont rendues instables par une attaque par saturation de type TCP SYN. Les deux techniques facilitent l'usurpation d'adresses IP tout en brouillant les pistes menant à l'origine des attaques.

CINQ ÉTAPES POUR SE PROTÉGER DES ATTAQUES DSD

Préparation:

La préparation est l'étape la plus importante de la défense contre les attaques DSD. Il faut établir une série exhaustive de procédures et de lignes directrices claires avant qu'elles ne surviennent. Toute organisation peut être victime d'attaques DSD directes ou indirectes. Elle doit donc instaurer un plan de protection rigoureux pour réduire les risques et atténuer les effets de ces attaques.

Identification:

Une attaque DSD se manifeste entre autres choses par le piètre rendement du réseau, des services indisponibles et des pannes de système. La capacité à la reconnaître, à en comprendre la nature et à en identifier les cibles facilite le processus de confinement et la reprise des services. C'est pourquoi chaque organisation a besoin d'outils qui lui permettent de voir l'ensemble de son infrastructure de technologie de l'information gérée. L'attaquant effectue souvent une reconnaissance du réseau ciblé avant de lancer une attaque DSD contre lui. Il cherchera ainsi à y déceler des vulnérabilités connues ou à y envoyer des paquets mal formés pour analyser les changements du temps de réaction. Une telle activité de reconnaissance s'avère parfois difficile à détecter, surtout parce qu'elle précède longtemps à l'avance l'attaque proprement dite. Un attaquant chevronné s'assurera également de limiter le trafic servant à l'analyse ne dépasse pas le seuil de déclenchement des alarmes par des outils de surveillance du réseau. Cependant, l'organisation peut avoir accès à de l'information qui l'informe d'une recrudescence des risques d'attaques DSD dirigées conte elle. Un exemple bien connu : les opérations du collectif Anonymous (ou anonops (http://anonops.blogspot.com/2011/09/tar-sands-action-september-3-press_04.html)) qui fait largement étalage de ses intentions et de ses cibles.

Confinement:

Un plan de confinement comportant divers scénarios et établi au préalable réduit considérablement le temps de réaction à une attaque DSD et l'étendue des dommages. Ainsi, on n'appliquera pas la même stratégie de confinement au serveur de courriel et au serveur Web. Négliger cette étape de la défense se traduit par des erreurs et d'importants dommages collatéraux. Il est donc crucial de bien comprendre la nature des attaques DSD et de documenter les processus décisionnels afférents. L'organisation doit identifier clairement le périmètre de son réseau et dresser la liste exhaustive des ressources exposées. Une organisation tirera profit de divers outils lui permettant de confiner une attaque DSD en cours, comme des équilibreurs de charge, des dispositifs pare-feu modernes (inspection approfondie des paquets, les serveurs mandataires, filtrage d'application), la mise en antémémoire du contenu, la diversité géographique des sites d'hébergement du contenu, le service DNS dynamique et les services de protection contre les attaques DSD fournis par les fournisseur d'accès Internet (FAI).

Reprise des services:

La pression exercée sur l'organisation pour qu'elle assure la reprise de ses services à la suite d'une attaque DSD varie en fonction de sa stratégie de confinement et de sa fragilité aux dommages collatéraux. Elle doit donc savoir reconnaître les caractéristiques d'une telle attaque pour assurer une reprise adéquate de ses services. L'attaque DSD tire profit des limites des ressources suivantes :

- Longueur de la file d'attente du serveur
- Ressources informatique du serveur

- Tolérance du client aux variations du niveau de service
- Bande passante

Les attaques DSD exploitent l'une ou l'autre de ces limites, ou plusieurs d'entre elles à la fois. Si l'organisation a appliqué un modèle souple de service à la demande à ces ressources, elle pourra s'adapter rapidement et résister à des attaques SDS soutenues. En revanche, certaines attaques profiteront des vulnérabilités des protocoles ou des logiciels pour causer d'importants dommages impossibles à prévoir (http://www.theregister.co.uk/2011/08/24/devastating_apache_vuln/). L'organisation qui s'est dotée d'un mécanisme de capture des paquets sera en mesure de comprendre le mode de prestation de l'attaque et de concevoir une solution efficace combinant système de prévention des intrusions et dispositif pare-feu. Certaines attaques DSD se poursuivront malgré les mesures d'atténuation en place. Pour assurer la coordination des mesures d'atténuation et permettre d'enquêter sur les sources criminelles, l'organisation utilisera ses journaux de session et d'autres outils pour signaler à son FAI en amont, aux services de police et à l'Équipe nationale d'intervention d'urgence en informatique (EIUI) les adresses IP suspectes – si elle n'ont pas été usurpées – qui pourraient avoir servi à perpétrer de telles attaques.

Leçons retenues:

Cette étape essentielle de la défense est trop souvent omise. Il faut faire le point le plus rapidement possible à la suite d'un incident et examiner chacune de décisions et des mesures prises tout au long de la gestion de la crise. Cet exercice permet de cerner ce qui doit être amélioré dans les procédures appliquées.

L'examen des leçons retenues comporte un volet particulièrement difficile à réaliser : la documentation des répercussions de l'incident sur l'organisation et les coûts qu'il représente. Bien qu'elle prenne beaucoup de temps, cette étape est essentielle puisqu'elle permet à l'organisation de justifier adéquatement l'acquisition de ressources de sécurité et de bien évaluer le rendement du capital investi. Les dommages subis par l'organisation se mesurent quantitativement d'une part, par exemple le volume de ventes perdues et la baisse de la productivité, et d'autre part qualitativement, quand la réputation et l'image de marque sont entachées.

L'examen systématique des leçons retenues permet à l'organisation de s'améliorer sans cesse et de réduire considérablement les répercussions négatives des incidents.

LISTE DE CONTRÔLE

La liste de contrôle ci-dessous facilite la prise de mesures d'atténuation durant les diverses phases d'une attaque DSD. Bon nombre de ces mesures s'appliquent également aux autres types d'attaques cybernétiques et doivent être envisagées en conséquence.

Préparation:

1. Identifier les ressources matérielles les plus cruciales et les services dont elles assurent la prestation.

- Les derniers correctifs ont-ils été installés?
- Exécutent-elles des services inutiles comme Telnet, FTP, etc.?

2. De concert avec le fournisseur d'accès Internet (FAI), établir des procédures pour connaître l'étendue du soutien qu'il peut apporter à l'organisation lorsqu'elle fait l'objet d'une attaque DSD. Savoir s'il existe un accord sur les niveaux de services (ANS) et connaître les coûts à assumer.

3. Dresser la liste des personnes-ressources du FAI que l'on peut joindre en tout temps, ainsi que des autres moyens de communiquer avec elles.

4. Bloquer tout trafic qui présente des signes évidents d'usurpation d'identité (p. ex., les adresses IP à l'intérieur du réseau de l'organisation qui ne devraient pas être associées à du trafic entrant ou sortant). Instaurer une liste de filtrage Bogon (plage d'adresses non allouées) au périmètre du réseau.

5. Établir des procédures sur la façon de cloisonner les réseaux de l'organisation en cas d'attaque DSD. Se servir des appareils existants, comme les routeurs et les commutateurs gérés, pour s'en protéger. Dans la mesure du possible, configurer les routeurs du périmètre pour filtrer les services afin de réduire la charge imposée aux dispositifs de sécurité, tels les pare-feu, qui analysent le trafic.

6. Désactiver tout service inutile et bloquer tout accès non autorisé vers et depuis les hôtes critiques identifiés précédemment.

7. Créer une liste blanche des adresses IP source s'il est nécessaire d'établir un trafic prioritaire durant une attaque.

8. Documenter la topologie de réseau, y compris toutes les adresses IP. Tenir cette information à jour.

9. Passer en revue plan de continuité des opérations (PCO) de l'organisation et s'assurer que la haute direction et le service du contentieux comprennent bien ce qu'est une attaque DSD et les rôles et responsabilités qui leur sont dévolus.

10. Comprendre ce que constituent des conditions normales. Établir le niveau de référence du trafic sur le réseau, de la charge de travail imposée aux processeurs, de l'utilisation des connexions et de la mémoire des hôtes essentiels en situation normale afin que les outils de surveillance du réseau entrent en œuvre lorsqu'une variation anormale se produit.

11. Reconnaître que l'organisation peut être attaquée. Solliciter la direction afin d'obtenir son approbation en vue d'élaborer et de mettre en œuvre des politiques, plans et procédures pour se défendre contre les attaques DSD. Identifier et obtenir les ressources nécessaires pour mettre en œuvre ces politiques, plans et procédures.

12. Attribuer les rôles et responsabilités. Connaître les intervenants dans la défense contre les attaques DSD et s'assurer qu'ils sont au fait de cette responsabilité. Ces personnes devraient appartenir au personnel affecté aux fonctions opérationnelles essentielles, aux opérations de TI, à la sécurité des réseaux et des TI, au service du contentieux et aux relations publiques. Tenir à jour la liste des points de contacts primaires et secondaires. Le réseau étant susceptible d'être en panne, y compris les appareils mobiles, mettre également en place d'autres mécanismes de communication.

13. Effectuer des exercices. Ce n'est plus le temps de faire l'essai des plans et des procédures lorsqu'une attaque se produit.

Identification:

1. Savoir si l'organisation est une victime ciblée ou accidentelle. (P. ex., la cible est-elle le fournisseur d'accès Internet (FAI) en amont ou le fournisseur de services d'hébergement de contenu?)

2. Comprendre le déroulement logique de l'attaque.

3. Déterminer le trafic dont se sert l'attaquant en identifiant les adresses IP, les ports et les protocoles qu'il exploite.

4. Envisager de recourir à des outils d'analyse du réseau pour déterminer le type de trafic qu'exploite l'attaquant (p. ex., TcpDump, Wireshark, Snort).

5. Consulter les journaux de serveur pour comprendre le fonctionnement de l'attaque et les cibles visées.

6. Aviser le personnel concerné, notamment celui de la haute direction et du service du contentieux.

Confinement:

1. Communiquer avec le FAI pour mettre en place un mécanisme de filtrage du trafic.

2. Bloquer le trafic le plus près possible du réseau en nuage (p. ex., avec un routeur, un pare-feu, un équilibreur de charges).

3. Changer l'adresse IP de l'hôte ciblé par l'attaque. Il s'agit là d'une solution provisoire.

4. Si l'attaque vise une application en particulier, envisager sa désactivation temporaire.

5. Identifier et corriger la vulnérabilité ou la faiblesse du système qui est exploitée. Il peut s'agir par exemple d'un service inutilisé maintenu involontairement en activité sur un dispositif destiné au public ou d'un système d'exploitation dont les correctifs n'ont pas été installés.

6. Mettre en place un mécanisme de filtrage en fonction des caractéristiques de l'attaque, par exemple le blocage des paquets IMCP Echo.

7. Limiter le trafic de certains protocoles à un nombre quelconque de paquets par seconde ou en n'autorisant l'accès des paquets qu'à certains hôtes.

Reprise des services:

1. Confirmer que l'attaque DSD a pris fin et que les services sont de nouveau disponibles.

2. Confirmer que le niveau de performance de référence des réseaux est rétabli.

3. Au besoin, installer les correctifs et les mises à jour sur les machines touchées.

4. Dans la mesure du possible, identifier l'origine de l'attaque. Solliciter l'aide du FAI.

5. Passer en revue les registres de journalisation pour y repérer la trace des tentatives de reconnaissance. Conserver ces registres en vue d'éventuelles poursuites judiciaires.

Leçons retenues:

1. Rédiger ou mettre à jour les documents suivants :

- Procédures d'opération normalisées
- Procédures d'opération d'urgence
- Plans de continuité des opérations

RECOMMANDATIONS

Le CCRIC recommande aux organisations d'évaluer les risques qu'elles soient exposées à des attaques par déni de service, qu'elles soient provoquées accidentellement ou volontairement. Elles sont invitées à prendre en considération les mesures d'atténuation conseillées dans le présent document et de les mettre en œuvre en fonction de leur propre environnement de GI-TI.

RÉFÉRENCES

1. US-CERT, Understanding Denial-of-Service Attacks (Comprendre les attaques par déni de service)

http://www.us-cert.gov/cas/tips/ST04-015.html (en anglais)

2. NIST, Computer Security Incident Handling Guide (Guide de gestion des incidents touchant la sécurité informatique)

http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf (en anglais)

3. GovCERT.NL, Factsheet: Protect your online services against dDoS attacks (Protégez vos services en ligne contre les attaques DSD)

http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html (en anglais)

4. CERT Société Générale – Déni de service distribué

http://cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf (en anglais)

s.16(2)(c)

SIGNALEMENT

Les opérateurs d'infrastructure critique canadiens peuvent signaler des incidents en utilisant la clé de chiffrement PGP de l'agent de cybersécurité de service du CCRIC (disponible à l'adresse http://www.publicsafety.gc.ca/prg/em/ccirc/enc-fra.aspx) et transmettre les rapports connexes par courriel à l'adresse cyberdo@ps-sp.gc.ca.

Les fichiers et échantillons potentiellement malveillants peuvent être envoyés au CCRIC à l'adresse : [redacted] Les fichiers et courriels douteux devraient être compressés et protégés avec le mot de passe [redacted]

NOTE CRUCIALE

Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à avertir le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique,

notamment l'exploration, le téléchargement, le balayage, ou même une recherche Web selon tout texte du présent rapport.

AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Le présent message et toutes les pièces jointes qui l'accompagnent contiennent des renseignements qui peuvent avoir été recueillis de diverses sources externes dont le CCRIC ne peut vérifier ni la fiabilité ni l'intégrité. Le CCRIC n'assume aucune responsabilité pour des conséquences négatives résultant de l'utilisation des renseignements fournis dans la présente.

Les liens vers d'autres sites Web ne relevant pas du gouvernement du Canada sont fournis aux utilisateurs uniquement pour des raisons de commodité. Le gouvernement du Canada n'assume donc pas la responsabilité de l'exactitude, du caractère actuel ni de la fiabilité de leur contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites et leur contenu.

AVIS AUX LECTEURS

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la réponse aux incidents. Le CCRIC est responsable d'assurer la résilience de l'infrastructure essentielle nationale en contrôlant les menaces et en coordonnant une réponse fédérale aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement à l'égard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements de nature générale, veuillez communiquer avec la division des Affaires publiques de l'organisme.

Téléphone : 613-944-4875 ou 1-800-830-3118

Télécopieur : 613-998-9589

Courriel : communications@ps-sp.gc.ca

En cas d'urgence, veuillez communiquer avec le Centre des opérations du gouvernement (GOC).

Government Operations Centre/

Centre des opérations du gouvernement
Email/courriel: [redacted]

s.16(2)(c)

Dvorkin, Corey

From: Barr, Corri <Corri.Barr@tbs-sct.gc.ca>
Sent: April-18-12 4:11 PM
To: Dvorkin, Corey
Subject: FW: Pour Info: Anonymous targets more government Web sites

Corri Barr
Director, Parliamentary and Cabinet Affairs | Directrice des affaires parlementaires et du cabinet.
Strategic Communications, Media and Parliamentary Relations | Communications stratégiques, médias et relations parlementaires
Strategic Communications and Ministerial Affairs | Communications stratégiques et affaires ministérielles
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Corri.Barr@tbs-sct.gc.ca
Telephone | Téléphone 613-952-1693 / Facsimile | Télécopieur 613-941-4000 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

From: Le Gras, Gilbert
Sent: April 18, 2012 4:10 PM
To: Barr, Corri
Subject: FYI: Pour Info: Anonymous targets more government Web sites

I've already forwarded to my Cyber Security clients, thought you'd be interested.

From: Marleau, Patrick
Sent: April 18, 2012 4:08 PM
To: Le Gras, Gilbert
Subject: Pour Info: Anonymous targets more government Web sites

Je ne sais si ceci sera d'intérêt ou non pour toi. Je te l'envoie au cas où.

Anonymous targets more government Web sites

By: Sophie Curtis On: **18 Apr 2012** For: **Techworld.com**

LONDON -- Hacktivist group Anonymous is staging a second wave of distributed denial-of-service (DDoS) attacks on government websites. It began by hitting Britain's electronics spy agency and...

LONDON -- Hacktivist group Anonymous is staging a second wave of distributed denial-of-service (DDoS) attacks on government websites. It began by hitting Britain's electronics spy agency and Home Office Web sites over the weekend, and moved on to other sites including MI6, the British international spy agency, yesterday.

U.S. government sites, including those of the CIA, Department of Justice, FBI and NASA have also come under attack this week.

The Home Office admitted in a statement that its Web site was targeted by protesters on Saturday night, resulting in intermittent interruption to the service.

"We had measures in place to protect the site, which is now running normally," a spokesperson told Techworld. "The site was not hacked and no other Home Office systems were affected."

The attack follows an earlier attempt to bring down the Web sites of 10 Downing Street and the Home Office over the Easter bank holiday weekend. The attacks were conducted under the banner #OpTrialAtHome, and were reportedly launched in support of Pentagon hacker Gary McKinnon and TVShack's Richard O'Dwyer, who face extradition from the UK to the United States.
Graham Cluley, senior technology consultant at Sophos, described the first attack as an "audacious move by Anonymous and its supporters," warning that other hacktivists who have launched DDoS attacks against websites belonging to British authorities - such as Ryan Cleary - have been arrested.

Meanwhile, Britain's Government Communications Headquarters (GCHQ), the signals intelligence agency, appears to have headed off a similar attempt by Anonymous to knock its website offline.

The organization claims it has "reasonable and proportionate information assurance measures in place to protect the site". However, its defences will be tested once again on 21 April, when Anonymous is threatening to launch another attack.

Both of these attacks were announced via the Anonymous Operations Twitter account, which seems to have become the primary mode of communication for the hacktivist collective. The account was also used yesterday to claim responsibility for bringing down the MI6 site in the U.K., as well as the CIA and Department of Justice sites in the U.S.

These attacks were initially claimed by a hacker from Brazil who goes by the Twitter handle @Havittaja, who claimed the attacks were done for the "lulz". However, Havittaja also advocates freedom for fellow "Anons" currently facing incarceration for their participation in previous Anonymous operations.

"It's all of us together," the Anonymous group stated on its Facebook page. "We are the 'little people', the hungry, the poor, the 'manipulated', and yet for all their power and might, these 'little people' brought their pride down."

Organizations that have successfully resisted attacks by Anonymous are understandably reluctant to reveal details of the security measures they have in place to defend against DDoS, for fear of making themselves an easy target. However, Anonymous hackers do tend to vary their methods until they find one that works.

Earlier this year, security firm Imperva published a detailed analysis of an attack by Anonymous on one of its customers, providing new insight into how the hacktivist group operates. The New York Times revealed that the target in question was the Vatican, and a week later the Vatican website was brought down in a repeat attack.

(From Techworld.com)

Patrick Marleau
Communications Officer | Agent des communications
Strategic Communications and Parliamentary Relations | Communications stratégiques et relations parlementaires
Strategic Communications and Ministerial Affairs | Communications stratégiques et affaires ministérielles
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Patrick.Marleau@tbs-sct.gc.ca
Telephone | Téléphone 613-946-6294 ***Hard of hearing - Malentendant
Facsimile | Télécopieur 613-952-3658 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

CYBERDO

From: CYBERDO
Sent: April-18-12 11:40 AM
To: Beaudoin, Luc; Billard, Sheldon; Breault, Stephen; Moore, Bruce; Murphy, Gregg; Phlek, Vireak; Williston, Sandra
Subject: Anonymous offers alternative to Pastebin.com

Summary: The Anonymous hacking collective has launched a new site that it claims will allow users to post material without fear of being tracked down.
AnonPaste offers 256-bit AES encryption at the browser layer. All data posted to the site will be encrypted and decrypted in the browser so no "usable paste data [is] stored on the server for the authorities or anyone else to seize," the statement claimed.

http://www.computerworld.com/s/article/9226322/Anonymous_offers_alternative_to_Pastebin.com?taxonomyId=17

[redacted]

From: Billard, Sheldon
Sent: April-13-12 10:34 AM
To: * CyberIH; [redacted]
Cc: Klassen, Nathan
Subject: Anonymous Handbook

s.16(2)(c)

Found on Pastebin.com

http://pastebin.com[redacted]

Sheldon Billard

Canadian Cyber Incident Response Centre | canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Ottawa, Ontario, Canada K1A 0P8
Telephone | Téléphone 613-991-7056
Facsimile | Télécopieur 613-991-3574
Government of Canada | Gouvernement du Canada

Dvorkin, Corey

From: Bradley, Kees
Sent: April-05-12 11:23 AM
To: Araneta, Allison; Bonvie, Jeff; Mohammed, Melanie; Dvorkin, Corey; Lahey, Daniel; Anderson, Ian
Subject: Anonymous hacks local Chinese sites

http://blogs.wsj.com/chinarealtime/2012/04/04/anonymous-hacks-chinese-government-websites/

CYBERDO

From:	CYBERDO	s.15(1) - Int'l
Sent:	April-05-12 1:17 PM	s.16(2)(c)
To:	[redacted]	
Cc:	CYBERDO	
Subject:	RE: [redacted] targeted by Anonymous [CCIRC CE12-002744]	
Importance:	High	

Thanks [redacted] - I'll pass that along to [redacted]

For your SA, attacks have continued even up to present time from a relatively small number of IP addresses. We have conducted an assessment of the scripts posted to Pastebin (see below for details). We've obtained logs on all attackers and interesting to note differences between IP addresses who are using the script in default mode (script kiddies) and other IP addresses who have modified the script and are [redacted] which means that the level of the attack is a bit more sophisticated (but not by much, because it is quite easy to modify the HOIC script).

The IPs we note who are participating in the attack and have modified the script in some way are:

[redacted]

Page 2245

is withheld pursuant to section

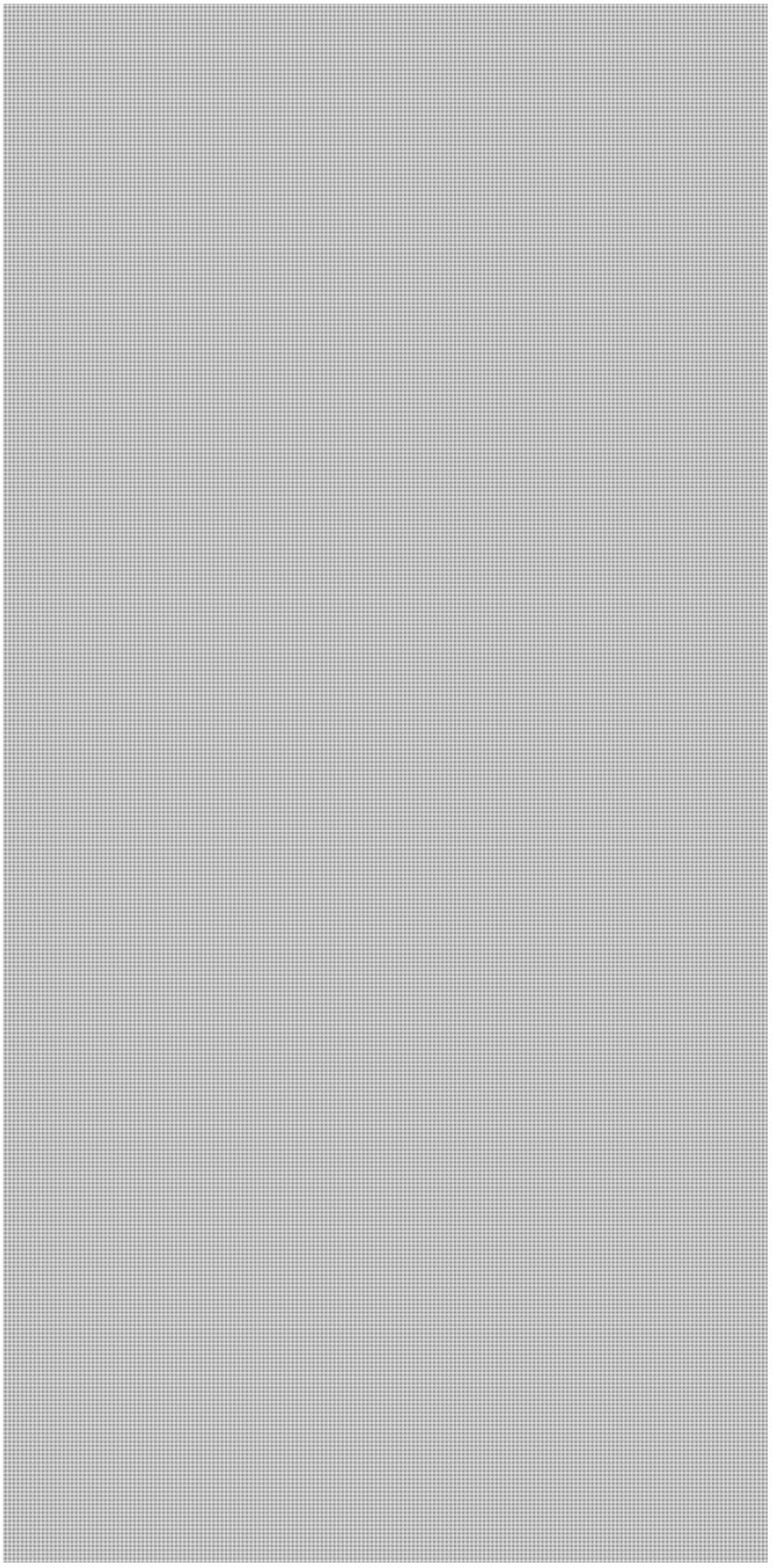
est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

s.16(2)(c)



Thanks again for your notification and sharing of this information. Great example of the usefulness of these types of exchanges when handled in real time.

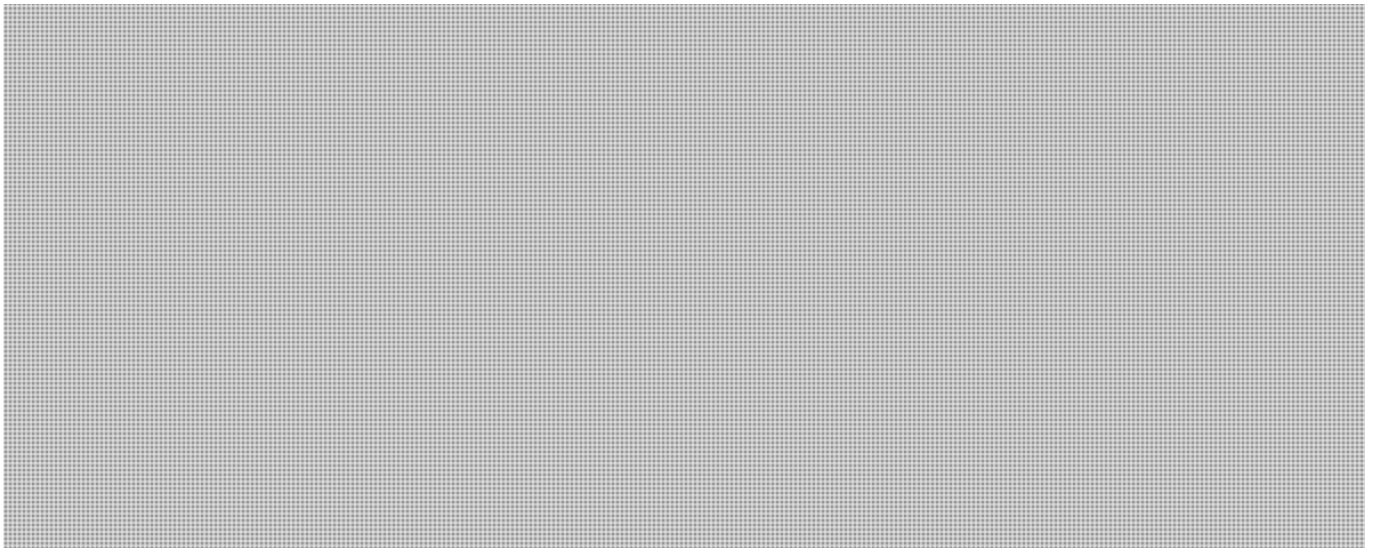
CYBERDO

From: Beaudoin, Luc
Sent: April-20-12 6:06 PM
To: CYBERDO
Subject: Anonymous op list on pastebin

s.16(2)(c)

For info (event-activity type)

ANONYMOUS
OPERATION DEFENSE
Objective: Combat CISPA
#OpDefense
*DON'T FORGET YOUR GUY FAWKES MASKES!!"



Full post at: http://pastebin.com/

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

CYBERDO

From: CYBERDO
Sent: April-20-12 11:06 AM
To: [redacted]
Subject: Has this been caught by anyone yet?

http://pastebin.com/[redacted]

Here's the first little bit of the paste: s.16(2)(c)

[redacted]

Page 2249

is withheld pursuant to section

est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

CYBERDO

From: Anderson, Windy
Sent: April-18-12 1:44 PM
To: CYBERDO
Subject: FW: Anonymous Dox's [redacted]

s.15(1) - Int'l
s.19(1)

fyi

Have a great day,

Windy

Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
windy.anderson@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Dick, Robert
Sent: April-18-12 10:44 AM
To: Beaudoin, Luc; Anderson, Windy
Subject: Fw: Anonymous Dox's [redacted]

Want me to keep passing these to you?

From: [redacted]
Sent: Wednesday, April 18, 2012 10:42 AM
To: [redacted]; GOC-COG; Darren.Sabourin@rcmp-grc.gc.ca <Darren.Sabourin@rcmp-grc.gc.ca>; [redacted]; Dick, Robert; 'Scott Foster' (Scott.Foster@rcmp-grc.gc.ca) <Scott.Foster@rcmp-grc.gc.ca>; [redacted] 'Tiago Alves de Jesus' (Tiago.Dejesus@rcmp-grc.gc.ca) <Tiago.Dejesus@rcmp-grc.gc.ca>; [redacted]; tim.oneil@rcmp-grc.gc.ca <tim.oneil@rcmp-grc.gc.ca>
Subject: Anonymous Dox's [redacted]

[redacted]

[redacted]

The posting of [redacted] Dox is at http://pastebin.com/[redacted]

[redacted]

s.15(1) - Int'l
s.16(2)(c)
s.19(1)

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

s.15(1) - Int'l
s.16(2)(c)
s.19(1)

-----Original Message-----
From: [redacted]
Sent: April-05-12 12:42 PM
To: CYBERDO
Subject: RE: [redacted] targeted by Anonymous [CCIRC CE12-002744]

Bruce,

Follow up. The researcher said [redacted] could contact her direct (if needed):

[redacted]

Regards,

[redacted]

-----Original Message-----
From: CYBERDO [mailto:[redacted]
Sent: Tuesday, April 03, 2012 12:42 PM
To: [redacted]
Cc: CYBERDO
Subject: RE: [redacted] targeted by Anonymous [CCIRC CE12-002744]
Importance: High

Thanks again - I'll pass along to [redacted] for further investigation.

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

-----Original Message-----
From:
Sent: April-03-12 1:36 PM
To: CYBERDO
Subject: RE: targeted by Anonymous [CCIRC CE12-002744]

s.15(1) - Int'l
s.16(2)(c)

Bruce,

The researcher passed this along as well.

http://pastebin.com/

They said that the post was labeled

Regards,

-----Original Message-----
From: CYBERDO [mailto
Sent: Tuesday, April 03, 2012 12:26 PM
To:
Cc: CYBERDO
Subject: RE: targeted by Anonymous [CCIRC CE12-002744]
Importance: High

- for your SA, the report their website is currently under DDoS. Thanks for the heads-up.

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

-----Original Message-----
From: CYBERDO
Sent: April-03-12 12:32 PM
To:
Cc: CYBERDO
Subject: RE: targeted by Anonymous [CCIRC CE12-002744]

Good Afternoon

Many thanks for this - I've assigned event number CE12-002744 to this report.

We'll notify the for SA.

Bruce Moore

Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

s.15(1) - Int'l
s.16(2)(c)

-----Original Message-----
From: [redacted]
Sent: April-03-12 12:16 PM
To: Moore, Bruce
Subject: [redacted] targeted by Anonymous

Bruce,

Came across this today from a security researcher.

Anonymous targeting [redacted]

http://pastebin.com[redacted]

http://pastebin.com[redacted]

Thought you guys would want to know.

Regards,

[redacted]

CYBERDO

From: CYBERDO
Sent: April-05-12 11:58 AM
To:
Cc: CYBERDO
Subject: CCIRC CE12-002744 [Analysis Report]

s.16(2)(c)
s.19(1)

Importance: High

Hi again

CCIRC technical analysis completed of the Indicators have been identified that could assist in filtering from "lazy" attackers (script kiddies who have not modified the original script).

Analysis summary:

s.16(2)(c)

[redacted]

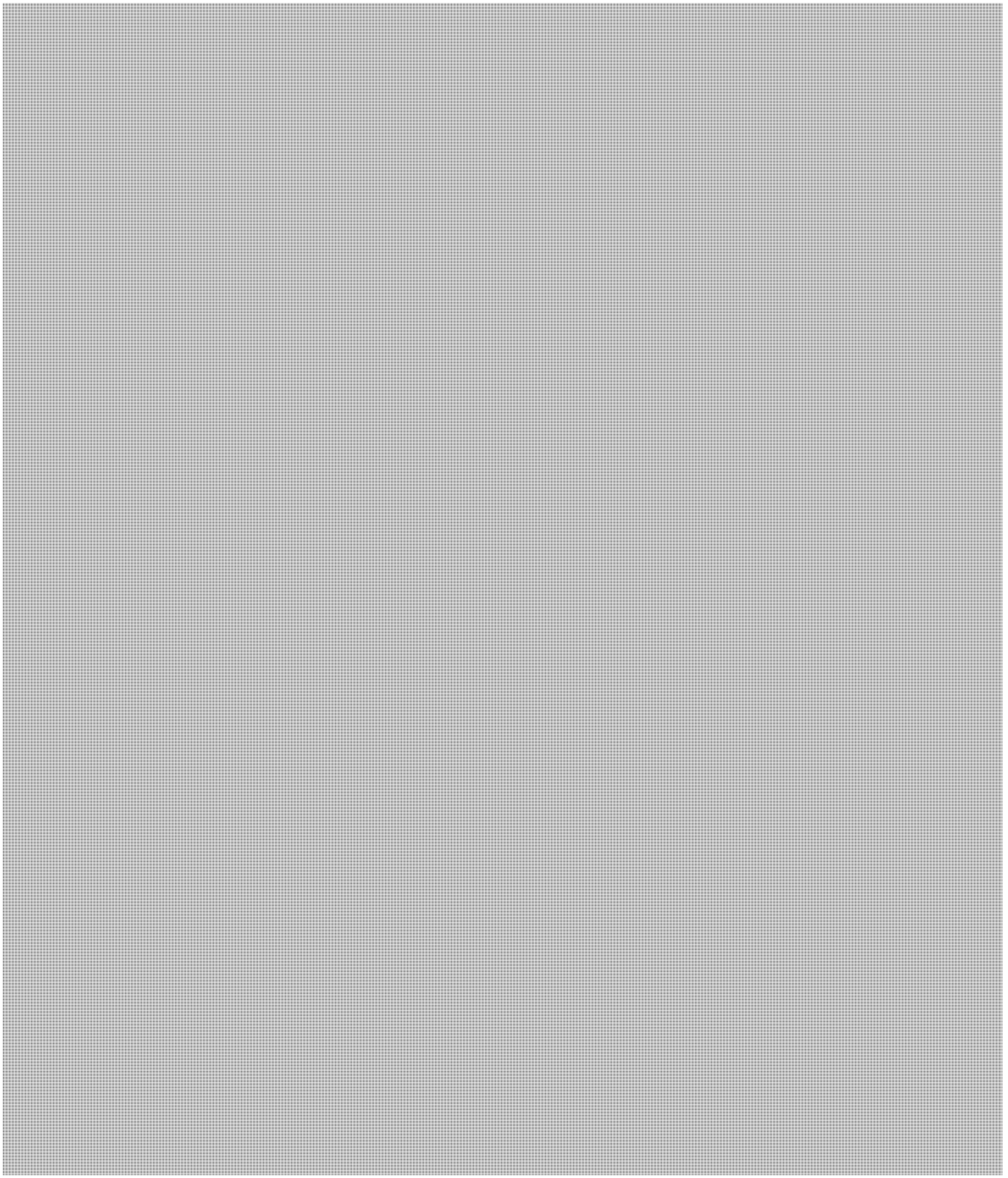
Additionally, as I mentioned during our earlier telecon at 9:20AM; CCIRC recently conducted an assessment of the [redacted] I have provided our analysis below for your awareness in case this tool is later used against your infrasturture.

[redacted]

Full CCIRC Technical Analysis of [redacted] is below.

s.16(2)(c)

Static Stand-Alone Dynamic Analysis



Hope these indicators and technical analysis reports are helpful. s.16(2)(c)

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC

http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

CYBERDO

From: CYBERDO
Sent: April-05-12 10:23 AM
To: [redacted] CYBERDO
Cc: [redacted]
Subject: RE: CCIRC CE12-002744 [redacted]

Thanks very much [redacted] for taking the time to speak with me by telephone this morning - Greatly appreciated.

Our technical analyst has retrieved the files so you can go ahead and remove them.

I'll update you later with our analysis of the [redacted] script and our previous analysis on the [redacted] released last month.

If at any time your upstream provider is overwhelmed or you require any assistance from CCIRC, please get in contact with us. If you need a cyber-duty officer anytime of the day, the best way to ensure you get immediate assistance is to call the government operations centre [redacted] explain circumstances and request the cyber duty officer be paged.

Great working with you and enjoy your long weekend.

s.13(1)(d)
s.16(2)(c)
s.19(1)

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

-----Original Message-----
From: [redacted]
Sent: April-05-12 10:01 AM
To: CYBERDO
Cc: [redacted]
Subject: RE: CCIRC CE12-002744 [redacted]

Hello,

Please find below links to logs from our webserver for the past several days, which should provide you with details about IPs involved in a recent DDoS attack on the [redacted] website.

[redacted]

Please let me know when you have downloaded these so I can remove them.

Thank you again for your assistance,

s.13(1)(d)
s.16(2)(c)
s.19(1)

[redacted]

-----Original Message-----
From: CYBERDO [mailto:[redacted]
Sent: Wednesday April 4, 2012 9:07 AM
To: [redacted] CYBERDO
Cc: [redacted]
Subject: RE: CCIRC CE12-002744 [redacted]

Good to hear that the attacks for now appear to be mostly contained.

If attacks increased in intensity, if you provided logs with timestamps, attacking IP addresses and traffic pattern, CCIRC would then coordinate with ISPs in Canada (and international CIRT teams if sources were outside of Canada), to filter attack traffic directed to your website. I am going to open up a Technical Analysis Request internally here at CCIRC to do some more analysis on the scripts and the [redacted] itself to see if we can provide you with additional information that will assist you in mitigation efforts.

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

-----Original Message-----
From: [redacted]
Sent: April-04-12 8:58 AM
To: CYBERDO
Cc: [redacted]
Subject: RE: CCIRC CE12-002744 [redacted]

Good Morning,

Yesterday's attack seems to have been rather small. [redacted] you've provided us with.

[redacted]

It would appear that an attack is still on-going, from [redacted] judging by the [redacted] But, it is having no effect [redacted]

[redacted]

Would you please advise what kind of other assistance could CCIRC render?

Thanks,

[redacted]

s.13(1)(d)
s.16(2)(c)
s.19(1)

-----Original Message-----
From: CYBERDO [mailto:[redacted]
Sent: Wednesday April 4, 2012 8:22 AM
To:
Cc: [redacted] CYBERDO
Subject: CCIRC CE12-002744[redacted]

Good Morning [redacted]

Can you provide an update on the DDoS attack reported yesterday. Are they still on-going or do you require any assistance from CCIRC?

Thanks,

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

********** This e-mail (including any attachments) may contain PRIVILEGED and CONFIDENTIAL INFORMATION only for use of the Addressee(s). If you are not the intended recipient of this e-mail or the employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any dissemination or copying of this e-mail is strictly prohibited. If you have received this e- mail in error, please immediately notify me by telephone or e-mail to arrange for the return or destruction of this document. Thank you. **********

Gordon, Robert

From: Gordon, Robert
Sent: April-03-12 2:49 PM
To: Clairmont, Lynda
Cc: Dick, Robert; Gordon, Robert
Subject: Fw: CP: Committee sheds little light on videos that take aim at public safety minister

Quick report - Session this AM went as predicted. CSEC's session focused on their mandate which means they are not involved in the issue at hand. Most of the questions during my session were directed to the RCMP. Questions to me were fairly general and did not address the actual investigation. Did manage to insert some information about PS's activities, e.g. Production of various types of information products which are distributed to P/Ts and critical infrastructure owners/operators.

Witnesses, including me, made the observation that the issues around the YouTube video are not cyber security issues.

Overall, don't believe I said anything that will cause difficulties - reporting below seems to suggest that the focus will be on RCMP. Comms rep was in attendance and observed that he had no concerns from his perspective.
Bob

From: Dick, Robert
Sent: Tuesday, April 03, 2012 02:32 PM
To: Gordon, Robert
Subject: Fw: CP: Committee sheds little light on videos that take aim at public safety minister

Martin Champoux was there from comms.

From: Champoux, Martin
Sent: Tuesday, April 03, 2012 02:00 PM
To: Gordon, Robert; Dick, Robert; Hatfield, Adam
Subject: FW: CP: Committee sheds little light on videos that take aim at public safety minister

.....not even a mention of Public Safety

Committee sheds little light on videos that take aim at public safety minister
April 3, 2012, 13:47 ET
Canadian Press

OTTAWA - The RCMP says its investigation into online video threats against the **public safety minister** is continuing, but has no details to share.

James Malizia, the RCMP's assistant commissioner for protective policing, told a House of Commons committee the force takes all threats to ministers seriously.

The committee is looking into videos that demanded **Public Safety Minister Vic Toews** resign over a federal bill that would give police and spies easier access to information about Internet users.

Toews angered many people by painting opponents of the bill as allies of child pornographers.

The videos, posted on YouTube under the banner of loosely knit collective Anonymous, threatened to reveal personal secrets about **Toews** if he did not abandon the legislation.

Toews, meanwhile, stayed overnight in an Ottawa hospital Monday after checking in with what aides said were flu-like symptoms.

Link (to Global News)

Gordon, Robert

From: Champoux, Martin
Sent: April-03-12 3:16 PM
To: Gordon, Robert; Dick, Robert; Hatfield, Adam
Subject: G&M: RCMP, spy agency shed no light on Anonymous threats against Toews

No mention of PS testimony

RCMP, spy agency shed no light on Anonymous threats against Toews
Latest testimony bolsters notion that parliamentary probe of online hacker group is ultimately futile
By Gloria Galloway, Globe and Mail, April 3, 2012

Representatives of Canada's electronic surveillance agency and national police force were called before a Commons committee Tuesday to tell politicians all they know about threats posted by online hacker group Anonymous against Public Safety minister Vic Toews.

And the answer is: Not much.

Toni Moffa, the assistant deputy minister who is responsible for technical security at the Communications Security Establishment, seemed genuinely confused by the questions being put to her and had to repeatedly explain that threats posted to public Internet sites are outside the jurisdiction of her organization.

And, while Chief Superintendant James Malizia of the RCMP agreed his organization was looking into the activities of Anonymous as they relate to Mr. Toews, he made it clear he could not discuss the details of the investigation.

The matter was referred to the House affairs committee by Speaker Andrew Scheer, who ruled that Mr. Toews's privileges as a parliamentarian may have been breached by Anonymous - a loose network of international protesters who, in this case, objected to controversial online-surveillance legislation introduced by the minister.

Some of the opposition MPs on the committee have previously expressed concern their inquiry is hampered by the fact Anonymous is anonymous. When they asked how they should get around that problem, Mr. Toews - who testified last week - suggested that they should call in the experts.

But the testimony of those experts Tuesday merely bolstered the notion that the committee's efforts are, in many ways, futile.

As Ms. Moffa told the committee, CSE collects foreign intelligence signals and provides assurances to the government that federal computer systems are secure. But when asked by Conservative MP Harold Albrecht to explain what she knows about Anonymous, how it operates and what threats the group may pose, Ms. Moffa was at a loss.

Anything CSE knows about Anonymous comes from "open sources," she said. And "from our perspective, it's not an [information technology] security breach and it would be best dealt with by an investigative body or agency that would do that type of investigation."

But the investigators were not much more informative.

Supt. Malizia confirmed it is public knowledge that there is an ongoing investigation. But, in response to any question about the case of Anonymous and Mr. Toews, he said: "I am not in a position to discuss any details or specifics with respect to any ongoing investigation."

The most important information provided to MPs on the committee by CSE and the RCMP was that they should follow good Internet security protocols and, if they are ever threatened, they should inform the authorities - none of which will get them very far in their current inquiry.

Toward the end of the committee meeting, which finished early because the MPs had nothing more to ask their witnesses and their witnesses had nothing more to tell them, Conservative MP Laurie Hawn conceded it is unlikely that the identities of the people behind the Anonymous threats will ever be revealed.

Searching for ways to make the committee's inquiry relevant, Mr. Hawn asked Supt. Malizia if he thought the process was worthwhile in reminding Internet users that posting threats against parliamentarians is a crime. "Has this process been useful at least in that respect?" he asked the police officer.

"Well, I am not in a position to comment on the committee's work and the process," Supt. Malizia replied, "but I can say is that advances in technology have created an environment where individuals achieve anonymity."

Gordon, Robert

From: Clairmont, Lynda
Sent: April-03-12 2:58 PM
To: Gordon, Robert; Dick, Robert
Subject: FW: CBC News: 'Anonymous' probe on Toews threats wilts under MP questioning

Assume you saw this

From: Despard, Sean **On Behalf Of** PSMediaCentre/CentredesmediasdeSP
Sent: April-03-12 2:07 PM
To: * COMMS ADG / Bureau du directeur général associé; * COMMS Communication Services Division / Division des services de communication; * COMMS DGO / Bureau de la directrice générale; * COMMS Program Communications Division / Secteur des communications de programmes; * COMMS Public Affairs Division / Secteur des affaires publiques; * Speeches / Discours; Astravas, Rutha; Banerjee, Ritu; Beaudoin, Serge C; Bolton, Stephen; Boucher, Patrick; Boucher-Lalonde, Murielle; Cameron, Bud; Carmichael, Julie; Champoux, Elizabeth; Clairmont, Lynda; Clifford, Kurtis; Coburn, Stacey; Crawford, Andrée; Csversko, Christine; Currie, St. Clair; Daoust, Normand; De Santis, Heather; Duschner, Gabrielle; Dussault, Josée; Easson, Grant; Gareau-Lavoie, Genevieve; Gordon, Robert; Gow, Robert; Hitchcock, Christy; House, Andrew; Huggins, Rachel; Humeniuk, Elena; Hunt, Ryan; Jarmyn, Tom; Johnson, Mark; Kelland, Stephen; Khouri, Lisa; Komm, Chantelle; Kubicek, Brett; Lavoie, Micheline; Leclair, Natalie; Leclerc, Carole; Leonidis, Nelly; Lesser, Robert; MacDonald, Nicholas; MacKinnon, Paul; Marchand, Renee; McAteer, Julie; Morris, Marika; Motzney, Barbara; Mueller, Mike; Mundie, Robert; Nicole, Jean-Thomas; Oldham, Craig; Panthaky, Jasmine; Patton, Michael; Pozhke, Nicholas; Rosario, Giselle; Roy, Isabelle; Saunders, Joanne; Shuttle, Paul; Slack, Jessica; Thibault, Stéphane; Tupper, Shawn; Van Criekingen, Jane; Verret, Scott; Wex, Richard; Wilson, Gina; Adam.Kates@cbsa-asfc.gc.ca; Allison.Wildgust@cbsa-asfc.gc.ca; Amitha.Carnadin@cbsa-asfc.gc.ca; Bateman, Paul; Bernard.Alladin@cbsa-asfc.gc.ca; Bev.Arseneault@csc-scc.gc.ca; Bindman, Stephen; Brunette, Lynn; cbsa.media@cbsa-asfc.gc.ca; Cgirouad@justice.gc.ca; Chad.Fleck@international.gc.ca; Williams, Christpher; Churney, Daryl; Cobbsu@csc-scc.gc.ca; Cocking, Marie; Couture, Jocelyne; Derek Cefaloni; Douglas, Caroline; C. Girouard; Hart, Melissa; Bradley, Jolene; Mackillop, Ken; Lamothe, Maureen; Lauzon, Raymond; Lavoie, Daniel; Mailhot, Esther; Stokes, Mark; Mary.Schlosser@rcmp-grc.gc.ca; Media.Monitoring@cbsa-asfc.gc.ca; CBSA Media Monitoring; RCMP Media Monitoring; Martin, Nadie; Robinson, N.; Parkes, Sara; Giolti, Patrizia; Prieur, Mark; Rioux, Veronique; Rondeau, Martine; Sbinman@justice.gc.ca; Dumoulin, Stéphanie; Tim.Cogan@rcmp-grc.gc.ca
Subject: CBC News: 'Anonymous' probe on Toews threats wilts under MP questioning

'Anonymous' probe on Toews threats wilts under MP questioning
April 3, 2012, 13:50 ET
CBC News, By: Laura Payton

A committee charged with looking into threats against **Public Safety Minister Vic Toews** by the hackers group Anonymous morphed into an examination of how the government handles cybersecurity as the experts appearing in front of MPs struggled to explain where they fit into the committee's investigation.

Representatives from **Public Safety Canada**, the RCMP and the Communications Security Establishment, an arm of the Defence Department that provides foreign signals intelligence to the goverment and works on national IT security, took questions from MPs on the Commons procedure and House affairs committee following a request by **Toews** that Parliament look into videos posted on the online video sharing site Youtube by Anonymous.

Anonymous is a loosely-organized group of hackers and activists in which anyone can declare their membership. Someone identifying him or herself as part of Anonymous posted videos on Youtube threatening to reveal details of **Toews'** public life if he didn't scrap his proposed online surveillance bill, C-30.

In the committee's first meeting on the subject of threats against **Toews**, House of Commons staff suggested it was a waste of time to try to track down whoever posted the video anonymously to a website.

Experts struggled to answer questions

In Tuesday's meeting, CSE's deputy chief of IT security turned to ways in which people's personal or work computers could be compromised.

Asked about the make-up of Anonymous, Toni Moffa said she couldn't speak to the intent of people who declare themselves members. What CSE looks at is techniques used to hack into systems, she said.

"Certainly what we look at are the techniques that are used by such groups and how to provide advice to prevent those things from being successful in our own systems. So I would be unable to comment," Moffa said.

She suggested MPs always install software patches as they arise and noted there's plenty of information about cybersecurity available on the agency's website. MPs were also advised not to open attachments from people they didn't know, or, upon receipt of an attachment from someone they know, to double-check that person intended to email an attachment.

Robert Gordon, a special advisor on cybersecurity to a unit within the Public Safety Department, said he couldn't give advice about the video itself.

***"The actual posting of the Youtube [video] wasn't a cyberevent ... so Public Safety Canada doesn't provide advice on it*," he said. "*We would provide advice on protecting the various networks, but the actual posting of a video is a fairly easy thing to do. Unfortunately we're not in a position to provide much advice on that*."**

MPs receive hate mail

Liberal MP Wayne Easter asked whether any countries are looking at ways of dealing with commenters on websites.

"Even for each and every one of us who's not a minister, who take policy positions because it's part of our job, we face hate mail, increasingly so. Because the people that are writing the letters do not have to sign their name," Easter said.

Moffa said she's a technical expert and couldn't comment.

The RCMP have confirmed there is an investigation into **Toews'** complaint. MPs and ministers are entitled to RCMP protection if they feel their safety has been threatened, said James Malizia, the RCMP's assistant commissioner of protective policing. But he couldn't comment on the investigation, he said.

Asked whether the RCMP could trace the person who uploaded the video, Malizia said he wasn't in a position to answer specific details about **Toews'** case.

"There are occasions where we are able to identify individuals. It's case by case, each case is unique... sometimes we aren't in a position to do so," he said.

At one point, the RCMP and **Public Safety's national security expert** couldn't say which department would be able to track down the IP address that could help identify who uploaded the videos. The RCMP doesn't have a mandate to work in cybersecurity, Malizia noted.

Link

Gordon, Robert

From: Matz, Mark
Sent: April-03-12 2:33 PM
To: Gordon, Robert
Subject: Live blog

Full live blog of today's committee appearances!

Mark Matz
Director, Policy and Issues Management /
Directeur, Politiques cyber et gestion des enjeux
NATIONAL CYBER SECURITY / CYBERSÉCURITÉ NATIONALE
613-993-9635

Kady:
Procedure and House Affairs continues its foray into the amorphous world of Anonymous in its efforts to determine whether the internet-based anti-collective ostensibly behind those "threatening" Youtube videos did indeed breach the privilege of Public Safety Minister Vic Toews.

On the witness list for today: the similarly shadowy Communications Security Establishment Canada, which is sending deputy IT chief Toni Moffa and "Cyber Defence" director general Scott Jones, as well as Robert Gordon, special advisor to the Canadian Cyber Incident Response Centre, and the RCMP Officer In Charge at the Mounties' Technological Crime Branch, which at least doesn't include the word 'cyber' in its name, so thank goodness for small mercies.

In any case, the show starts at 11am, so check back for full coverage!
Share

Tuesday April 3, 2012 7:34 Kady

10:00 [redacted]**kady:**
BTW, if you need a break from the F-35 debacle-thon, I'll be covering #PROC vs. Anonymous (Round Three) at 11am. Watch for liveblog URL! #hw *[via Twitter]*
Share

Tuesday April 3, 2012 10:00 kady

11:03 **Kady:**
Greetings, privilege enthusiasts and students of the enigmatic entity known as Anonymous! After hearing from the complainant -- Public Safety Minister Vic Toews -- and the House of Commons officials responsible for safeguarding parliament, it's time to bring in the ostensible experts: Communications Security Establishment e-spooks Scott Jones and Toni Moffa, followed by representatives from the RCMP personal protection unit. Will they, too, explain to the committee that attempting to hunt down the perpetrator of those Youtube videos may be an exercise in futility? We'll soon find out!
Share

Tuesday April 3, 2012 11:03 Kady

11:06 **Kady:**
And we're off! First up: the aforementioned CSE officials, who get the usual cheery welcome from the chair before being invited to deliver their opening statements. Which, at least as far as Moffa is concerned, appears to bear a haunting resemblance to the About Us page of the agency website, so I'll not be chronicling every syllable, although if either she or Jones -- can we call him 'Agent Jones'? ideally in a British accent? Oh *fine*; you never let me have any fun - veer, by

happenstance, on to the topic currently confronting the committee, I will leap into action.

Share

Tuesday April 3, 2012 11:06 Kady

11:09 **Kady:**

Fear not the malevolent Others lurking online, government -- and parliamentarians! - CSE is on the job. (Aren't there potential privilege issues inherent in the notion of CSE monitoring precinct internet use, even if ostensibly for the most benign of reasons?)

Share

Tuesday April 3, 2012 11:09 Kady

11:15 **Kady:**

And now, questions! Starting with Harold Albrecht, who can't help but notice that the opening statements, while fascinating and informative, was largely devoted to the technical issues of securing government networks and computers. Can they tell us all about Anonymous now, he wonders, a look of pure, if faint hope on his face. No, as it turns out -- not beyond what can be found through "open source" research. Albrecht tries again, noting that this is a *serious matter*, and wonders if there is any mechanism where there are international arrangements that would allow parliamentarians to identify the poster behind a Youtube video. Full credit to Moffa for keeping a straight face, and giving a straight answer: No, that's not an IT security issue, and is best handled by law enforcement, which CSE, for the record, is not. What advice, Albrecht wondered, would she have in dealing with 'an amorphous, anonymous group?' He then becomes an early contender for Statement of the Obvious of the Day by observing, somewhat plaintively, "We don't even know who they are." Is *this* when the penny drops?

Share

Tuesday April 3, 2012 11:15 Kady

11:17 **Kady:**

(The answer, if anyone was wondering, was no, since - all together now - that's not what CSE does. Protecting parliamentarians from Youtube is not within its mandate.)

Share

Tuesday April 3, 2012 11:17 Kady

11:19 **Kady:**

Hrrm. Not sure if this is a new revelation, or not a revelation at all but a symptom of lack of understanding of the technology involved in posting a video to Youtube (1.) a video 2) an open tab for Youtube 3) A finger with which to click 'upload') but I think Philip Toone just suggested that the video was posted by someone outside Canada.

Share

Tuesday April 3, 2012 11:19 Kady

11:21 **Kady:**

I hope these poor witnesses didn't have to leave important cyber-defending work unattended to show up for this meeting, because from what I can see, the sum total of their contribution to the discussion is to repeat, over and over, that this is not an IT security threat.)

Share

Tuesday April 3, 2012 11:21 Kady

11:23 **Kady:**

Okay, really, how many time does poor Agent Moffa (it isn't quite 'Agent Jones', but I'll take it) say that *this is not within her jurisdiction*? At this point, I almost wish one of the MPs *would* pull out a laptop and ask if either official can make a few of those annoying toolbars go away.)

Share

Tuesday April 3, 2012 11:23 Kady

11:25 **Kady:**

Oh, Wayne Easter. I admire your moxie, but I'm just not sure these particular witnesses will share your concern over online surveillance.

Share

Tuesday April 3, 2012 11:25 Kady

11:26 **Kady:**
Also not within the CSE's purview, I suspect: Comment threads. (Yes, Easter just brought that up as an example of the menace of the anonymous.) (That's small-a anonymous, for the record.)
Share

Tuesday April 3, 2012 11:26 Kady

11:28 **Kady:**
I must say that for shadowy intelligence officers, these witnesses certainly seem to have a sizeable entourage of stone-faced, besuited staffers.
Share

Tuesday April 3, 2012 11:28 Kady

11:34 Kady:
And now, Bob Zimmer will ask the witnesses for tips on protecting oneself from security threats, which, for the record -- as stated, restated and we're this close to finger puppet time -- THE ALLEGED BREACH UNDER SCRUTINY IS NOT. Oh, and he also wants to know more about the "membership" of Anonymous; specifically, what proportion is made up of srs bsns criminal types versus digital hangers on. Not surprisingly, Moffa notes that she's not qualified to answer that. Don't worry, ma'am: you're halfway through this surreal ordeal, and then you can go back to stalking rogue foreign cell signals.
Share

Tuesday April 3, 2012 11:34 Kady

11:37 Kady:
Yes, it's come to this: Laurie Hawn is asking for tips on internet security. Moffa points him to the public safety department website. I wonder when Agent Jones will snap and suggest that an MP just *Google* it already.
Share

Tuesday April 3, 2012 11:37 Kady

11:37 Kady:
CSE ProTip: Always patch your software when upgrades are available!
Share

Tuesday April 3, 2012 11:37 Kady

11:41 Kady:
I do appreciate that Hawn refers to "guys .. or gals!" of Anonymous when he observed, correctly, that not much expertise is required, and they are very likely "enthusiastic amateurs." Interestingly, Moffa cautions him against suggesting that "we're" keeping up with the threat, and notes that it's a constant battle. Finally, he wonders about "spear-fishing" -- standard email hack, always remember not to click on attachments from unknown sources (or familiar sources inexplicably using broken English in the subject line/body). Also, data sticks! You don't even *know* how risky those suckers can be.
Share

Tuesday April 3, 2012 11:41 Kady

11:42 Kady:
And with that, the committee officially runs out of ways to pretend that calling these witnesses wasn't a total and complete waste of time. Espooks excused! Bring on the RCMP, who may actually have something relevant to contribute to the discussion!)
Share

Tuesday April 3, 2012 11:42 Kady

11:44 Kady:
Alright, the Mounties - and PSEPC officials - have taken their seats, and we're off to the races, this time, on an actual *horse*, although we'll see whether it makes it anywhere near the finish line.
Share

Tuesday April 3, 2012 11:44 Kady

11:47 Kady:
Well, so far, we're getting the About Us for the Canadian Cyber Incident Response Centre, as well as

Canada's Cyber Security Action! Plan, but I fear that we will soon end up with the same seemingly unavoidable conclusion: That a video posted on Youtube is not an IT security threat, even if it allegedly threatens a minister, just like murdering someone and posting the resulting clip to Youtube would not be an internet security issue. (Although it would totally be known as The Youtube Murder by the media.)

Share

Tuesday April 3, 2012 11:47 Kady

11:51 Kady:

And there we are: as noted just now by special advisor Robert Gordon, the Canadian Cyber Incident Response Centre - or C-CIRC - is *not* a law enforcement agency. You're our only hope for relevant answers now, RCMP protective policing branch! (Not you, technological crime branch officer in charge Tony Pickett.)

Share

Tuesday April 3, 2012 11:51 Kady

11:56 Kady:

And here he is - RCMP assistant commissioner for protective policing James Malizia, who begins by noting that ministers are entitled to protection if required at home and abroad, and notes that MPs can also report such incidents and ask for additional measures. That -- didn't actually provide much information into the issue before the committee at the moment, but I'm still hopeful, or at least not hope*less*. "We take all threats to ministers and members of parliament seriously," Malizia stresses. Also, the internet -- beautiful but deadly, or something like that. Cybercrime! The RCMP views cybercrime as *any* crime committed by using a computer or network, which -- wait, that makes no sense. If I hatched a plot to rob a bank, wrote it up in Google Docs and printed out a copy for my reference, that wouldn't magically make it a cybercrime.

Share

Tuesday April 3, 2012 11:56 Kady

11:59 Kady:

If you're keeping track, so far, Malizia has said nothing remotely relevant to the instant matter, although he does seem to hold a downright Charlie Angus-ian view of social media, and -- stop saying cyber, sir. Please. It's killing me. Sorry, where was I? Cybercrime! Cyberthreats! All around the Cyberworld! Cyber, baby! (That used to mean something rather different, by the way.)

Share

Tuesday April 3, 2012 11:59 Kady

12:03 Kady:

Malizia *did* mention Anonymous, I should note, albeit in passing, and characterized them as a "movement with no official membership". Meanwhile, we've moved to questions, and Albrecht is once again attempting to get us to take this threat with the solemnity it merits (done!). He reads the alleged threats included in the video into the record -- for the second time, for those keeping track -- and wonders where, in the "contiuum of criminality", the Youtube threats fall. The witnesses look at each other before silently delegating Malizia to field this one, whereupon he kills off any chance of actual news coming out of this hearing by noting that he cannot comment on ongoing investigations.

Share

Tuesday April 3, 2012 12:03 Kady

12:06 Kady:

Albrecht once again tries to draw a firm line between anonymous threats in letter form, and videos that can be viewed by millions, although I'm still not sure I agree with his contention that the latter is more serious: a threat, after all, is a threat regardless of audience share. Also, Albrecht seems almost aggrieved to be told, yet again, that there's a good chance the IP address behind the posting will ever be outed.

Share

Tuesday April 3, 2012 12:06 Kady

12:09 Kady:

Okay, it seems that Malizia *is* confirming an ongoing investigation, and thank you, Joe Comartin, for asking the question in such a simple, easy to answer way. Unfortunately, Malizia *is not* able to provide

more information on what other agencies may be involved in that investigation, but Comartin is insistent: Who, he demands, is "most able" to identify who posted that video? I forgot what a hawk Comartin is on this particular issue.

Share

Tuesday April 3, 2012 12:09 **Kady**

12:11 Kady:

Comartin once again wonders about cooperation with investigative agencies in *other* countries -- this came up during his questioning of the House of Commons officials, I believe - but comes up similarly empty, even when he cites recent arrests of self-claimed Anonymii. He then moves back to the danger of double jeopardy, as far as parliamentary findings vs. criminal charges, which, I suspect, may be an example of borrowing trouble, given the likelihood of either investigation resulting in a collar.

Share

Tuesday April 3, 2012 12:11 **Kady**

12:14 Kady:

Comartin tries to get Malizia to confirm whether the investigation extends beyond the Youtube video to physical threats. Nice try, but no chance, sir. Also, Easter notes that asking for a minister's resignation is *not*, in fact, a threat -- he's asked for a few himself, he recalls, and doesn't want to walk out to handcuffs. With that, he turns to the issue at hand: Did Toews ask for police protection? Malizia goes vague, noting that yes, ministers have been protected in the past, noting that he's "not at liberty" to discuss the specifics.

Share

Tuesday April 3, 2012 12:14 **Kady**

12:20 Kady:

It's Come To This II: Easter wonders why, in his opening statement, C-CIRC advisor Robert Gordon emphasized security from threats *outside* government, and wondering why, exactly, he employed such syntax. Gordon seems bemused. Back to Anonymous for a moment -- if he/she/it is identified, and turns out to be just across the border, what would happen next? Malizia assures him that the RCMP does indeed cooperate with its counterparts in other countries.

Share

Tuesday April 3, 2012 12:20 **Kady**

12:24 Kady:

Back to the Conservative side of the table, and Greg Kerr, who begins by thanking the witnesses for being here, despite "trepidation" and an inability to say everything about what they know, he gives Malizia the opportunity to repeat -- for the third time, very nearly word for word -- his opening statement vis a vis threats against ministers and members. Malizia does not respond directly to Kerr's shameless solicitation for an endorsement of increased surveillance power in an age of overprotective privacy mavens, although he does express his theoretical future appreciation for such measures.

Share

Tuesday April 3, 2012 12:24 **Kady**

12:28 Kady:

Over to Alexandrine Latendresses, who gently but firmly steers the committee back on topic: Is there any way to find the IP address of the person on Youtube? It's a case by case basis, Malizia repeats -- sometimes they can do it, sometimes they can't. Latendresse wonders if an anonymous letter would provoke a similar investigation; depends on the analysis, Malizia tells her -- they would investigate in each case, video or paper -- "all types" of threats. Latendresse wonders if the witnesses have seen the video in question; could anything be done from a criminal investigation? No comment due to ongoing criminal investigation. Oh, this is fun.

Share

Tuesday April 3, 2012 12:28 **Kady**

12:32 Kady:

Laurie Hawn wonders if "we have a grip" on the number and intensity of threats outside the government, which is, of course, not remotely within the terms of reference of this committee. Hawn, however, sees

this as a threat to the system itself -- our very system of government, and not the minister. "Do you have an opinion on that?" He asks the witnesses. "Um. No." says Malizia, who simply won't offer his opinion -- concurring or dissenting -- on that.

Share

Tuesday April 3, 2012 12:32 **Kady**

12:35 Kady:

Hawn really has to work on his pronunciation of "these people." Also, he wonders whether there have been instances where individuals have claimed ignorance of the law, which -- they have. "Do you think this process is shedding some helpfui light for those out there?" Hawn asks. Oh, for heaven's sakes, stop trying to make the witnesses justify this study. It's unseemly.

Share

Tuesday April 3, 2012 12:35 **Kady**

12:35 Kady:

(To his credit, Malizia managed not to comment in as polite a way as possible.)

Share

Tuesday April 3, 2012 12:35 **Kady**

12:37 Kady:

"Do you have A/anonymous agents," Zimmer wonders, and I'm honestly not sure whether he meant small-a or big-A, nor does it matter, since the witnesses can't say.

Share

Tuesday April 3, 2012 12:37 **Kady**

12:39 Kady:

So It's Come To This III: Despite being pointed to the public safety website - as mentioned earlier at the meeting - Zimmer forces Gordon to provide two security tips for protecting yourself against digital threats. He goes with firewalls -- keep 'em up to date -- and "think before you click". This is going to be one of those days he'll remember forever, I suspect.

Share

Tuesday April 3, 2012 12:39 **Kady**

12:40 Kady:

And with that, the torture of our poor, long suffering witnesses ends. Meeting adjourned! Let us never speak of it again!

Share

Tuesday April 3, 2012 12:40 **Kady**

12:42

Gordon, Robert

From: Strasbourg, Christina
Sent: April-03-12 2:56 PM
To: 'PCO'
Cc: Dupuis, Chantal; 'Nicole Rainville'; 'Helen Hopfauf (helen.hopfauf@rcmp-grc.gc.ca)'; 'Rene Ouellette'; Baran, Tara; McLaren, Victoria; Dussault, Josée; Champoux, Elizabeth; McAteer, Julie; Leclair, Natalie; 'tim.klodt@forces.gc.ca'; 'Justice'; 'Gauthier, Amy-Lyne (Amy-Lyne.Gauthier@justice.gc.ca)'; Durand, Stéphanie; Veilleux, Martine; Mueller, Mike; Scheewe, Nathan; 'Reesha'; ' (charles-eric.lepine@rcmp-grc.gc.ca)'; Cintrat, Jean; Pozhke, Nicholas; Koops, Randall; Johnson, Mark; Jarmyn, Tom; House, Andrew; Easson, Grant; 'julie.gauthier@justice.gc.ca'; Issues / Enjeux; Hunt, Ryan; Baker, Tia Leigh; Browness, Monica; Gordon, Robert
Subject: Summary Report - PROC - April 3, 2012
Attachments: PS-SP-#595604-1-Summary Report - PROC - April 3, 2012.DOC

On April 3, 2012, the Standing Committee on Procedure and House Affairs met earlier today with respect to their study on the Question of Privilege relating to threats to the Member for Provencher. The Committee heard from Communications Security Establishment Canada during the first hour. Officials from Public Safety and the RCMP appeared during the second hour. A brief summary of the meeting is attached.

The meeting went well. Questions focused primarily on the investigative tools and techniques for cybercrimes. Committee members were keenly interested in the details relating to the investigation into Anonymous. Witnesses responded that they could not comment on any ongoing investigations or techniques used by law enforcement.

Christina Strasbourg
Advisor, Parliamentary Affairs / Conseillère, Affaires parlementaires
Public Safety Canada / Sécurité Publique Canada
T: (613) 949-9913
F: (613) 949-2931
E: christina.strasbourg@ps.gc.ca

REPORT ON COMMITTEE MEETING

Name of Committee: **Procedure and House Affairs**
Report prepared by: Christina Strasbourg, Public Safety, 949-9913
Date and time: Tuesday, April 3, 2012, 11:00 a.m. to 12:40 p.m.
Location: Room 253-D, Centre Block
Subject: **Question of Privilege Relating to Threats to the Member for Provencher**

Witnesses:

11:00 a.m. to 11:40 p.m.

Communications Security Establishment Canada
- Toni Moffa, Deputy Chief, IT Security
- Scott Jones, Director General, Cyber Defence

11:40 p.m. to 12:40 p.m.

Public Safety Canada
- Robert Gordon, Special Advisor, Cyber Security, Canadian Cyber Incident Response Centre

Royal Canadian Mounted Police
- James Malizia, Assistant Commissioner Protective Policing, Protective Policing Branch
- Tony Pickett, Officer In Charge, Technological Crime Branch

Overview of Meeting

- The meeting went well. Questions focused primarily on the investigative tools and techniques for cybercrimes. Committee members were keenly interested in the details relating to the investigation into Anonymous. Witnesses responded that they could not comment on any ongoing investigations or techniques used by law enforcement.

Highlights of hearing:

- Mr. Albrecht (CPC) inquired on several occasions whether or not the Government had the tools required to trace the IP address of an individual who posted a video on YouTube. Witnesses responded that they could not comment on any ongoing investigations or techniques used by law enforcement.

- In response to Mr. Toone (NDP), Ms. Moffa responded that there was not technical threat or IT breach with respect to the Anonymous video that was posted on YouTube.

- Committee members had several questions related to the structure and membership of Anonymous as well as their hacking techniques. The witnesses responded that they could not comment on any ongoing investigations or techniques used by law enforcement. Ms. Latendresse (NDP) noted that anyone can post a video and say that it is under the guise of Anonymous as there is no real membership for the group.

- Mr. Comartin (NDP) was interested in learning about information sharing among RCMP and its partners. Mr. Malizia responded that the RCMP shares information with other countries, government departments and law enforcement agencies.

- Mr. Easter (Lib.) noted that he did not feel that requesting the resignation of a Minister should be considered a threat. Mr. Easter had several questions regarding whether the Minister requested protecting from the RCMP. Mr. Malizia responded that the RCMP takes all threats to Ministers and Members of Parliament seriously and assesses whether or not RCMP protection is required. He noted that he could not comment on who has sought protective services from the RCMP.

Follow-up required/Next meeting:

- The Committee will likely resume their study at their next meeting. There is no agenda posted at this time.

Gordon, Robert

From: Gordon, Robert
To: Clairmont, Lynda
Subject: Procedure and House Affairs Committee

It appears that the Committee will commence a series of hearings the week of March 26. A possible flow of speakers is as follows:

Initial session: Sergeant at Arms and Chief of IT, House of Commons to outline the overall cyber threat that they have observed

Second session: likely CSIS, CSEC and RCMP to examine the issue broadly including a review of the technical capacity of entities such as Anonymous. It will likely be less about technology and more about social engineering

Third session: someone from CCIRC to discuss what they know about cyber incidents

Fourth session: RCMP, Cyber Fraud Centre

Fifth session: representative from the Canadian Bankers Association

Six session: Joel Brenner, author of "America the Vulnerable: Inside the new Threat Matrix of Digital Espionage, Crime, and Warfare" (2011). Brenner is an attorney specializing in cyber security and related issues and a former senior counsel at the National Security Agency

Bob

Proulx, Véronique

From: Bendelier, Kenneth
Sent: April-02-12 2:47 PM
To: Proulx, Véronique
Subject: Anon Related Products
Attachments: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous; CCIRC Technical Report TR12-001: Mitigation Guidelines for Denial-of-Service Attacks / CCRIC Rapport technique RT12-001: Principes de prévention contre les attaques par déni de service ; CCIRC CYBER FLASH CF12-001: Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property

1. Information Note IN12-501 Overview of the Hacktivist Group "Anonymous"
   Released: 01 Mar 2012
   Reason: Recent high profile Anonymous activities had been widely-reported in the media. Some events, including legislation before Parliament and activities relating to the Oilsands are the types of activities that could potentially interest hackivist groups. In addition, a campaign claiming to be attributed from Anonymous had the stated objective of shutting the Internet down. As a CCIRC' role is to monitor and provide mitigation advice on cyber threats, this clearly falls within CCIRC's area of responsibility to produce and distribute.

2. Technical Report TN12-001 Mitigation Guidelines for Denial-of-Service Attacks
   Released: 22 Feb 2012
   Reason: This is a best practices document. It was originally drafted and envisioned to be released September 2011, however, resource constraints and task prioritization delayed this. As CCIRC develops mitigation advice and best practices for our partners to use in defending their cyber infrastructure, this clearly falls within CCIRC's area of responsibility to produce and distribute.

3. Cyberflash CF12-001 Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property
   Released: 26 Jan 2012
   Reason: CCIRC had received information about coordinated distributed denial-of-service (DDoS) attacks with multiple international targets including government and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA). "Anonymous" allegedly promoted attacks in response to the shutdown of the file hosting site MegaUpload and in protest of proposed U.S. legislation concerning online trafficking of copyrighted intellectual property and counterfeit goods. Follow-on attacks reported in the media targeted various governments organizations involved in the ratification of ACTA, namely the governments of Ireland and Poland. Information posted on the Internet site Pastebin suggests active monitoring of the Canadian position by the hacktivists. The update to Canada's Copyright Act is currently bill C-11 - Copyright Modernization Act, which is still in parliament. The Cyberflash contained detection and mitigation advice to reduce risk faced by Canadian partners.

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada

269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-993-5042
Facsimile | Télécopieur +1 613-954-3097
Kenneth.Bendelier@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

CYBERDO

From: CYBERDO
Sent: May-28-12 6:58 PM
To: [redacted]@certaq.gouv.qc.ca' s.16(2)(c)
Cc: CYBERDO
Subject: CCRIC CE12-002994 [Nouvelle list de proxy]

anonyops.europe http://www.facebook.com/pages/[redacted]

[redacted] (350 x) AND [redacted] test proxies first,they burn out fast !

[redacted]

Pages 2281 to / à 2301

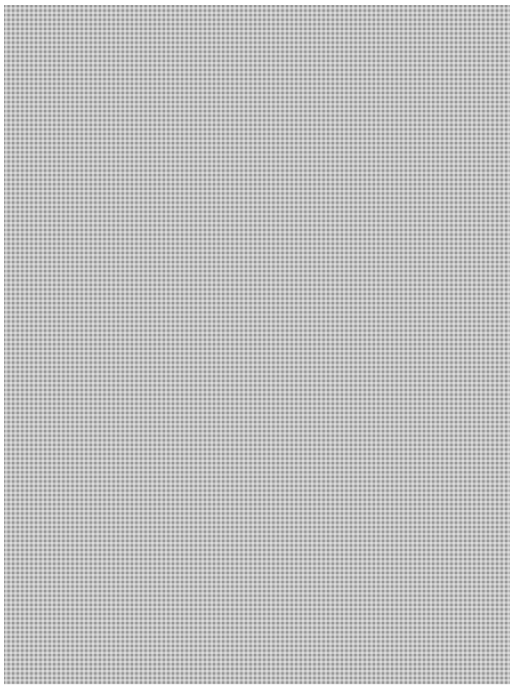
are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information



s.16(2)(c)

Thanks to [redacted]

Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
www.publicsafety.gc.ca

CYBERDO

From: [redacted]
Sent: May-28-12 10:25 AM
To: CYBERDO
Subject: RE: CCIRC-CCRIC CE11-2195

s.13(1)(d)
s.16(2)(c)
s.19(1)

Categories: Sheldon

Hello,

To follow up on this incident from last year, we have received several tweets last night relating to possible release of our website database.

It is not clear though whether this is the old information from the original incident, or something new (a new breach unknown to us). Perhaps your contacts could (discretely) determine that?

[redacted]

Regards,

[redacted]

From: CYBERDO [mailto:[redacted]
Sent: Wednesday July 13, 2011 2:24 PM
To: [redacted] CYBERDO
Cc: [redacted]
Subject: RE: CCIRC-CCRIC CE11-2195

Hello,

Sorry, but we have no further information for you at this time. If anything should change, we will notify you and your organization immediately.

Thank you,

Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
www.publicsafety.gc.ca

s.13(1)(d)
s.16(2)(c)
s.19(1)

From: [redacted]
Sent: July 13, 2011 12:58 PM
To: CYBERDO
Cc: [redacted]
Subject: RE: CCIRC-CCRIC CE11-2195

Hello,

Would you please advise if you have had any further updates to our incident file since the last communication below?

thanks,

[redacted]

CYBERDO <[redacted]

2011.07.07 15:22

To [redacted]
cc
Subject RE: CCIRC-CCRIC CE11-2195

Greetings,

Here is the response we from our contact:
"
This information was obtained from an IRC during an investigation. That is all information we have. They (anonymous) were collecting information from many government web sites from others countries. It was a list of sites and vulnerabilities.

regards,
"

That's all we have.

Vireak Phlek
Cyber Duty Officer | Agent chargé des incidents cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-5451
Facsimile | Télécopieur +1 613-991-3574
vireak.phlek@ps-sp.gc.ca

PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

s.13(1)(d)
s.16(2)(c)
s.19(1)

-----Original Message-----
From:
Sent: July 7, 2011 11:08 AM
To: CYBERDO
Subject: RE: CCIRC-CCRIC CE11-2195

Morning,

I am following up whether you have received any more details/information, as per the email below.

thanks,

CYBERDO

2011.07.06 17:24 To
"'
cc
CYBERDO
Subject
RE: CCIRC-CCRIC CE11-2195

Greetings,

Thank for providing us the update. I will checked with our source for the web site, but he already left for the day.

Thanks,

Vireak Phlek
Cyber Duty Officer | Agent chargé des incidents cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-5451
Facsimile | Télécopieur +1 613-991-3574
vireak.phlek@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

s.13(1)(a)

s.16(2)(c)

s.19(1)

-----Original Message-----
From:
[mailto:]
Sent: July 6, 2011 5:15 PM
To: CYBERDO
Subject: Re: CCIRC-CCRIC CE11-2195

Hello,

As a follow up to your email, we have taken action to secure our website from further intrusion.

and we are working towards identifying any other potential vulnerabilities.

In the mean time,

Thank you for your assistance,

CYBERDO <

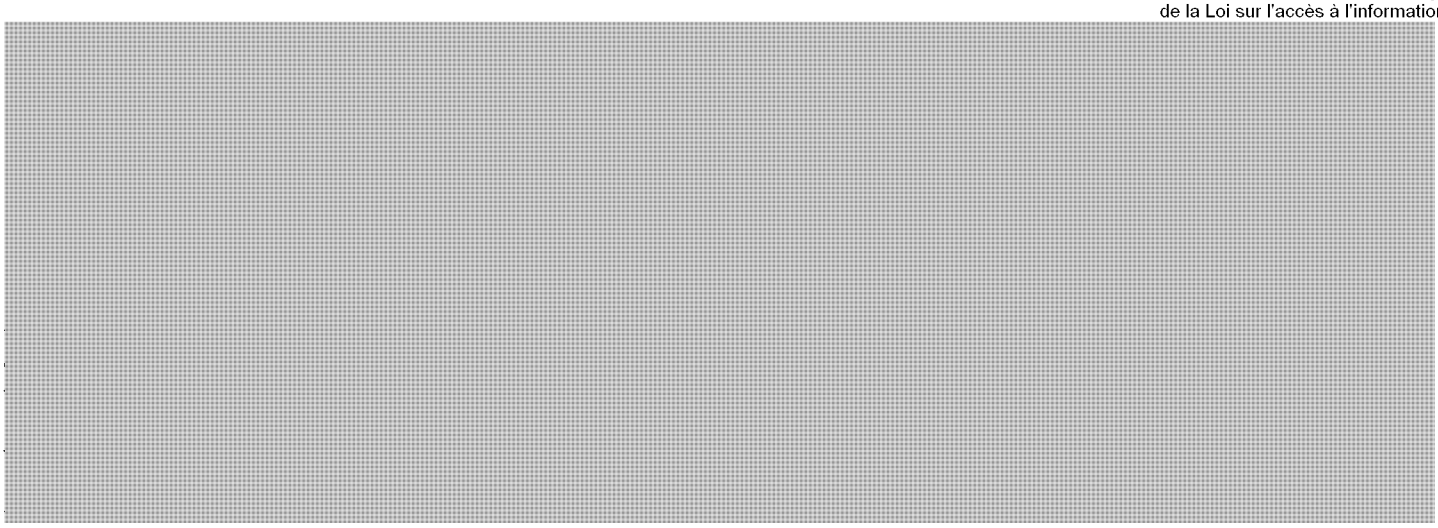
2011.07.06 14:27 To
" cc CYBERDO <
Subject CCIRC-CCRIC CE11-2195

Greetings,

We have assigned the following cyber incident number to this event, please use that number for any correspondence regarding this matter.

Include are the

+



+

From the following site:

Regards,

Vireak Phlek
Cyber Duty Officer | Agent chargé des incidents cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-5451 Facsimile | Télécopieur +1 613-991-3574 vireak.phlek@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

s.13(1)(d)
s.16(2)(c)
s.19(1)

****
This e-mail (including any attachments) may contain PRIVILEGED and CONFIDENTIAL INFORMATION only
for use of the Addressee(s). If you are not the intended recipient of this e-mail or the employee or agent
responsible for delivering it to the intended recipient, you are hereby notified that any dissemination or copying
of this e-mail is strictly prohibited. If you have received this e-mail in error, please immediately notify me by
telephone or e-mail to arrange for the return or destruction of

this document. Thank you.
****

****
This e-mail (including any attachments) may contain PRIVILEGED and CONFIDENTIAL INFORMATION only for use of the Addressee(s). If you are not the intended recipient of this e-mail or the employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any dissemination or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please immediately notify me by telephone or e-mail to arrange for the return or destruction of this document. Thank you.
****

********** This e-mail (including any attachments) may contain PRIVILEGED and CONFIDENTIAL INFORMATION only for use of the Addressee(s). If you are not the intended recipient of this e-mail or the employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any dissemination or copying of this e-mail is strictly prohibited. If you have received this e- mail in error, please immediately notify me by telephone or e-mail to arrange for the return or destruction of this document. Thank you. **********

CYBERDO

From: Billard, Sheldon
Sent: May-24-12 11:00 AM
To: CYBERDO
Subject: Good news item

Hacker Adrian Lamo Who Betrayed Wikileaks' Manning Turns Fire on Anonymous

Adrian goes on to say that Anonymous is reputed to be invincible, by the media...

http://www.ibtimes.co.uk/articles/344388/20120523/adrian-lamo-snitch-anonymous-bradley-manning-wikileaks.htm

Sheldon Billard

Canadian Cyber Incident Response Centre | canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Ottawa, Ontario, Canada K1A 0P8 Telephone | Téléphone 613-991-7056 Facsimile | Télécopieur 613-991-3574 Government of Canada | Gouvernement du Canada

CYBERDO

s.16(2)(c)

From: CYBERDO
Sent: May-22-12 4:19 PM
To: [redacted]@certaq.gouv.qc.ca'
Cc: '[redacted]@certaq.gouv.qc.ca'; CYBERDO
Subject: CE12-002994 DDOS Anonymous
Attachments: pastebin_com_[redacted]

Bonjour CERTAQ,

Le CCRIC est au courant de la publication d'une attaque iSQL du site [redacted] au lien :
http://pastebin.com/[redacted]
Le contenu de la publication est fournie en attachement.

Merci

Vireak Phlek

Cyber Duty Officer
Public Safety Canada
CCIRC
613-991-7029
www.publicsafety.gc.ca

CYBERDO

From: Beaudoin, Luc
Sent: May-24-12 11:47 PM
To: CYBERDO
Cc: Anderson, Windy; Clow, Patrick; Bendelier, Kenneth; Murphy, Gregg
Subject: CE12-003019 DDOS from Anonymous tomorrow: OpNewSon
Attachments: operation-new-son.pdf

s.16(2)(c)
s.20(1)(c)

For close monitoring tomorrow. [redacted] and a few others are of particular Canadian interest....

I am working from home tomorrow.

[redacted]

\\\\
Content:

[redacted]

Page 2312

is withheld pursuant to section

est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

CYBERDO

From:	Beaudoin, Luc	s.16(2)(c)
Sent:	May-24-12 10:30 PM	s.20(1)(c)
To:	[redacted]@ic.gc.ca	
Subject:	CE12-003019 OpNewSon tomorrow: DDOS from Anonymous	
Attachments:	operation-new-son.pdf; IN12-501-Overview of the Hacktivist Group Anonymous.txt; CF12-001_EN [Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property].txt	

U1-N2 (N3 without my comments)

http://pastebin.com/[redacted]

We received the attached document. A number of these companies have operations in Canada, to an extent I am not fully aware of but likely significant and dependent on this group's services. We should keep an eye open as this unfolds, or not, tomorrow, 25 May. Credibility is unknown (medium is my own guess, based on some chats I observed).

Feel free to leverage our recent Anonymous mitigation products as required.

[redacted]

Luc

CYBERDO

From: CYBERDO
Sent: May-22-12 10:27 AM
To: [redacted]@certaq.gouv.qc.ca' s.16(2)(c)
Cc: CYBERDO; '[redacted]@certaq.gouv.qc.ca'
Subject: CE12-002994 DDOS Anonymous

Bonjour,

Nous essayons d'en savoir plus sur la situation des sites du Gouvernement du Québec qui ne sont plus accessible à cause du Dénie se service.
Est-ce CERTAQ est en mesure de partager cette information? Encore une fois si vous avez besoin d'aide n'hésitez pas à nous contacter.

Vireak Phlek
Cyber Duty Officer
Public Safety Canada
CCIRC
613-991-7029
www.publicsafety.gc.ca

-----Original Message-----
From: CYBERDO
Sent: May-21-12 11:01 AM
To: CYBERDO; [redacted]@certaq.gouv.qc.ca'
Subject: RE: CE12-002994 DDOS Anonymous

Bonjour encore. Nous avons discuté au téléphone avec le gestionnaire d'incident en devoir. Merci pour l'information (référence la raison pour laquelle le site est hors ligne).

Encore une fois, si vous avez besoin d'assistance additionnelle, n'hésitez pas à nous contacter. Nous sommes également intéressés à vos leçons apprises dans la gestion de ce cas, si elles sont disponibles.

Bonne journée

CCRIC

From: CYBERDO
Sent: May-21-12 10:01 AM
To: CYBERDO; [redacted]@certaq.gouv.qc.ca'
Subject: RE: CE12-002994 DDOS Anonymous

s.16(2)(c)
s.20(1)(c)

Correction: le site mels.gouv.qc.ca semble toujours affecté.

Avez-vous contacté vos ISPs ?

[redacted]

Mitigations :

1) voir piece jointe

2) http://www.securitepublique.gc.ca/prg/em/ccirc/2012/tr12-001-fra.aspx

CYBERDO

From: CYBERDO
Sent: May-21-12 9:36 AM
To: [redacted]@certaq.gouv.qc.ca
Cc: CYBERDO
Subject: CE12-002994 DDOS Anonymous

CERT AQ,

Les CCRIC a noté les différents rapports dans les médias et sur Twitter concernant l'attaque sur vos réseaux et ceux du PLQ. Ils semblent que le site du PLQ soient toujours affectés mais le site du gouvernement du Québec semble accessible.

N'hésitez pas à nous contacter si vous avez besoin d'assistance avec la mitigation.

Nous serions également intéressés à toute information concernant les sources [redacted] et techniques des attaques [redacted], ainsi que les mesures défensives effectives que vous avez utilisés de manière à assister et prévenir de futures attaques.

merci

s.16(2)(c)

Cyberdo

[redacted]

CYBERDO

From: Beaudoin, Luc
Sent: May-22-12 9:41 AM
To: [redacted]CYBERDO
Cc: [redacted]@ic.gc.ca; CYBERDO
Subject: RE: DDOS against Quebec Government (CE12-002994)

s.16(2)(c)
s.19(1)

Yes they did, and they may be partly correct. One may ask whether self-denial in this context (note that the mels site is up now) does not serve an encouraging message to hacktivists.

A 404 page with a clear message may have been more efficient that the site is not down for accidental reasons.
Ex:
http://www.securitepublique.gouv.qc.ca/
(ref: http://www.lapresse.ca/actualites/quebec-canada/politique-quebecoise/201205/19/01-4526911-le-gouvernement-du-quebec-encore-attaque-par-anonymous.php)

about 404 as a response strategy, one may consider things like this cool TED presentation:
Renny Gleeson: http://www.ted.com/talks/renny_gleeson_404_the_story_of_a_page_not_found.html

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: [redacted][mailto:[redacted]
Sent: May-22-12 9:31 AM
To: CYBERDO
Cc: [redacted]@ic.gc.ca; CYBERDO
Subject: RE: DDOS against Quebec Government (CE12-002994)

s.16(2)(c)
s.19(1)

Hi,

According to this article (in french) Anonymous took responsibility for that.

http://www.lapresse.ca/actualites/dossiers/conflit-etudiant/201205/22/01-4527335-attaques-en-ligne-au-nom-de-la-liberte-dexpression.php

Regards,

[redacted]

[redacted]

Devez-vous imprimer ce courriel ?

CYBERDO <[redacted]

2012-05-21 10:20

A [redacted]@ic.gc.ca" <[redacted]@ic.gc.ca>
cc CYBERDO [redacted]
Objet RE: DDOS against Quebec Government (CE12-002994)

Too funny. Ignore (partially) my last. [redacted]

The PLQ site is still down though....so there is likely still DDOS activity around these but from a mitigation stand point, there is not urgency or assistance request being made.

Luc

From: Beaudoin, Luc
Sent: May-21-12 10:10 AM
To: [redacted]@ic.gc.ca
Cc: CYBERDO
Subject: DDOS against Quebec Government (CE12-002994)

Reference:
http://www.torontosun.com/2012/05/19/quebec-liberal-government-sites-hacked
www.youtube.com/watch?v=xPrfqfdJn8U

It appears to still be active.

Plq.org and **mels.gouv.qc.ca** are still down

s.16(2)(c)

Would appreciate any information available. If some of you are working already with CERT AQ please let me know.

Luc

CYBERDO

From: Beaudoin, Luc
Sent: May-21-12 11:06 AM
To: Anderson, Windy
Cc: Champoux, Martin; Clow, Patrick; Bendelier, Kenneth; CYBERDO
Subject: CE12-002994 DDOS attack on the Quebec government

s.16(2)(c)

Reference :

- CE12-002994
- http://www.torontosun.com/2012/05/19/quebec-liberal-government-sites-hacked
- www.youtube.com/watch?v=xPrfqfdJn8U

CCIRC noticed on Twitter feeds Friday the 18 May 2012 that the collective ``Anonymous`` may be planning an operation against the Quebec government related to the adoption of Bill 78 aimed at limiting the public impact of student protests.

On Saturday, media reported that the web site of the Quebec ministry of education (mels.gouv.qc.ca) and the Quebec liberal party (plq.org) were down as a result of Anonymous attacks.

CCIRC confirmed that both sites were still down Monday morning 20 May. CCIRC contacted the CERT AQ to verify the status of their mitigation efforts. CERT AQ confirmed they were aware and have been engaged with mitigating malicious activities surrounding the education ministry website for about 3 weeks. As a result, [redacted] CERT AQ has also been working with their ISPs accordingly. They confirmed that they do not require CCIRC support at this time, but thanked us for the call.

Taking the site off-line is likely the cause of the exaggerated impact of the Anonymous attack in the media.

The PLC site is another story. They are not part of our CI client community. CCIRC sent a courtesy note to the PLC site administrator to inform them of open source media reports and the publicly available DDOS mitigation guide we have on our site.

Luc

CYBERDO

From: CYBERDO
Sent: May-21-12 9:14 AM
To: Beaudoin, Luc
Subject: Re: Critical: Heads-Up - Quebec Liberal Party and Education Ministry websites take down in massive Cyber Attack

Having login issues on laptop. Could be me (recent pwd change) or the corp system. I am waiting to see when Bruce comes back for dog walking. Meantime, I am drafting email on bb incase he can't get logged on too.

I will cc u on the certAQ email.

Yeah, I just saw it was saturday.

Sandra

---

s.16(2)(c)

Cyber Duty Officer

[redacted]

----- Original Message -----
From: Beaudoin, Luc
Sent: Monday, May 21, 2012 08:58 AM
To: CYBERDO
Subject: Fw: Critical: Heads-Up - Quebec Liberal Party and Education Ministry websites take down in massive Cyber Attack

READ THIS.... It was SATURDAY !!! Ask them how it wnt and if we can do something now...

Sorry. Just saw this

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----
From: Beaudoin, Luc
Sent: Monday, May 21, 2012 08:57 AM
To: Anderson, Windy; Bendelier, Kenneth
Subject: Re: Critical: Heads-Up - Quebec Liberal Party and Education Ministry websites take down in massive Cyber Attack

1) We notified them Friday;
2)I just spoke to cyberdo requesting that she reaches out to CERT AQ with the media reporting and offer our assistance if needed.

3) The sites are up. Everything happened Saturday apparently...(Just checked)

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----
From: Anderson, Windy
Sent: Monday, May 21, 2012 08:51 AM
To: Beaudoin, Luc; Bendelier, Kenneth
Subject: Fw: Critical: Heads-Up - Quebec Liberal Party and Education Ministry websites take down in massive Cyber Attack

Luc,

Are you actually paging Cyberdo. Will they do research (what happened, what is still going on, does anyone need our help, etc)?

Windy

----- Original Message -----
From: Beaudoin, Luc
Sent: Monday, May 21, 2012 08:47 AM
To: Bendelier, Kenneth; CYBERDO
Cc: Anderson, Windy
Subject: Re: Critical: Heads-Up - Quebec Liberal Party and Education Ministry websites take down in massive Cyber Attack

Ack, paging CYBERDO.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----
From: Bendelier, Kenneth
Sent: Monday, May 21, 2012 08:31 AM
To: Beaudoin, Luc
Subject: Fw: Critical: Heads-Up - Quebec Liberal Party and Education Ministry websites take down in massive Cyber Attack

----- Original Message -----

From: E-Secure-IT [mailto:alert@e-secure-it.com]
Sent: Monday, May 21, 2012 06:14 AM
To: Bendelier, Kenneth
Subject: Critical: Heads-Up - Quebec Liberal Party and Education Ministry websites take down in massive Cyber Attack

Generated by your Alert Subscription on Folder:
- Government CA
- Major Site Security Breaches - Hack / DDos Attacks
- Anonymous
Source: The Hacker News
Complete item: http://thehackernews.com/2012/05/quebec-liberal-party-and-education.html

Description:
Two provincial government websites as well as Quebec Liberal Party and Education Ministry websites went down early Saturday morning and remained inaccessible for most of the day. No one has claimed responsibility for the downed sites but Twitter was full of rumours on Saturday pointing to Anonymous, the loose group of cyber activists.

The cyber troubles began just hours after a new law, Bill 78, passed in the National Assembly. It requires any group of 50 or more people holding a demonstration in the province to inform police eight hours in advance of their planned route and other pertinent details such as the start and end times. One of Anonymous Twitter accounts tweeted on Friday: Quebec Considers Draconian Anti-Protest Law ... Expect us.

Anonymous also threatened the website belonging to the provinces National Assembly. While some reported that the legislature's website had been taken offline, it was functioning as of 9:25 a.m. on Saturday. Referring to the province as Quebecistan, the group wrote that Rule 78 must die.

A spokesman for the Quebec Liberal Party said the partys site was hacked.They are attacks that are pretty common, said Michel Rochette. We have been victims of cyber-attacks for the past few weeks.

E-Secure-IT
https://www.e-secure-it.com

CYBERDO

From: Beaudoin, Luc
Sent: May-21-12 7:54 AM
To: CYBERDO; Anderson, Windy; Champoux, Martin; * CyberIH
Subject: Anonymous threat to Qc

FOR YOUR INFO

Anonymous posted a youtube video on "Operation Quebec", threatening the Quebec government following bill 78 on student protest.

CCIRC was aware of potential anonymous activity Friday and notified CERTAQ. CCIRC is monitoring.

Luc
Luc

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

CYBERDO

From: Sheldon.Billard@ps-sp.gc.ca
Sent: May-18-12 9:18 AM
To: Clow, Patrick
Subject: RE: Quebec

Historically, this type of step-in from anonymous (in support of the protesters), will presumably result in a DDOS against the government body the protesters are targeting.

- Sheldon.

-----Original Message-----
From: Clow, Patrick
Sent: May-18-12 9:16 AM
To: CYBERDO
Subject: Quebec

Good morning,

FYI An Anonymous Twitter account (Anonymous Operations) has retweeted a tweet on the proposed 'special law' the Quebec government is currently debating re the ongoing student protests.