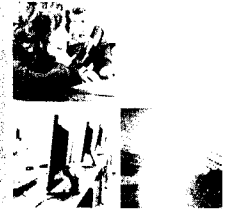


Recent Canadian Events



General

- In 2012 Canada was ranked second worldwide for hosted phishing sites
- Number of sites hosting malware in Canada has increased by over 200% percent since 2011
- 39% increase in over 2011 in botnet activity

Recent (Summer 2012)

- Canadian energy firm affected by cyber attack

Anonymous (2012)

- Ontario Association of Chiefs of Police: Compromise and publication of accounts
- Operation Quebec: DDOS against Quebec government
- Operation Vic.Tory: Smear campaign against supports of Bill C-30
- Operation Party Crasher: DDOS against government institutions (Provincial and Federal)

Past (2011)

- Well publicized attacks against the Department of Finance and the Treasury Board



UNCLASSIFIED

TIMELINE – ANONYMOUS OPERATIONS

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 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.

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.

UNCLASSIFIED

Operation Payback / Operation Sony (worldwide)

Action: DDoS attacks were launched against Sony PlayStation websites. Millions of users' personal information, in some cases including credit card information were publicly released.

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.

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.

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 Federal's website was defaced, company files were deleted, phone systems were taken down and 68,000 employee emails were published.

Reason: An HBGary Federal 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 and WikiLeaks.

UNCLASSIFIED

Operation Green Rights/ Project Tarmaggedon (Canada)

In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline and the Alberta Tar Sands project.

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.

Occupy Toronto (Canada)

Action: 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. Over 50 businesses based in Toronto had their websites hacked, and were automatically redirected to the homepage of Occupy Toronto.

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, 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 (SOPA) and the Protect IP Act (PIPA).

STRATFOR (worldwide)

Action: STRATFOR is a US company that provides services to intelligence and law enforcement agencies, among others. 200 gigabytes of data was stolen from the company'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. The Canadian federal government was an indirect target of Anonymous activity in connection with STRATFOR. Some of the usernames and passwords released included those of federal employees.

UNCLASSIFIED

Reason: Following the HBGary Federal 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.”

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. Most notably in February 12, Anonymous posted a 17 minute long video on YouTube of a conference call between Scotland Yard and the FBI discussing the group itself, Anonymous, garnering worldwide media attention.

Reason: The declaration of cyber warfare on governments and corporations worldwide in response to perceived corruption and government censorship.

Bill C-11 and Bill C-30 (Canada)

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, which were extensively covered in the media.

Operation Blackout / Black March (worldwide)

Action: On January 18, 2012, Anonymous associated itself to a blackout campaign lead by sites such as Reddit, Wikipedia, and Google, who for 12 hours blacked out their websites to protest SOPA/PIPA legislations. On January 19 2012, following the take down of megaupload.com by the US government, Anonymous retaliated by defacing the websites of the FBI, the CIA, the US Department of Justice, in addition to the websites of Universal Music, Warner Music Group, BMI, the Motion Picture Association of America, and the Recording Industry Association of America. Over 5000 users were participating in the attacks although it appears that some may have done so unwittingly. Anonymous is now asking those opposed to ACTA, SOPA and PIPA to abstain from buying media (books, music, movies, etc.) through the month of March 2012. Anonymous is also claiming that it will engage in cyber attacks every Friday. The group also indicated that 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. The stated objective of this DDoS attack is to “shut the Internet down”.

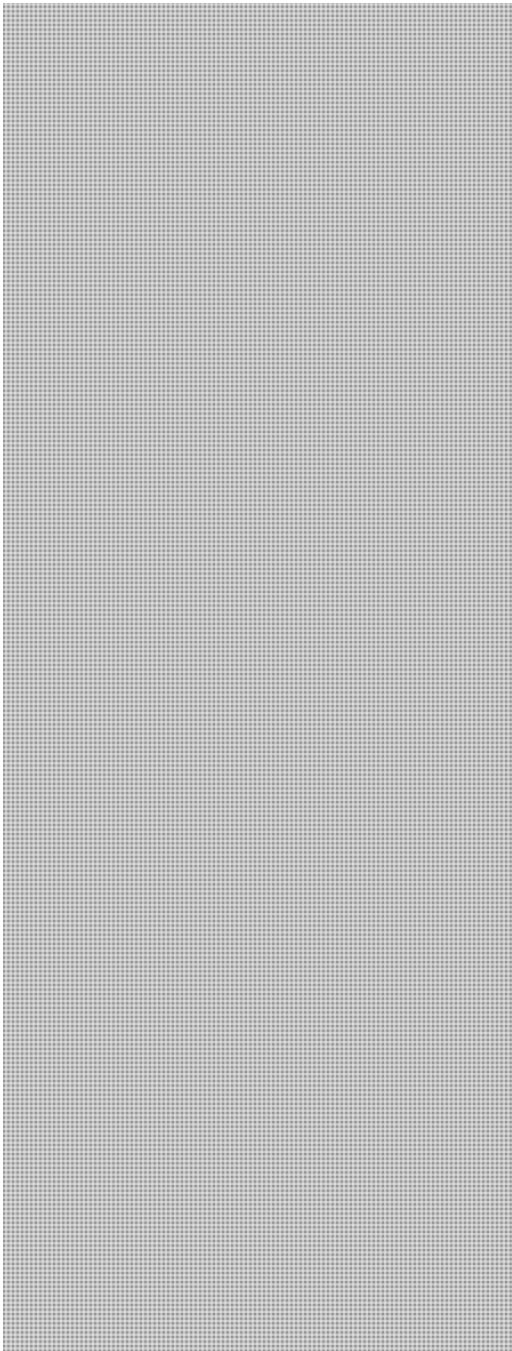
Reason: Related to Operation Blackout (below), Operation Black March aims to protest ACTA, SOPA, PIPA and other policies that are aimed at stopping online piracy.

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/\[REDACTED\]](http://www.facebook.com/pages/[REDACTED])

[REDACTED] (350 x) AND [REDACTED] test proxies first,they burn out fast !



**Pages 1899 to / à 1919
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 

Cyber Duty Officer
Public Safety Canada
CCIRC


www.publicsafety.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.

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.

CYBERDO

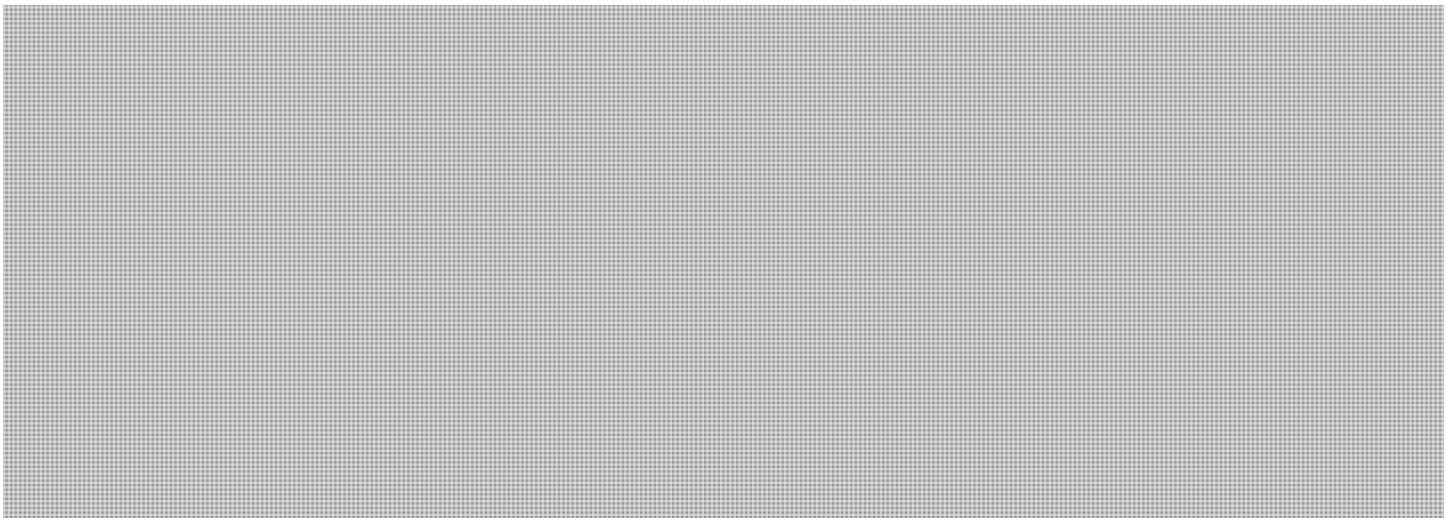
From: [REDACTED] s.13(1)(d)
Sent: May-28-12 10:25 AM s.16(2)(c)
To: CYBERDO s.19(1)
Subject: RE: CCIRC-CCRIC CE11-2195

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?



Regards,



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

www.publicsafety.gc.ca

s.13(1)(d)

s.16(2)(c)

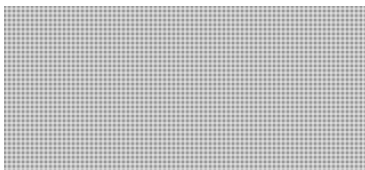
s.19(1)

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,



CYBERDO <[REDACTED]>

2011.07.07 15:22

To: [REDACTED]
cc: [REDACTED]
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: [REDACTED]
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,

[REDACTED]

CYBERDO [REDACTED]

2011.07.06 17:24 To

" [REDACTED]

cc
CYBERDO [REDACTED]

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

-----Original Message-----

From: [redacted]
[mailto:[redacted]]
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. [redacted]

[redacted] and we are working towards identifying any other potential vulnerabilities.

In the mean time, [redacted]
[redacted]

Thank you for your assistance,

[redacted]

CYBERDO <[redacted]>
2011.07.06 14:27 To [redacted] cc CYBERDO <[redacted]>
" [redacted] Subject CCIRC-CCRIC CE11-2195

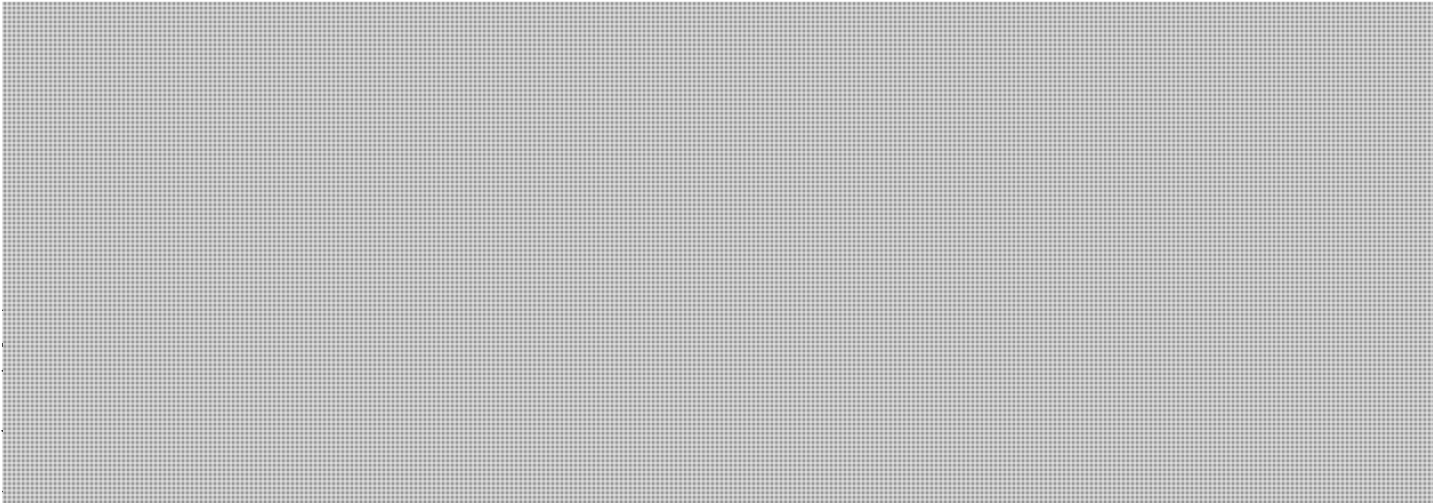
Greetings,

We have assigned the following cyber incident number to this event, please use that number for any correspondence regarding this matter.

Include are the [redacted]

[redacted]

+



+

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

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.

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

From: CYBERDO
Sent: May-22-12 4:19 PM s.16(2)(c)
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/\[REDACTED\]](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

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.

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.

CYBERDO

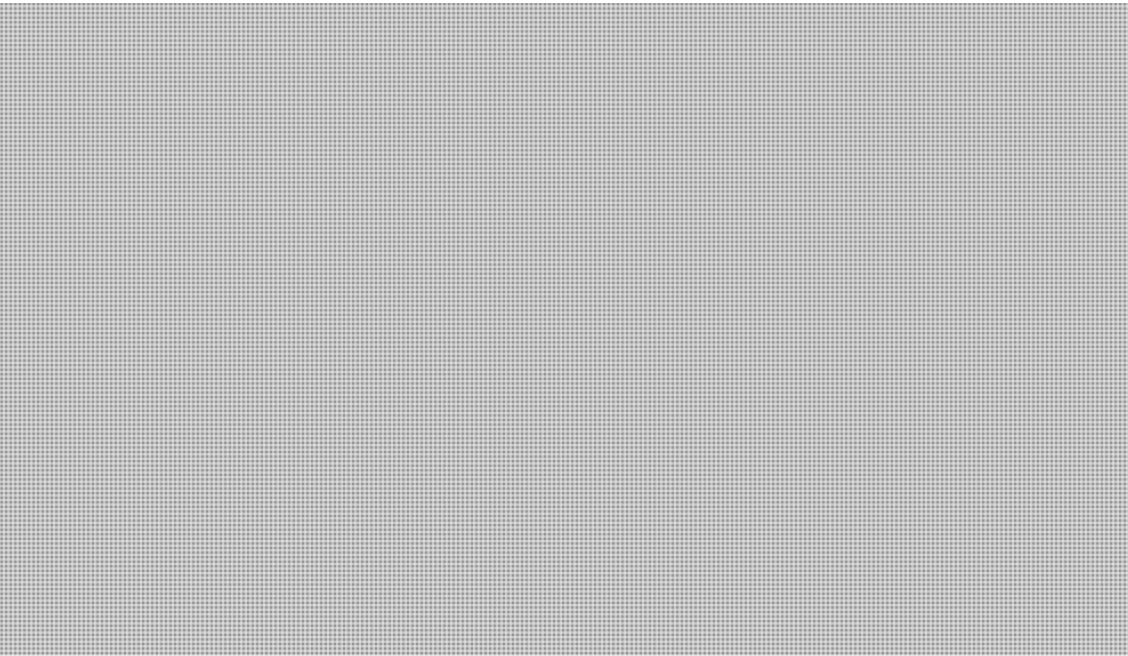
From: Beaudoin, Luc
Sent: May-24-12 11:47 PM
To: CYBERDO
Cc: Anderson, Windy; Clow, Patrick; Bendelier, Kenneth; Murphy, Gregg
Subject: CE12-003019 DDOS from Anonymous tomorrow: OpNewSon
Attachments: operation-new-son.pdf

s.16(2)(c)

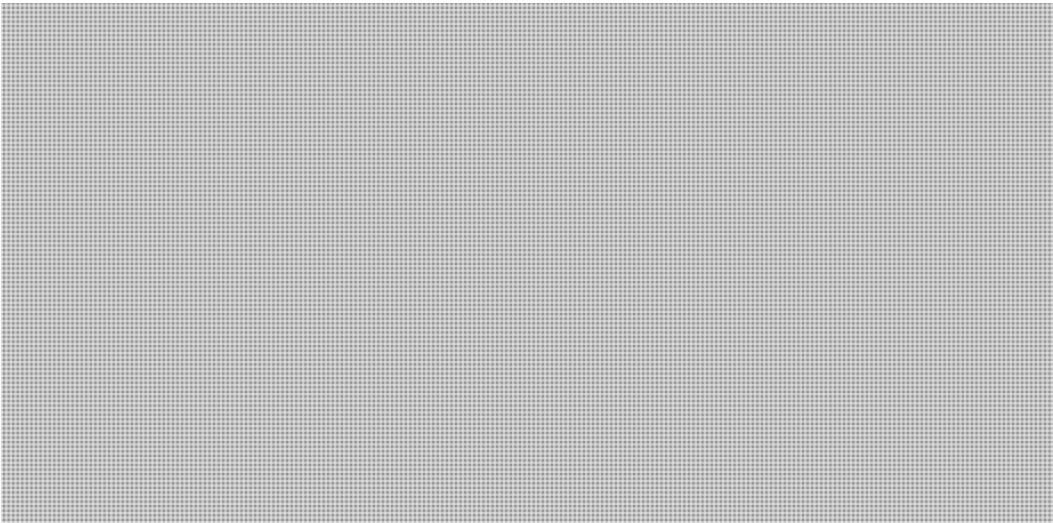
s.20(1)(c)

For close monitoring tomorrow. [REDACTED] and a few others are of particular Canadian interest....

I am working from home tomorrow.



\\\\\\
Content:



Page 1930

**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

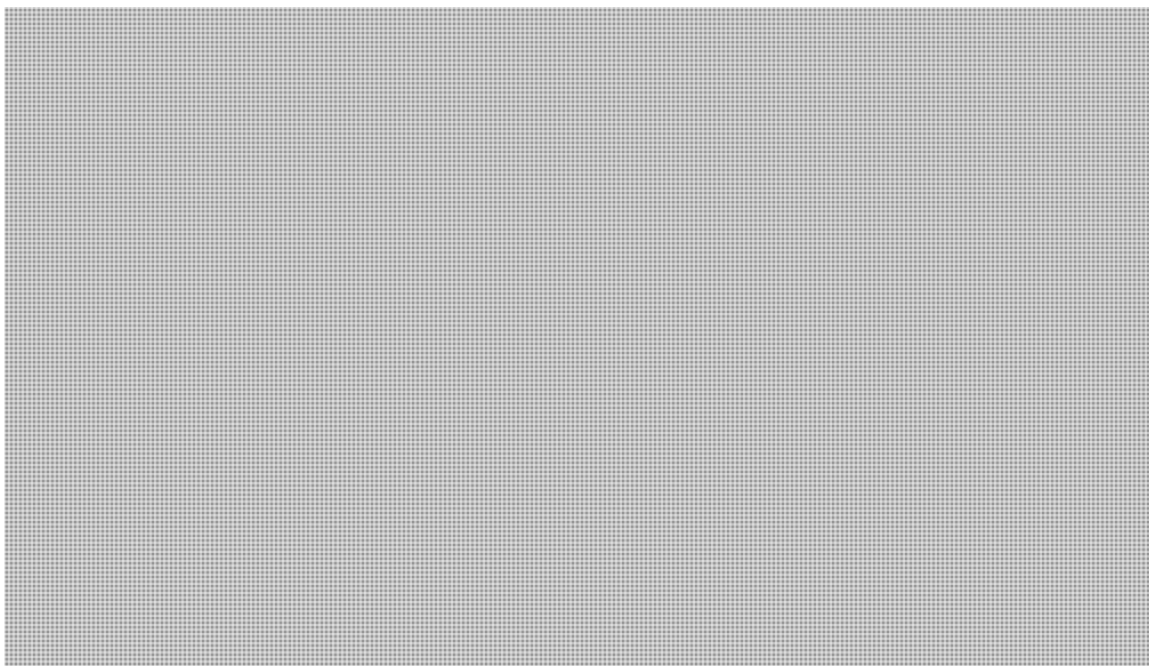
From: Beaudoin, Luc s.16(2)(c)
Sent: May-24-12 10:30 PM s.20(1)(c)
To: CanadianTCP@ic.gc.ca
Subject: CE12-003019 OpNewSon tomorrow: DDOS from Anonymous
Attachments: operation-new-son.pdf; IN12-501-Overview of the Hactivist Group Anonymous.txt; CF12-001_EN [Hactivist Group Anonymous - DDOS Activity Related to Copyrights and Intellectual Property].txt

U1-N2 (N3 without my comments)

<http://pastebin.com/> 

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.



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

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.

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.

-----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 ?



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 s.16(2)(c)
Sent: May-22-12 9:41 AM s.19(1)
To: [REDACTED] CYBERDO
Cc: CanadianTCP@ic.gc.ca; CYBERDO
Subject: RE: DDOS against Quebec Government (CE12-002994)

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 hackers.

A 404 page with a clear message may have been more efficient than the site is not down for accidental reasons.

Ex:

<http://www.securitepublique.gouv.gc.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

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.

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.

From: [REDACTED] [mailto:[REDACTED]]
Sent: May-22-12 9:31 AM
To: CYBERDO
Cc: CanadianTCP@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 ?

Avis de confidentialité : Ce message, transmis par courriel, est confidentiel. peut être protégé par le secret professionnel et est à l'usage exclusif du destinataire dont l'adresse figure ci-dessus. Toute autre personne est par la présente avisée qu'il lui est strictement interdit de le diffuser, le distribuer ou le reproduire. Si vous avez reçu ce courriel par erreur, veuillez m'en informer par courrier électronique et détruire immédiatement ce message et toute copie de celui-ci. Merci.

Confidentiality notice: The content of this e-mail is confidential, may be privileged and is intended for the exclusive use of the addressee. Any other person is strictly prohibited from disclosing, distributing or reproducing it. If you have received this e-mail by error, please notify me by e-mail and delete all copies. Thank you.

CYBERDO <[Redacted]>

A "CanadianTCP@ic.gc.ca" <CanadianTCP@ic.gc.ca>

cc CYBERDO [Redacted]

Objet RE: DDOS against Quebec Government (CE12-002994)

2012-05-21 10:20

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: CanadianTCP@ic.gc.ca

Cc: CYBERDO

Subject: DDOS against Quebec Government (CE12-002994)

Reference:

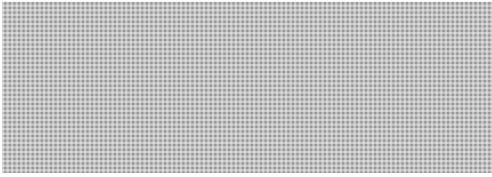
<http://www.torontosun.com/2012/05/19/quebec-liberal-government-sites-hacked>

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

Cyber Duty Officer

s.16(2)(c)

----- 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.

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 | Tél'imprimeur 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

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/\[REDACTED\]](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

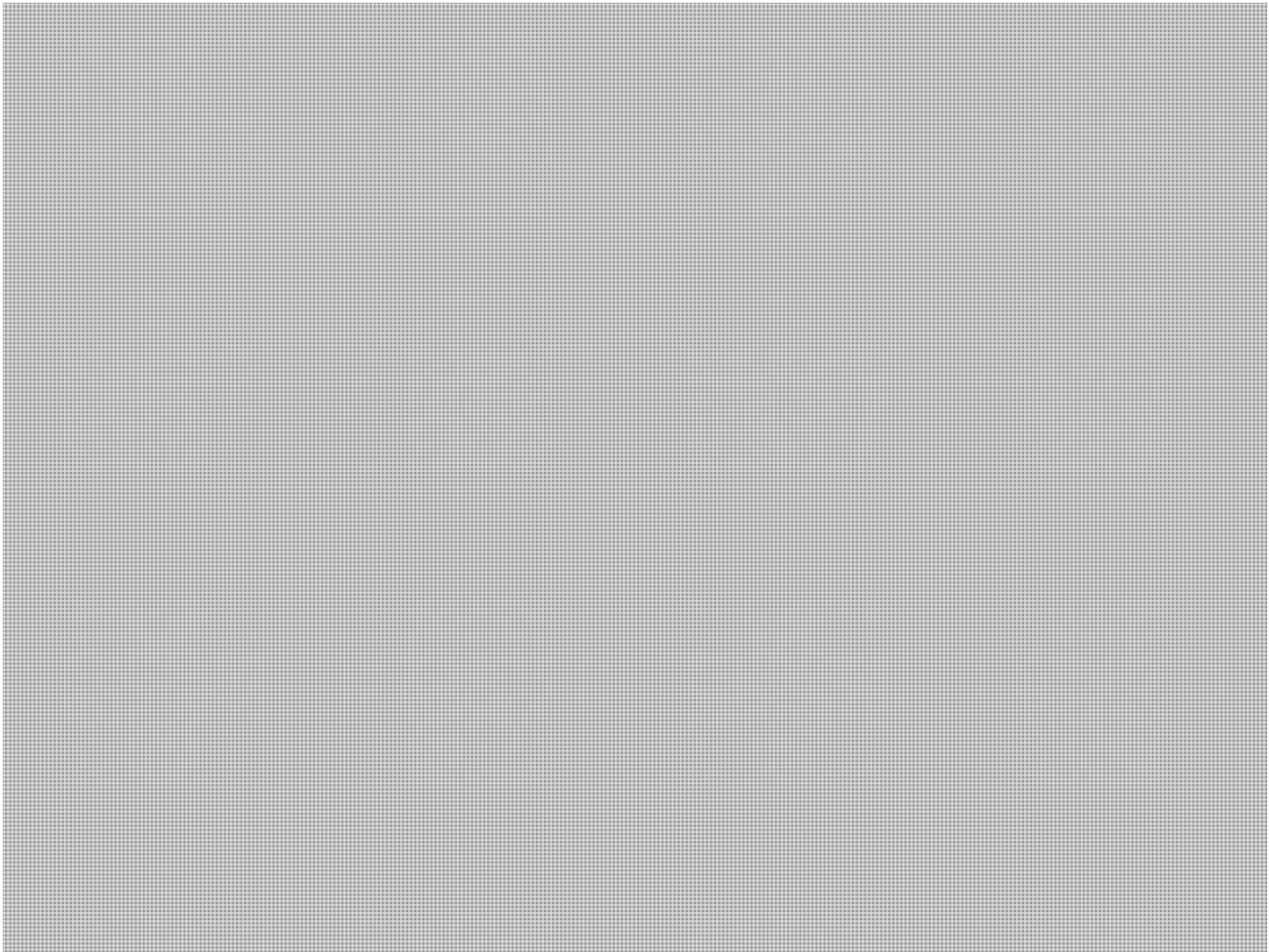
From: CYBERDO s.15(1) - Int'l
Sent: April-05-12 1:17 PM s.16(2)(c)
To: [REDACTED]
Cc: CYBERDO
Subject: RE: [REDACTED] targeted by Anonymous [CCIRC CE12-002744]

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:



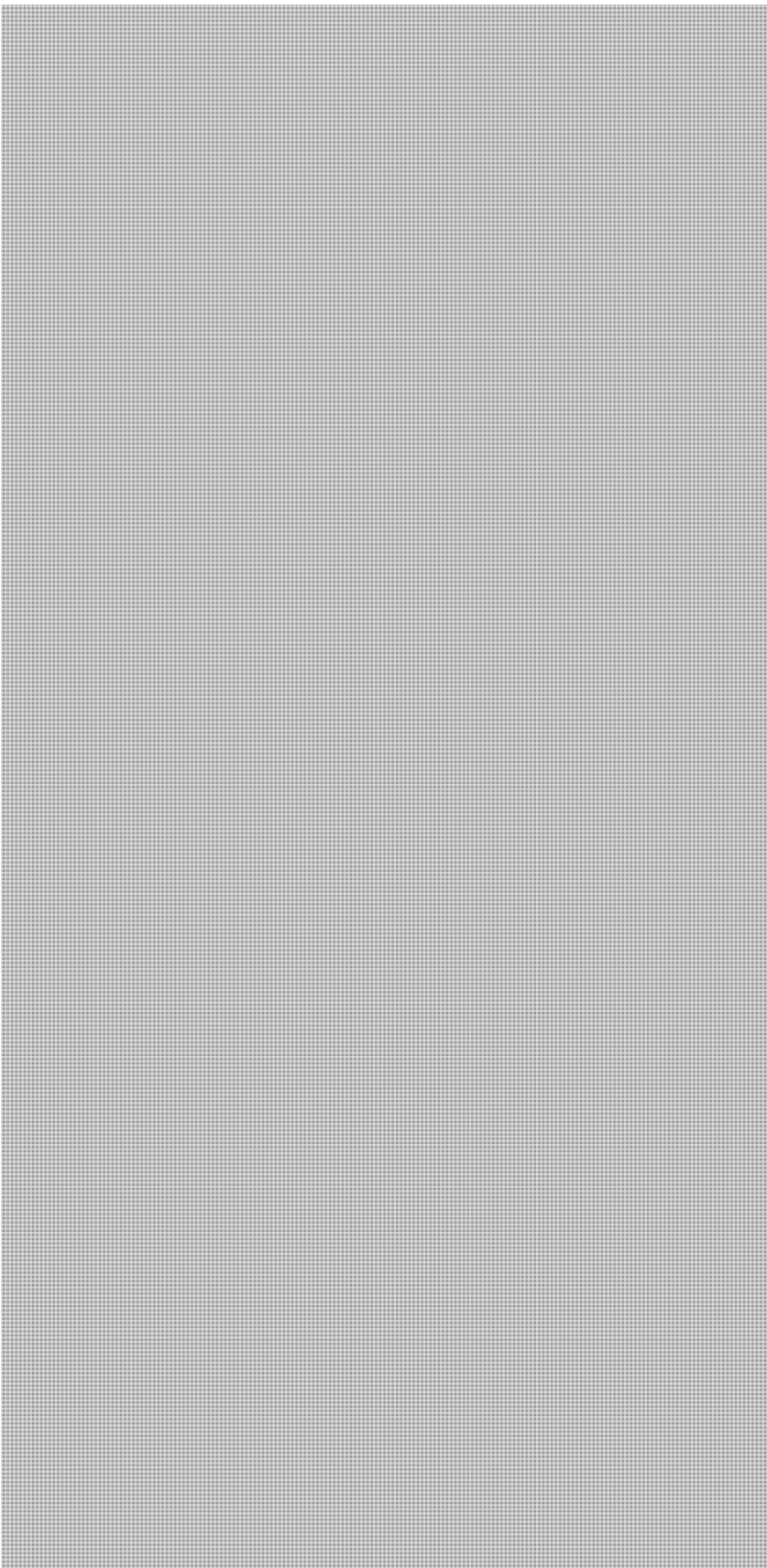
Page 1951

**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.

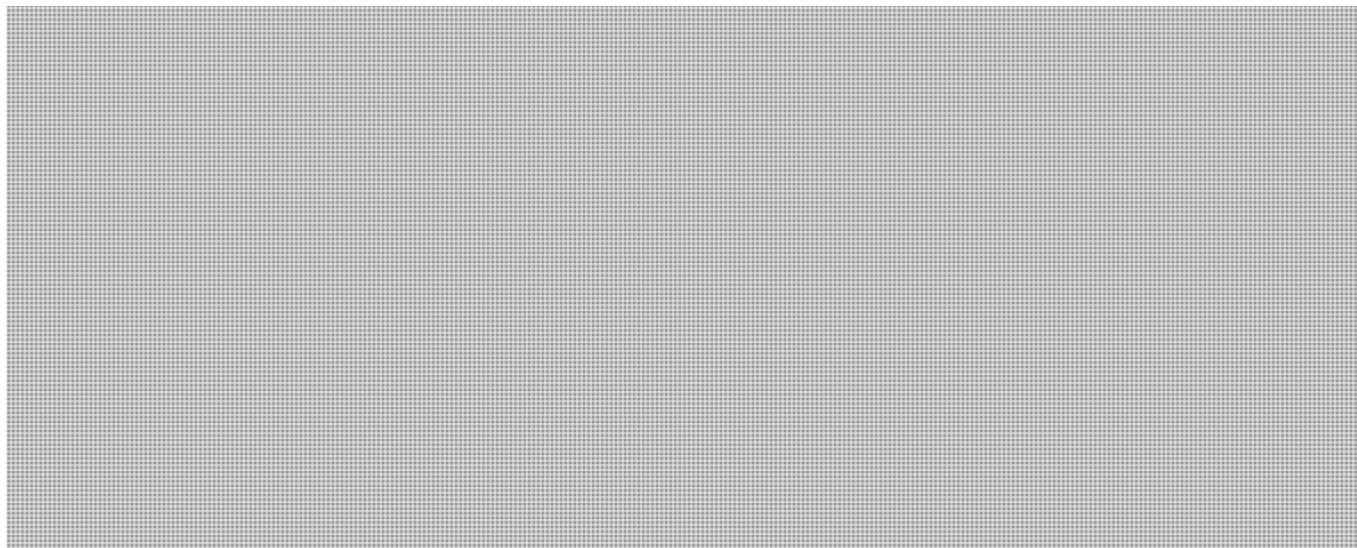
CYBERDO

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

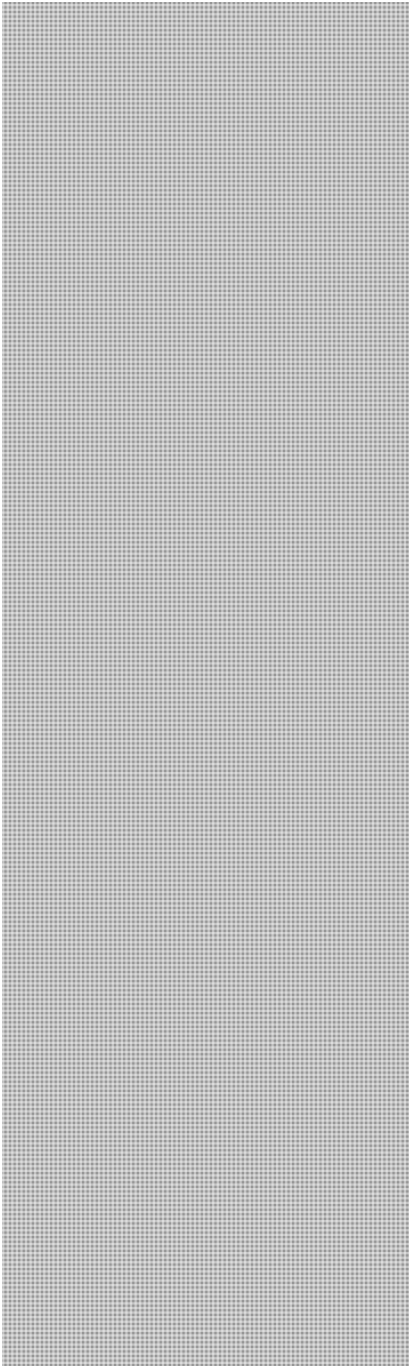
CYBERDO

From: CYBERDO
Sent: April-20-12 11:06 AM
To: [REDACTED]
Subject: Has this been caught by anyone yet?

[http://pastebin.com/\[REDACTED\]](http://pastebin.com/[REDACTED])

Here's the first little bit of the paste:

s.16(2)(c)



Page 1955

**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 s.15(1) - Int'l
To: CYBERDO s.19(1)
Subject: FW: Anonymous Dox's [REDACTED]

fyi

Have a great day,

Windy

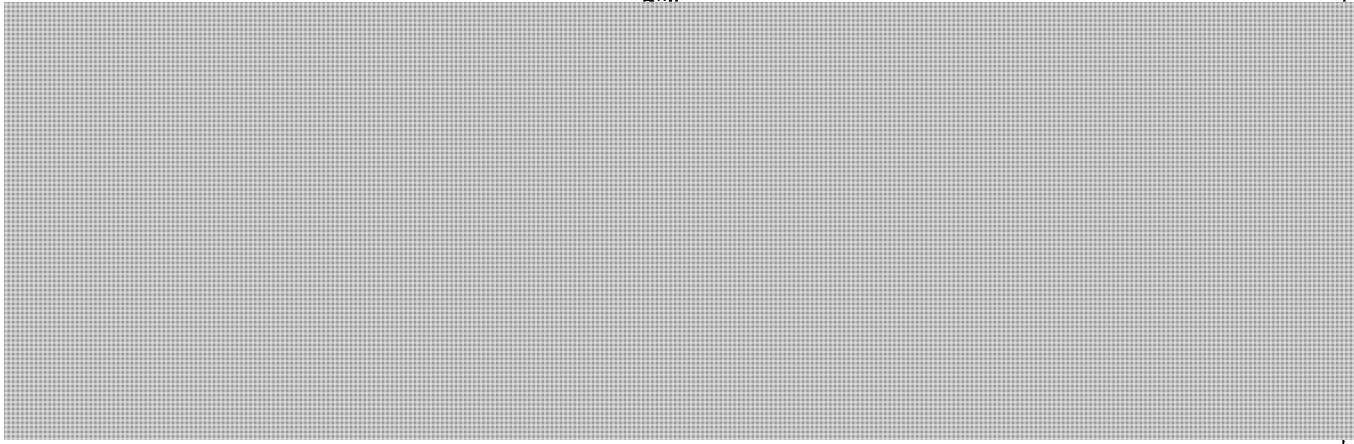
Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097
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]

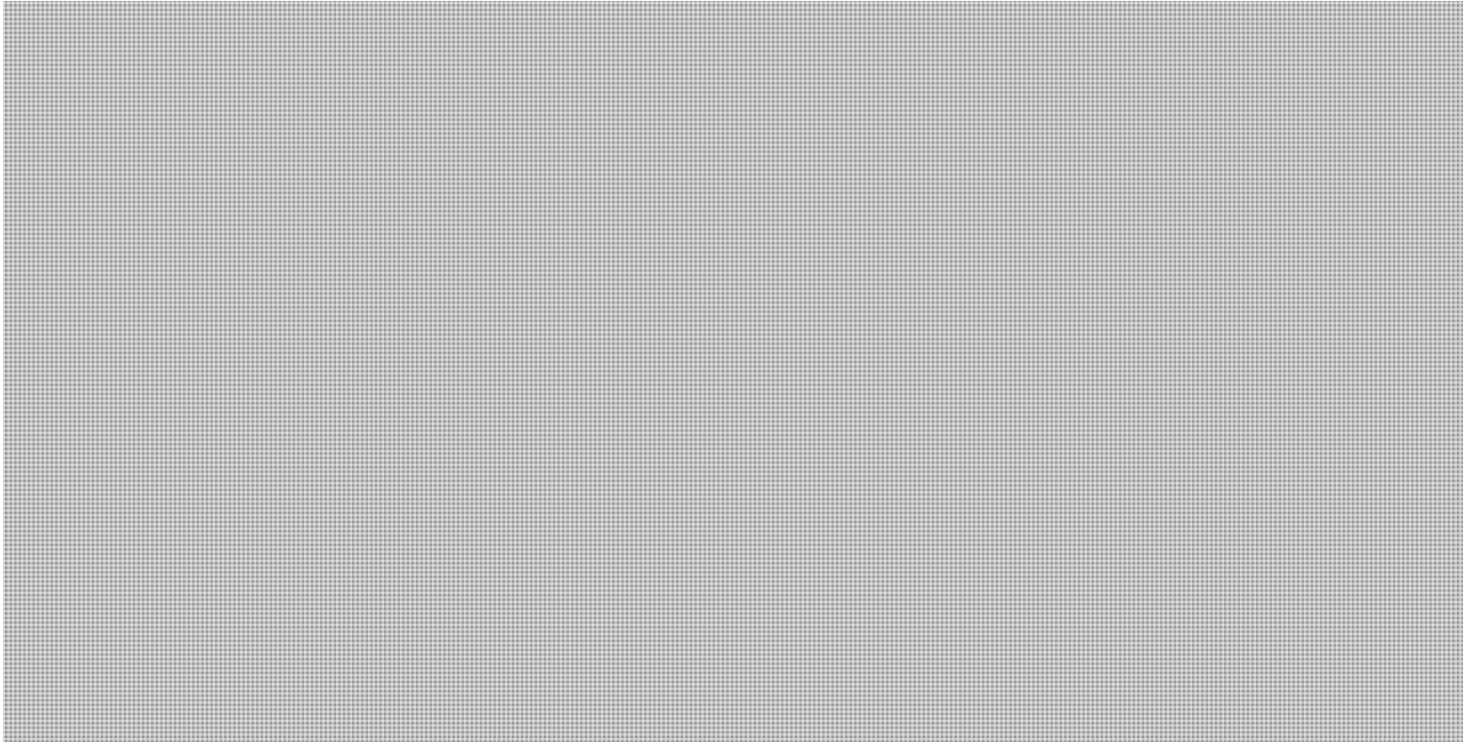
Want me to keep passing these to you?

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>; '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]



The posting of [redacted] Dox is at <http://pastebin.com/> [redacted]



s.15(1) - Int'l
s.16(2)(c)
s.19(1)

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC

s.15(1) - Int'l
s.16(2)(c)
s.19(1)

[REDACTED]
<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

-----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: [REDACTED]
Sent: April-03-12 1:36 PM
To: CYBERDO
Subject: RE: [REDACTED] 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/\[REDACTED\]](http://pastebin.com/[REDACTED])

They said that the post was labeled [REDACTED]

Regards,

[REDACTED]

-----Original Message-----

From: CYBERDO [mailto:[REDACTED]]
Sent: Tuesday, April 03, 2012 12:26 PM
To: [REDACTED]
Cc: CYBERDO
Subject: RE: [REDACTED] targeted by Anonymous [CCIRC CE12-002744]
Importance: High

[REDACTED] - for your SA, the [REDACTED] report their website is currently under DDoS. Thanks for the heads-up.

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC

[REDACTED]
<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

-----Original Message-----

From: CYBERDO
Sent: April-03-12 12:32 PM
To: [REDACTED]
Cc: CYBERDO
Subject: RE: [REDACTED] targeted by Anonymous [CCIRC CE12-002744]

Good Afternoon [REDACTED]

Many thanks for this - I've assigned event number CE12-002744 to this report.

We'll notify the [REDACTED] 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])

[http://pastebin.com/\[REDACTED\]](http://pastebin.com/[REDACTED])

Thought you guys would want to know.

Regards,

[REDACTED]

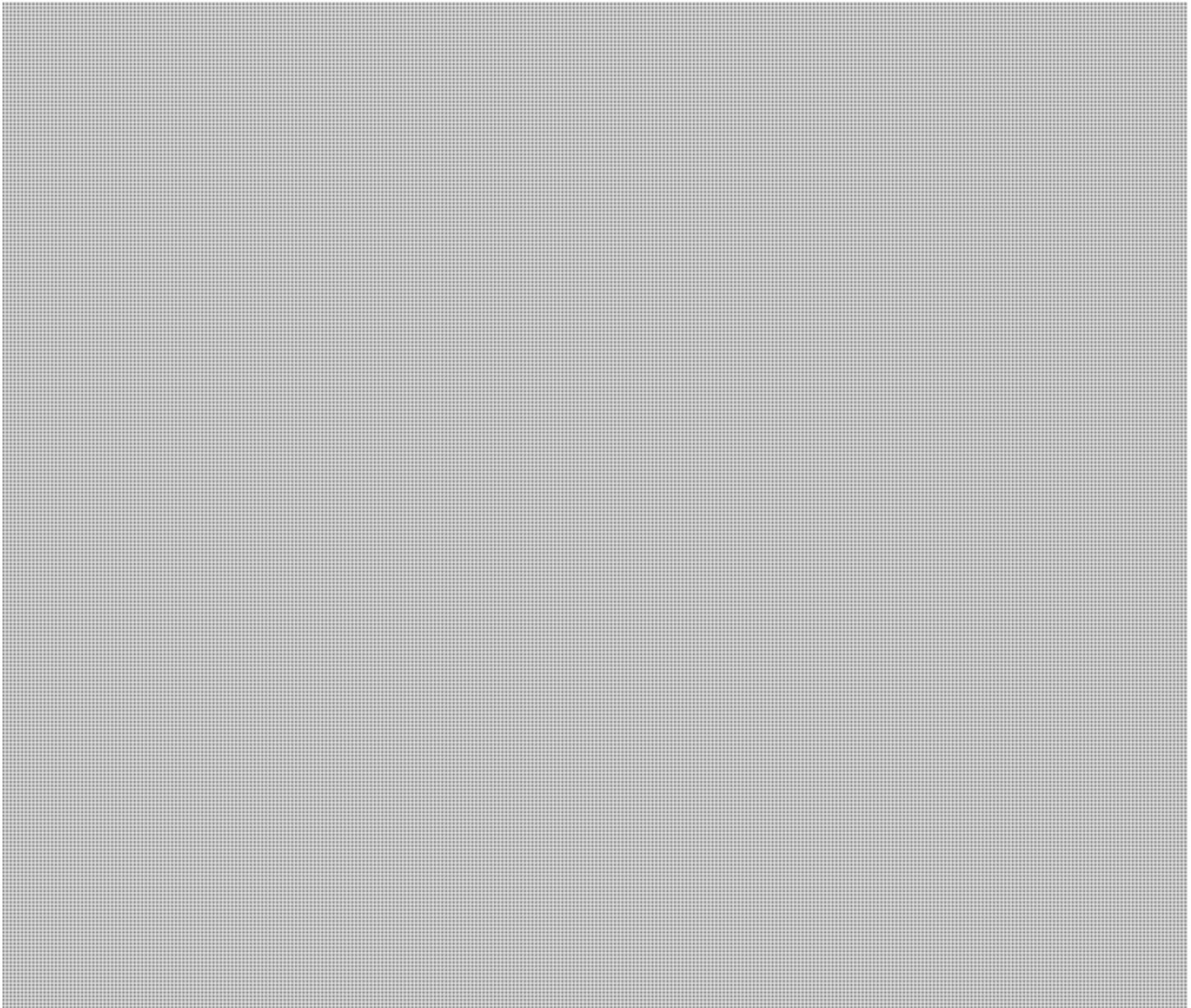
CYBERDO

From: CYBERDO
Sent: April-05-12 11:58 AM
To: [REDACTED] s.16(2)(c)
Cc: [REDACTED] CYBERDO s.19(1)
Subject: CCIRC CE12-002744 [Analysis Report]
Importance: High

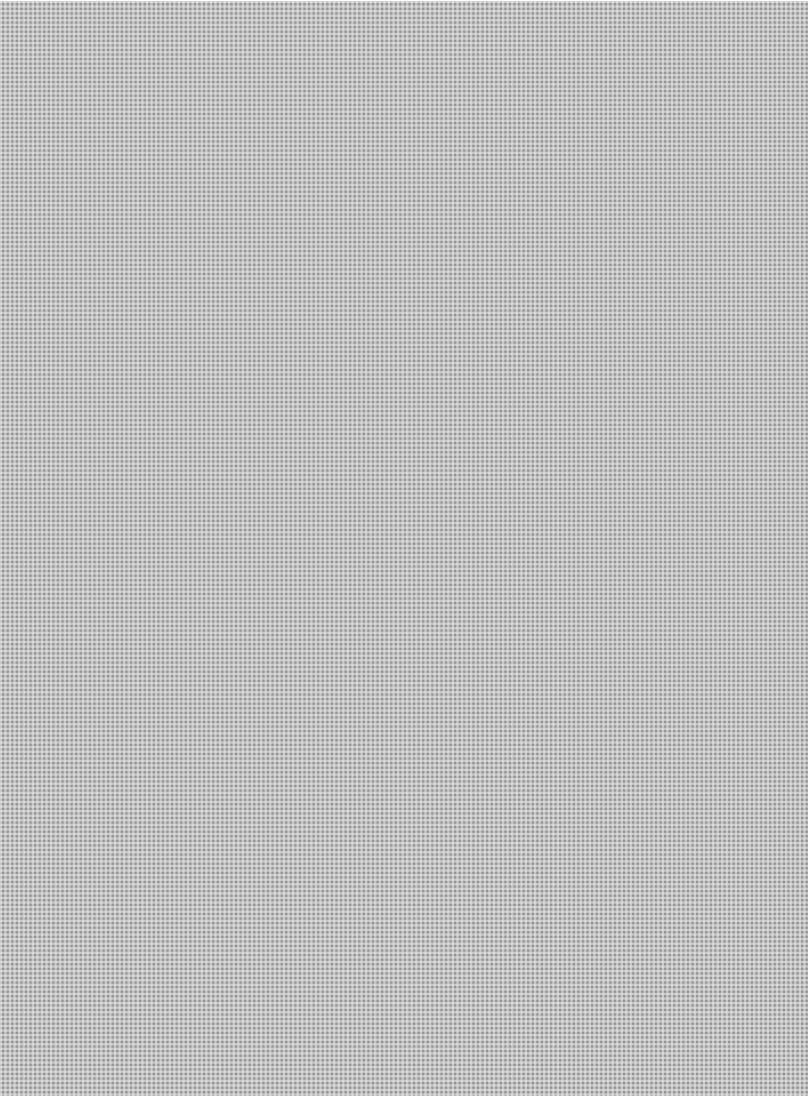
Hi again [REDACTED]

CCIRC technical analysis completed of the [REDACTED] Indicators have been identified that could assist [REDACTED] in filtering [REDACTED] from "lazy" attackers (script kiddies who have not modified the original script).

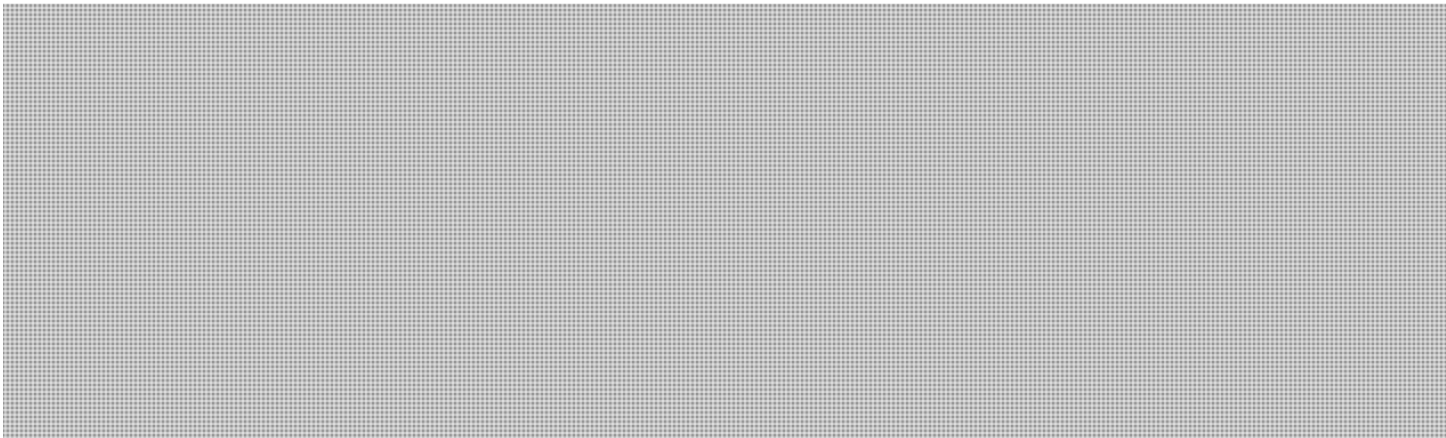
Analysis summary:



s.16(2)(c)

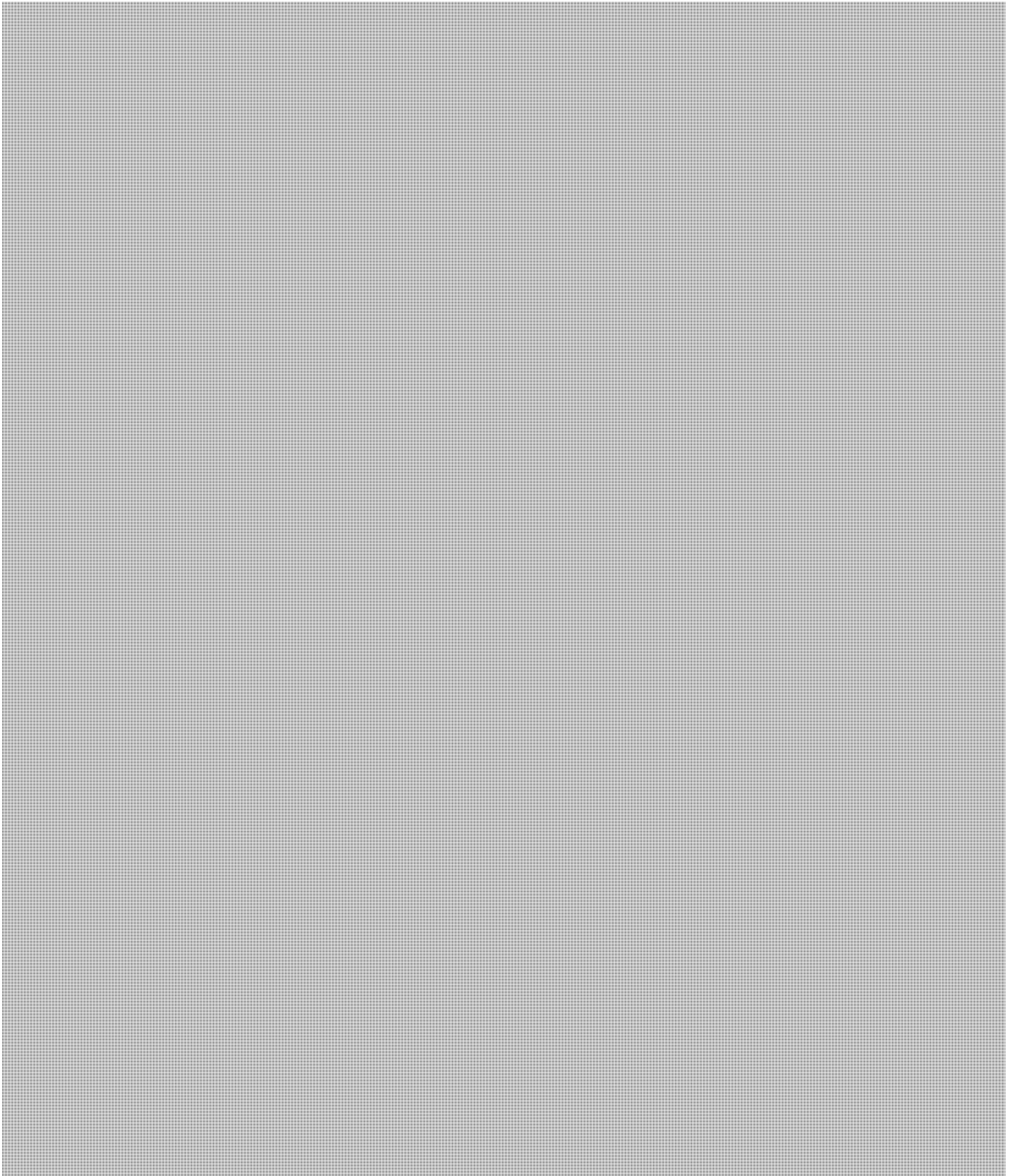


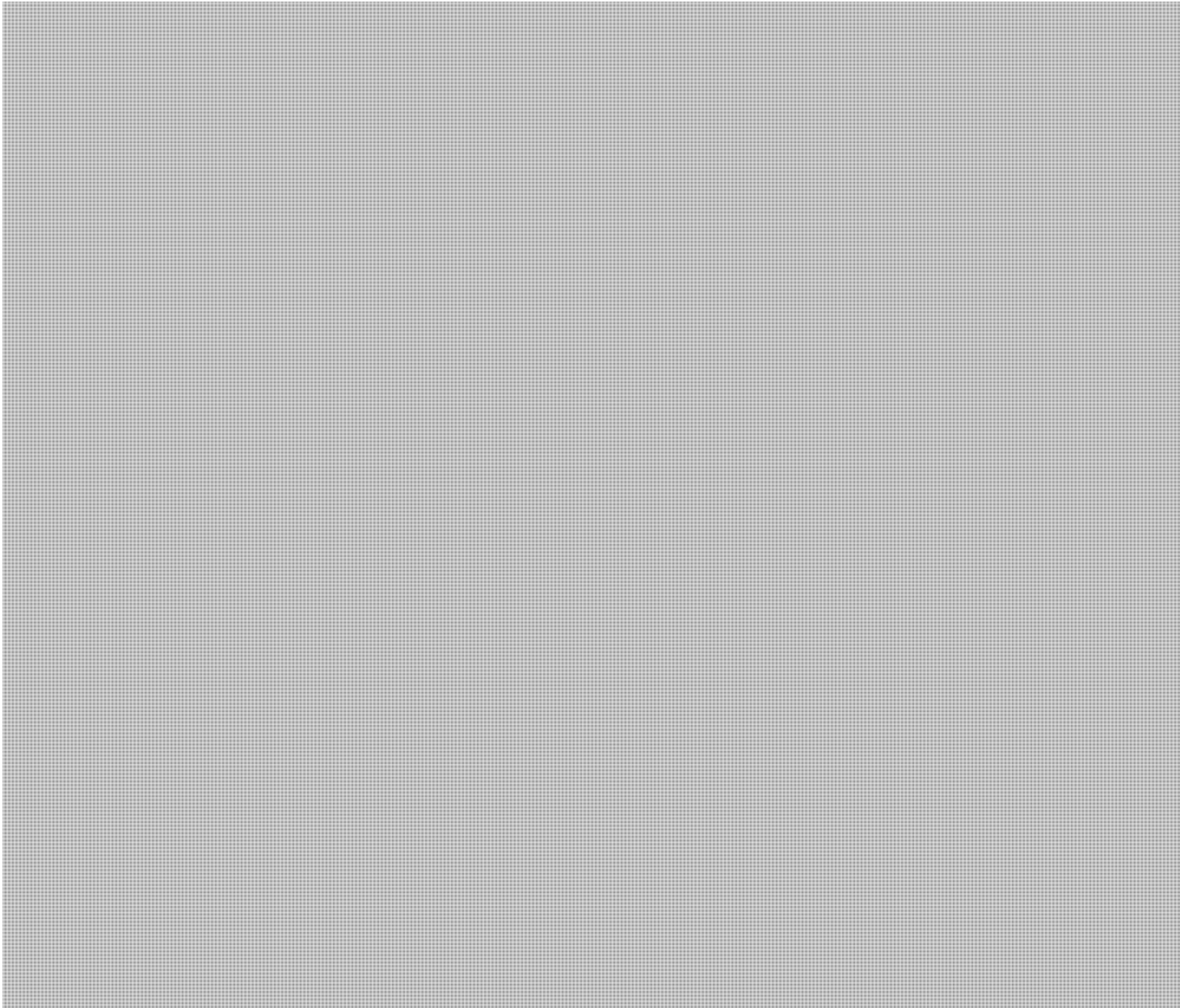
Additionally, as I mentioned during our earlier telecon at 9:20AM; CCIRC recently conducted an assessment of the [REDACTED] I have provided our analysis below for your awareness in case this tool is later used against your infrastructure.



Full CCIRC Technical Analysis of [REDACTED] is below.

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)

-----Original Message-----

From: CYBERDO [mailto:]

Sent: Wednesday April 4, 2012 9:07 AM

To: CYBERDO

Cc:

Subject: RE: CCIRC CE12-002744

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 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

<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

-----Original Message-----

From:

Sent: April-04-12 8:58 AM

To: CYBERDO

Cc:

Subject: RE: CCIRC CE12-002744

Good Morning,

Yesterday's attack seems to have been rather small. you've provided us with.

It would appear that an attack is still on-going, from judging by the But, it is having no effect

[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: [Redacted]
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. *****

***** 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 Superintendent 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 Crieckingen, 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, Christopher; 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 government 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!

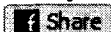
Mark Matz
Director, Policy and Issues Management /
Directeur, Politiques cyber et gestion des enjeux
NATIONAL CYBER SECURITY / CYBERSÉCURITÉ NATIONALE
613-993-9635

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!



Tuesday April 3, 2012 7:34 Kady

10:00

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]



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!



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

happenance, on to the topic currently confronting the committee, I will leap into action.



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?)



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?



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.)



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.



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.)



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.)



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.



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.)



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.



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.



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.



Tuesday April 3, 2012 11:37 Kady

11:37 **Kady:**

CSE ProTip: Always patch your software when upgrades are available!



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.



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!



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.



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.)



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.)



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.



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.)



Tuesday April 3, 2012 11:59 Kady

12:03 Kady:

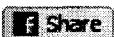
Malizia **did** mention Anonymous, I should note, albeit in passing, and characterized them as a "movement with no official membership". Meanwhile, we've moved to questions, and Albrecht is once again attempting to get us to take this threat with the solemnity it merits (done!). He reads the alleged threats included in the video into the record -- for the second time, for those keeping track -- and wonders where, in the "contium 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.



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.



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.



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.



Tuesday April 3, 2012 12:11 Kady

12:14 Kady:

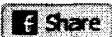
Comartin tries to get Malizia to confirm whether the investigation extends beyond the Youtube video to physical threats. Nice try, but no chance, sir. Also, Easter notes that asking for a minister's resignation is *not*, in fact, a threat -- he's asked for a few himself, he recalls, and doesn't want 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.



Tuesday April 3, 2012 12:14 Kady

12:20 Kady:

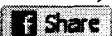
It's Come To This II: Easter wonders why, in his opening statement, C-CIRC advisor Robert Gordon emphasized security from threats *outside* government, and wondering why, exactly, he employed such syntax. Gordon seems bemused. Back to Anonymous for a moment -- if he/she/it is identified, and turns out 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.



Tuesday April 3, 2012 12:20 Kady

12:24 Kady:

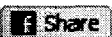
Back to the Conservative side of the table, and Greg Kerr, who begins by thanking the witnesses for being here, despite "trepidation" and an inability to say everything about what they know, he gives Malizia the opportunity to repeat -- for the third time, very nearly word for word -- his opening statement 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.



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.



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.



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.



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.)



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.



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.



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!



Tuesday April 3, 2012 12:40 Kady

12:42

COVERITLIVE *Thank you for reading today.*

Thousands of Users. Millions of Readers.
Free and simple to use. Try CoveritLive today!

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; Brownness, 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 Hactivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hactivistes 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: Hactivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property

1. Information Note IN12-501 Overview of the Hactivist 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 hactivist 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 Hactivist 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 hactivists. 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*

Proulx, Véronique

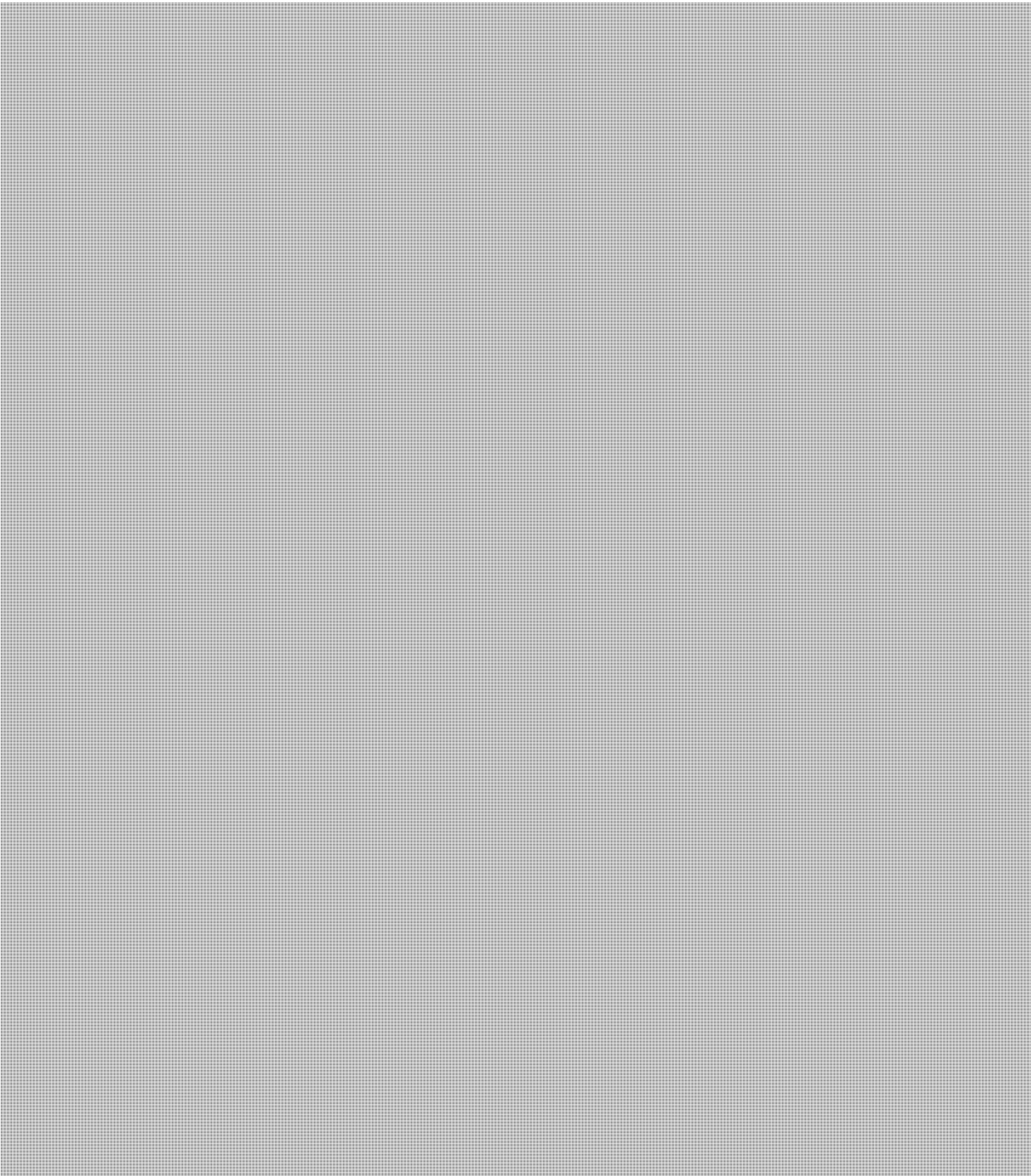
From: Pilon, Claude
Sent: March-27-12 4:24 PM
To: Proulx, Véronique
Cc: Bradley, Kees
Subject: RE: Another tasking from Robert with respect to his Parliament Meeting

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 / claudio.pilon@ps-sp.gc.ca

**PROTECTED: SOLICITOR-CLIENT PRIVILEGE/PROTÉGÉ: PRIVILÈGE 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,

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,

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 / claudio.pilon@ps-sp.gc.ca

**PROTECTED: SOLICITOR-CLIENT PRIVILEGE/PROTÉGÉ: PRIVILÈGE DU SECRET
PROFESSIONNEL DE L'AVOCAT**

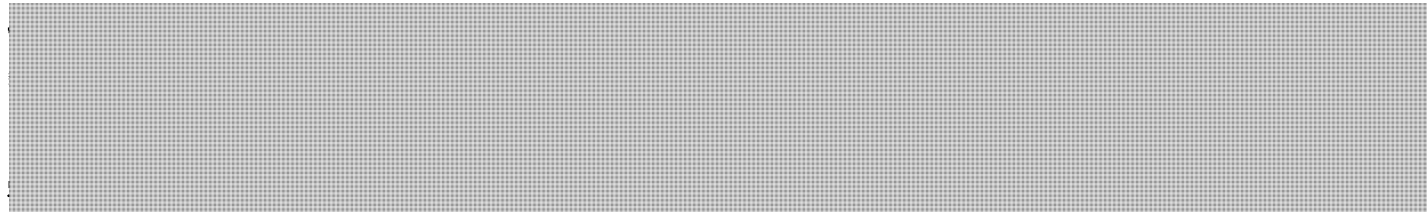
Please feel free to reply in the official language of your choice/ N'hésitez pas à me répondre dans la langue officielle de votre choix

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



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



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 0P8
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,



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] s.15(1) - Int'l
Cc: CYBERDO; [REDACTED] s.16(2)(c)
Subject: FW: CCIRC CE12-2682 [DDoS website hosted in Sweden]

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 Service (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.](http://canopycanopycanopy.com/15/our_weirdness_is_free)

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 1999 to / à 2001
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

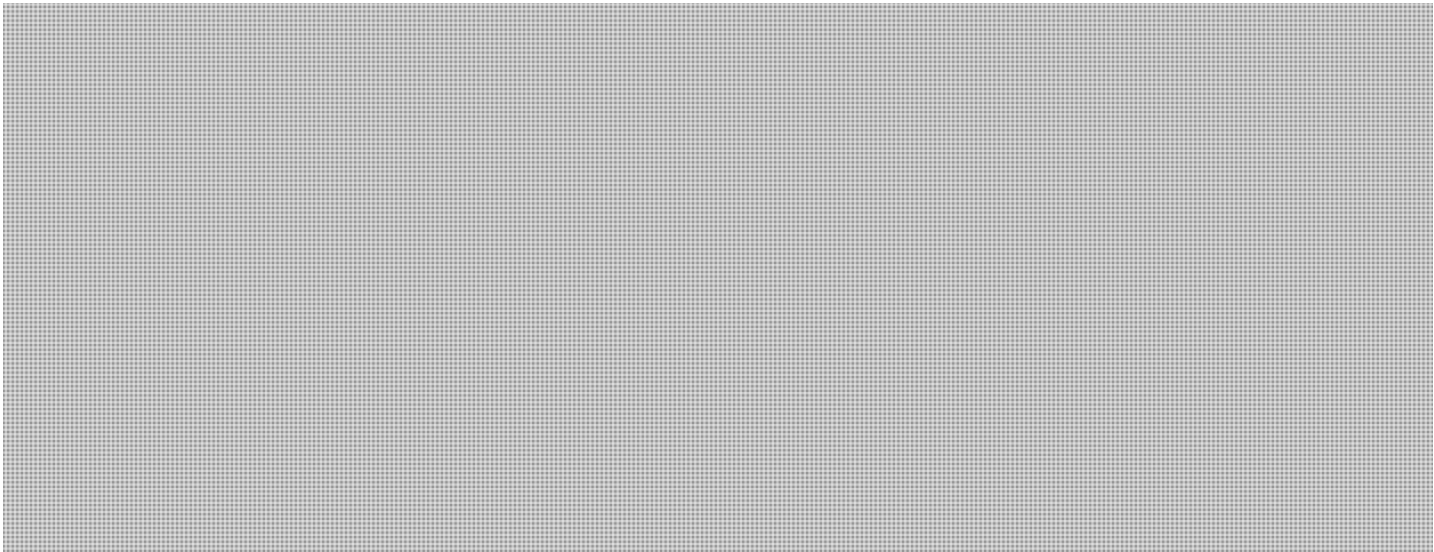
s.16(2)(c)

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 Hactivist 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](http://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

Untitled

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, 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. 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 and 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.

Untitled

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.

Untitled

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:

Untitled

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 Tarmageddon (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:

Untitled

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

Untitled

(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->

Untitled

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
Page 8

Untitled

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 logiciels malveillants (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, TeaMp0ison 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

Untitled

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.

Untitled

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 (Australie)

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.

Untitled

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

Untitled
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,

Untitled

#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).

Untitled

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 Anonymous 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.

Untitled

(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 loi 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

From: CYBERDO s.16(2)(c)
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
image has
been under
cyberdo
so will*

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



Provided by NewsDesk

<http://www.infomedia.gc.ca/allcontent/>

Fourni par InfoMÃ©dia

Published | PubliÃ©: 2012-03-07
Received | ReÃ§u: 2012-03-07 3:20 AM

THE GLOBE AND MAIL
CANADA'S NATIONAL NEWSPAPER • FOUNDED 1858

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.

**Media contents in NewsDesk are
copyright protected.**

Please refer to **Important Notices** page for
the details.

**Le contenu médiatique d'InfoMedia est protégé
par les droits d'auteur.**

Veillez vous reporter à la page des **avis importants** pour les
détails.

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)

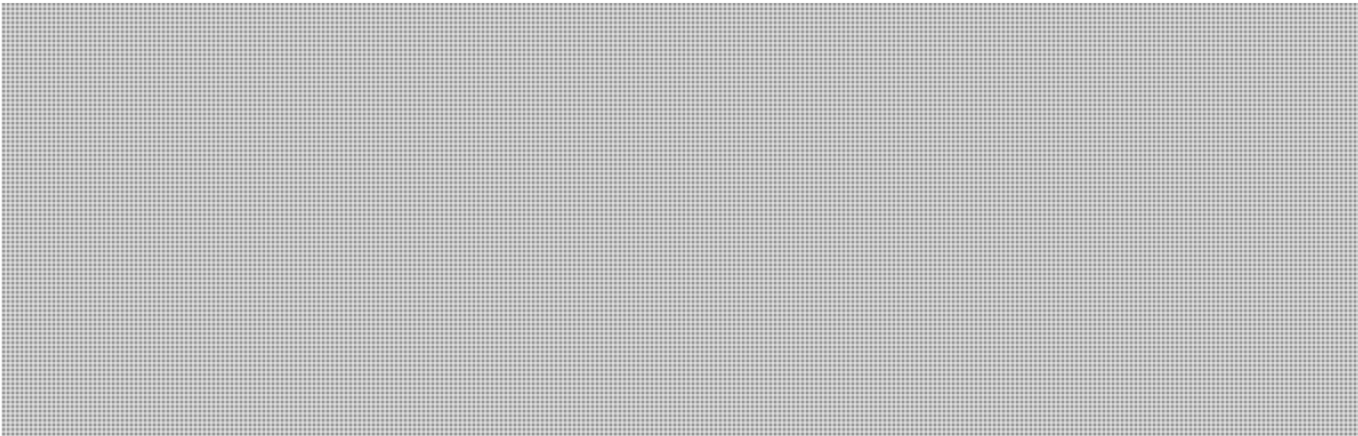
CTEC,

FYI and something to monitor on your end.

Luc

[http://pastebin.com/\[REDACTED\]](http://pastebin.com/[REDACTED])

Description:



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 accidentally 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.

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 or copying of the contents of this communication by anyone other than the intended recipient is strictly prohibited without the consent of the originator. 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 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 zombimètres (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 contre 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 équilibrateurs 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 fournisseurs 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)

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]

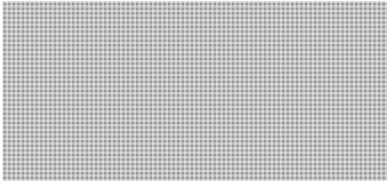
Executive Summary

[REDACTED]

**Pages 2050 to / à 2051
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 2062
is a duplicate
est un duplicata**

**Page 2063
is a duplicate
est un duplicata**

**Page 2064
is a duplicate
est un duplicata**

**Page 2065
is a duplicate
est un duplicata**

**Page 2066
is a duplicate
est un duplicata**

**Page 2067
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)'; [REDACTED]
Cc: CYBERDO; 'Lee Shields (Lee.Shields@rcmp-grc.gc.ca)'; Bergeron, Dominic; Anderson, Windy; Bendelier, Kenneth
Subject: RE: Anonymous and Minister of PS
Attachments: [REDACTED]

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/\[REDACTED\]](http://pastebin.com/[REDACTED])

Cyber Duty Officer
Public Safety Canada
CCIRC
[REDACTED]
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); [REDACTED]
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]
Sent: February-20-12 11:58 AM
To: Beaudoin, Luc
Cc: CTEC
Subject: RE: Anonymous and Minister of PS

s.15(1) - Subv

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.

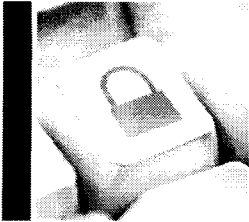
More than 100,000 people have signed an Openmedia.ca petition opposing the bill, and online comment boards are packed with users expressing concern about its privacy implications. But pollster Darrell Bricker said it's unlikely that most people in the broader public would have paid attention to the issue 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

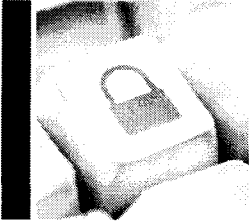
This report provides an overview of the hacktivist group, "Anonymous" and contains: information on its organizational structure, tradecraft, and targets; the threat to GC systems; and, CTEC's prevention and mitigation advice. "Anonymous" targets governments, private firms and individuals whose activities 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 (IRC¹); 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 (DDoS²), password cracking, SQL injections³, 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-ops⁵, LulzSec⁶) 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 LulzRaft⁷.

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several "unofficial" spokespeople⁸, 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.)

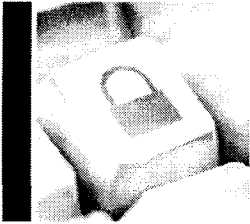
CHOOSING TARGETS

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. HBGary¹⁰), 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 Occupy¹¹ 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):

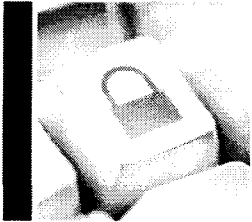
Action: DDoS attack against the Australian Parliament's website and web defacement of the Prime Minister's website.

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 applications¹².



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 Spring¹³.

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 Bay¹⁴ 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 Act¹⁵, 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):

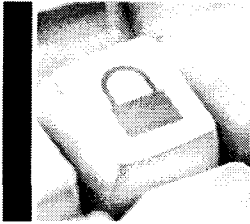
Action: In November, Anonymous threatened action against the US government.

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 employees¹⁷.

Municipal Governments:

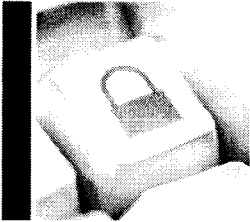
TORONTO (November 2011):

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 legislation¹⁸ 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 Facebook¹⁹.)

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.)

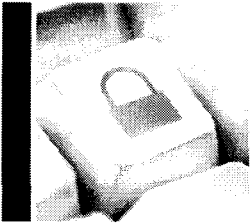
Open Source resources:

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:

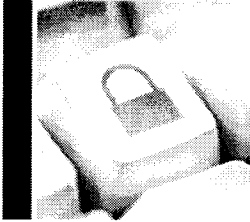
Anonymous developed and released a Perl DDoS tool in September, #RefRef, that exploits SQL²¹ vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline. #RefRef could be 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 Fawkes²² 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 recommended²³. In addition, the following mitigation is available for some of the tradecraft²⁴ 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.

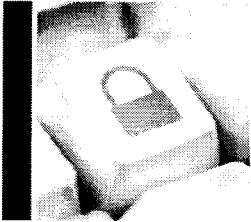
b) In some cases, if a DDoS is anticipated, it may be possible to temporarily have additional bandwidth provisioned to your network. This will lessen the impact on the target for some DDoS incidents.

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 hardened²⁵ 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.

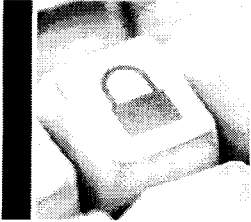
8 Unofficial spokespeople for Anonymous include Jake Davis (also known by his online nickname "Topiary,") Barrett Brown, etc. For more information on Jake Davis, please see <http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-ukpolice/>. For more information on 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 2083
is a duplicate
est un duplicata**

**Page 2084
is a duplicate
est un duplicata**

**Page 2085
is a duplicate
est un duplicata**



Canada

[Home](#) > [National security](#) > [Cyber Security: A Shared Responsibility](#) > [Cyber Security Publications](#) > [Analytical releases 2012](#) > [TR12-001: Mitigation Guidelines for Denial-of-Service Attacks](#)

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. <ul style="list-style-type: none"> ■ 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.		

TR12-001: Mitigation Guidelines for Denial-of-Service Attacks

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 accidentally 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 ICMP 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: <ul style="list-style-type: none"> ■ 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.

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 or copying of the contents of this communication by anyone other than the intended recipient is strictly prohibited without the consent of the originator. 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.

[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 s.16(2)(c)
Sent: February-17-12 1:27 PM s.20(1)(c)
To: CYBERDO; Anderson, Windy
Cc: Beaudoin, Luc
Subject: RE: CCIRC ACT 3497 FW: DDOS Parl.gc.ca

Windy;

Update: CTEC was informed of the DDoS at 08:34 AM this morning. At 9:11 AM Shared Services Director advised CTEC the following;



Still no further request for assistance requested for CTEC or CCIRC.

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: CCIRC ACT 3497 FW: DDOS Parl.gc.ca
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 House of Commons and Shared Services.

Shared Services is working with [REDACTED] and has advised CTEC 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

s.16(1)(b)

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

From: [REDACTED]
Sent: February-17-12 1:10 PM
To: stephan.aube@parl.gc.ca; Beaudoin, Luc; CYBERDO
Subject: RE: DDOS Parl.gc.ca
Importance: High

Hi All,

As you may be aware, parl.gc.ca 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]

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 aujourd'hui.

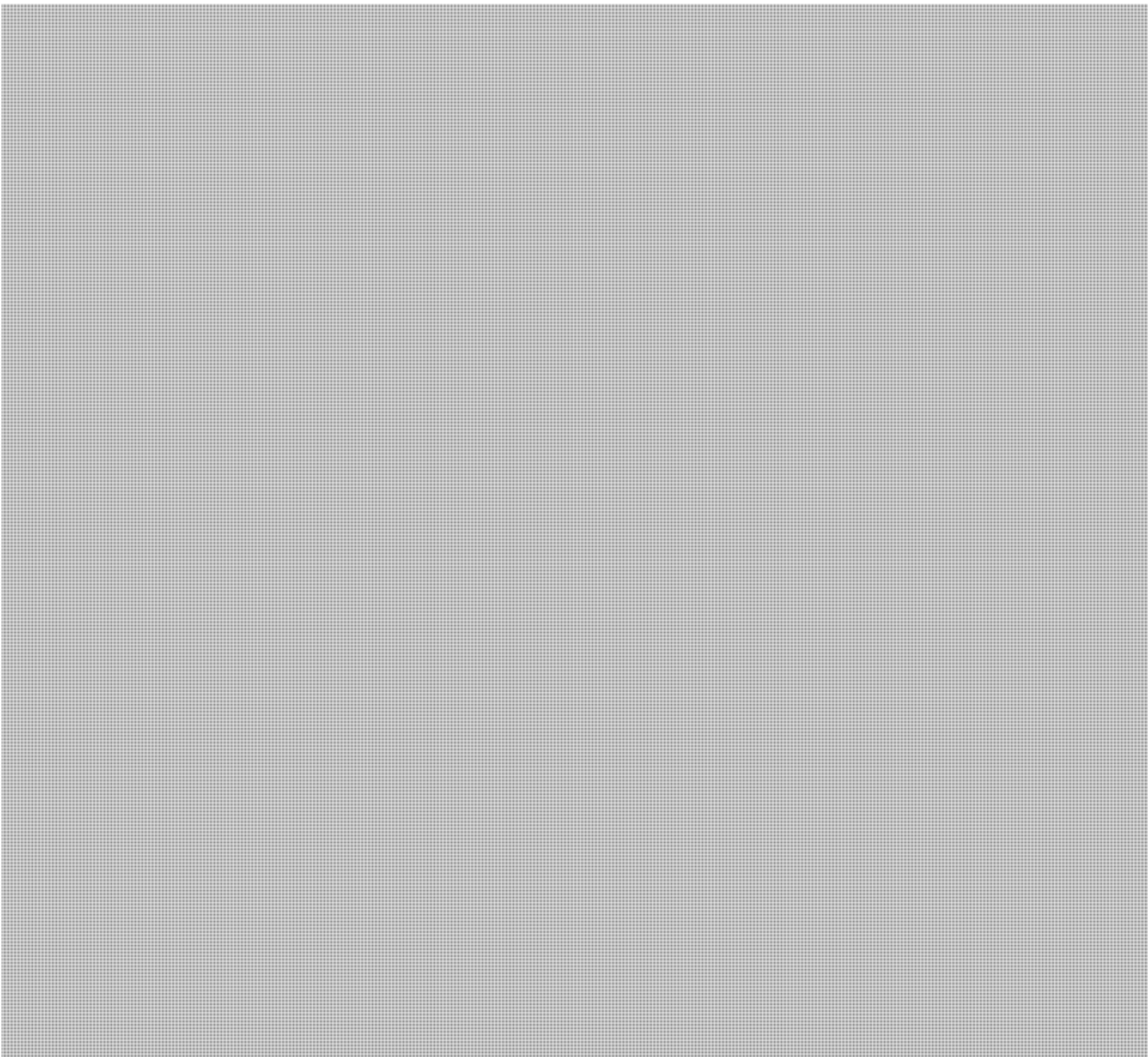
Le booster est parl.gc.ca

[REDACTED]

<http://search.mibbit.com/channels/AnonOps>

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: [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

FN 12-502

BUILDING A SAFE AND RESILIENT CANADA

ANONYMOUS

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).

created
Feb 17, 2012
Consult
CSGC

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
(IRC¹); 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 (DDoS²), password cracking, SQL injections³, 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 ATEP
- I recommend
throwing this version
002096



CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

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, "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 LulzRaft⁷.

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several "unofficial" spokespeople⁸, 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. HBGary¹⁰), 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 Occupy¹¹ 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 applications¹².



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 Spring¹³.

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 Bay¹⁴ 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 Act¹⁵, 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 employees¹⁷.

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 legislation¹⁸ 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 Facebook¹⁹.)

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:

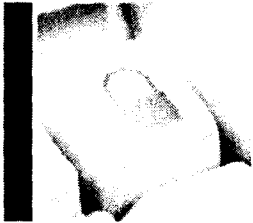
Anonymous developed and released a Perl DDoS tool in September, #RefRef, that exploits SQL²¹ vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline. #RefRef could be 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 Fawkes²² 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 recommended²³. In addition, the following mitigation is available for some of the tradecraft²⁴ 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.

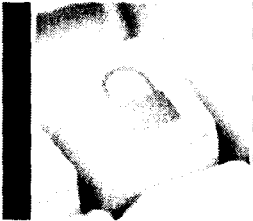
b) In some cases, if a DDoS is anticipated, it may be possible to temporarily have additional bandwidth provisioned to your network. This will lessen the impact on the target for some DDoS incidents.

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 hardened²⁵ 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; [REDACTED] Beaudoin, Luc
Subject: Re: [Activity 3497] RE: DDOS [REDACTED] s.16(1)(b)
s.16(2)(c)

Thank you Bruce !

Stephan

----- Original Message -----

From: CYBERDO [mailto:[REDACTED]]
Sent: Friday, February 17, 2012 01:20 PM
To: [REDACTED] Aubé, Stéphan; Beaudoin, Luc <LucS.Beaudoin@ps-sp.gc.ca>
Cc: CYBERDO [REDACTED]
Subject: [Activity 3497] RE: DDOS [REDACTED]

Good Afternoon [REDACTED]

We have forwarded your report to CTEC, who is the Federal CIRT. They 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

[REDACTED]
<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

-----Original Message-----

From: [REDACTED] [mailto:[REDACTED]]
Sent: February-17-12 1:10 PM
To: stephan.aube@parl.gc.ca; Beaudoin, Luc; CYBERDO
Subject: RE: DDOS [REDACTED]
Importance: High

Hi All,

As you may be aware, [REDACTED] 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

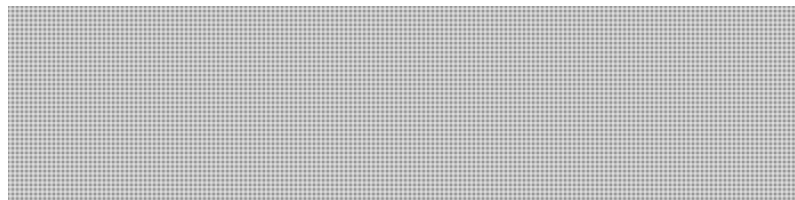
Dir. Opérations des TI, Chambre des communes Dir. IT Operations, House of Commons 181, Queen, bureau-room 6-028,
Ottawa, Ontario, Canada K1A 0A6

Tel.: (613)992-7449 - Fax: 613-947-6292 - E-Mail : aubes@parl.gc.ca

Regards,



s.16(1)(b)



From: 

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)

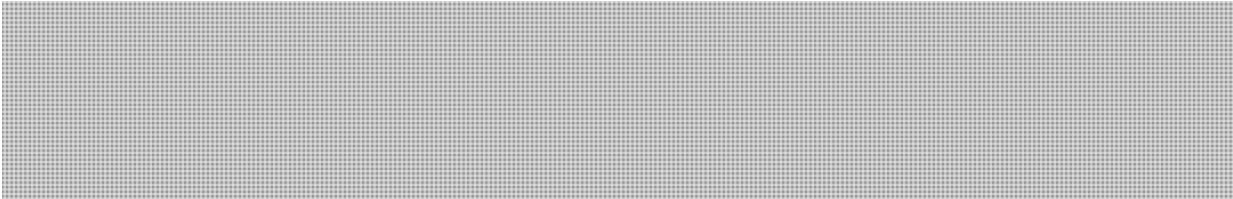
Poste aujourd'hui.

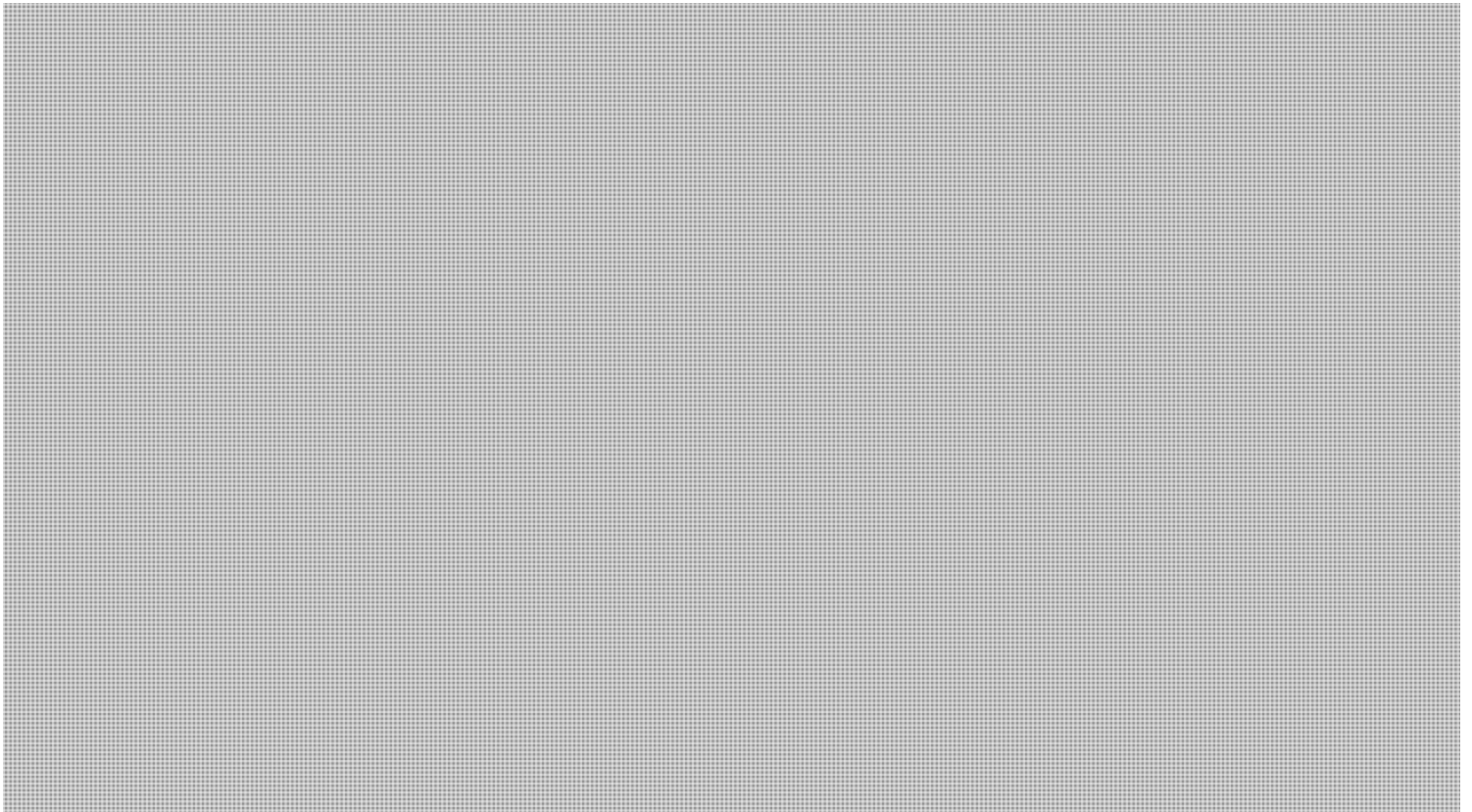
s.16(1)(b)

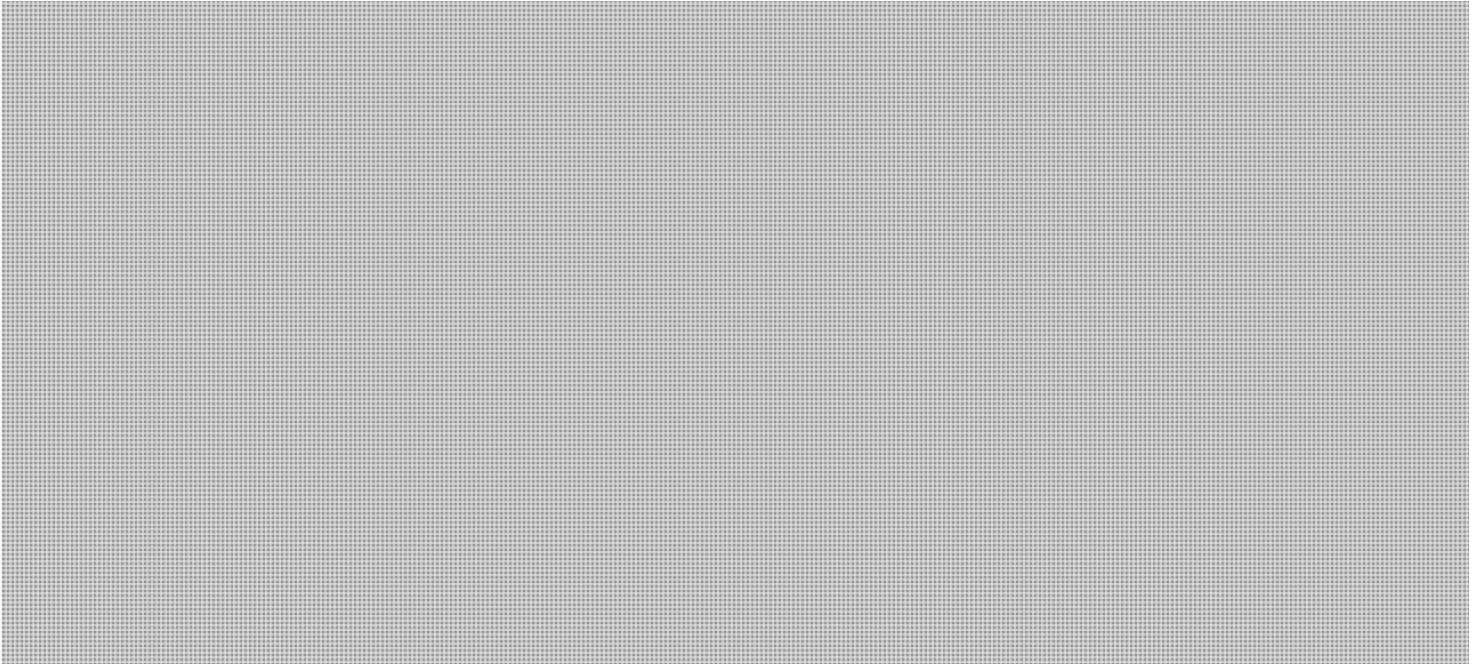
s.16(2)(c)

Le booster est 









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: [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

**Page 2111
is a duplicate
est un duplicata**

**Page 2112
is a duplicate
est un duplicata**

**Page 2113
is a duplicate
est un duplicata**

**Page 2114
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!

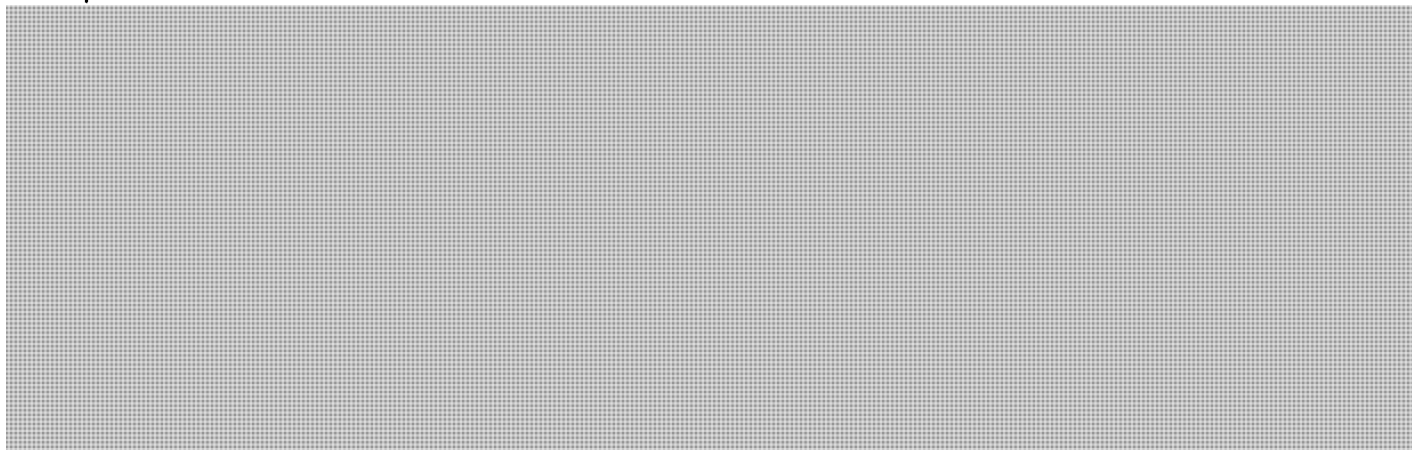
Bruce Moore
Public Safety Canada
CCIRC
Cyber Duty Officer

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*

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)

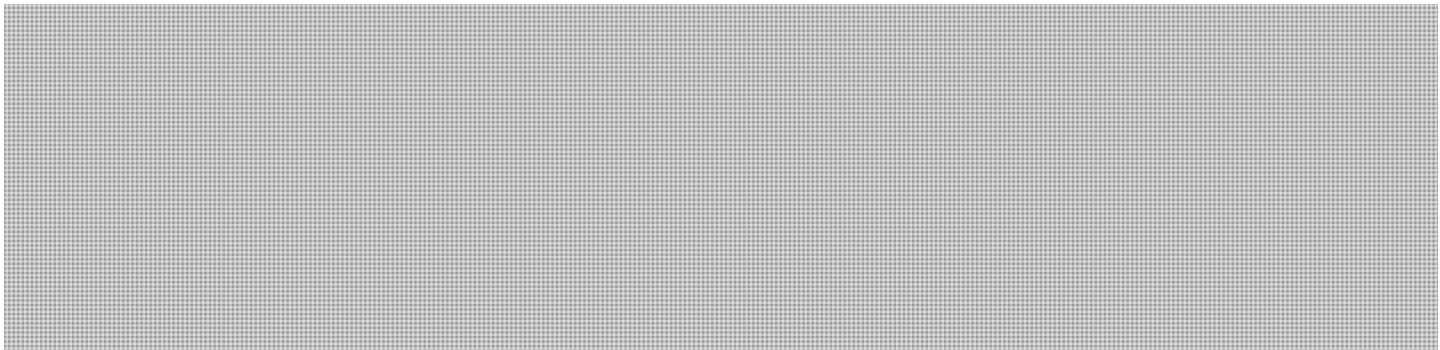
s.20(1)(c)


Security Evangelist

Team Cymru

<http://www.team-cymru.org/About/contact.html>

'To communicate simply you must understand profoundly'



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 0P8
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"

s.16(2)(c)
s.19(1)
s.20(1)(c)

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>; CanadianTCP@ic.gc.ca <CanadianTCP@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: CanadianTCP@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.

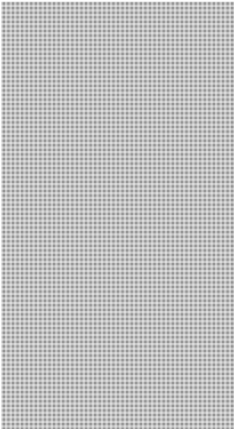
I have pasted a portion of the text below and here is the link:

[http://pastebin.com/\[REDACTED\]](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 Servers on 31 March 2012.

Request CTCP members evaluate and provide comments back to IC and CCIRC.

Pastebin URL: <http://pastebin.com/> [redacted]

Thanks

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC

[redacted]
<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 Servers on 31 March 2012.

Request [REDACTED] members evaluate and provide comments back to IC and CCIRC.

Pastebin URL: [http://pastebin.com/\[REDACTED\]](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: CanadianTCP@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:

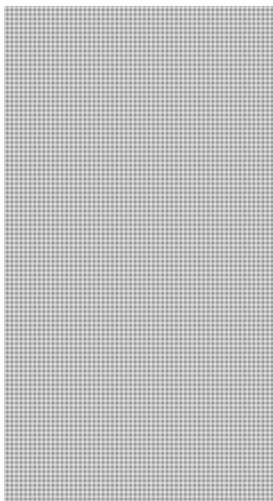
<http://pastebin.com/> 

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:



CYBERDO

From: CYBERDO
Sent: October-28-11 2:06 PM
To: [REDACTED]
Cc: 'Alain.Labossiere@ic.gc.ca'; Ron Rimnyak; CYBERDO
Subject: Anonymous is targetting TSE on Nombor 7th, 2011 (CCIRC Activity 3197)
Attachments: DDOS_BestPractice.doc; A-0011-NCCIC -120020110914 AnonTools1.pdf

Good day,

Please find attached some documents containing information about hacktivism threat and Denial of Service attacks which may be helpful.

Do not hesitate to contact us if your require any assistance.

s.16(2)(c)

s.19(1)

Regards

Vireak Phlek
Cyber Duty Officer
Public Safety Canada
CCIRC

[REDACTED]
www.publicsafety.gc.ca

UNCLASSIFIED // FOR OFFICIAL USE ONLY



NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER BULLETIN

A-0011-NCCIC -120020110914

DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE.

"ANONYMOUS" AND ASSOCIATED HACKER GROUPS DEVELOPING AND DEPLOYING NEW CYBER ATTACK TOOLS

EXECUTIVE SUMMARY

(U//FOUO) This Bulletin is being provided for your Executive Leadership, Operational Management, and Security Administrators situational awareness. The hacker collective known as 'Anonymous' has successfully attacked a wide range of public and private sector entities since 2003 with relatively crude tools. Historically, they rely on tools such as the Low Orbit Ion Cannon (LOIC) or Botnets to deny access to websites, or hijack or deface web pages and post quasi-political statements, or perform other malicious activity. Since many of these older tools made it relatively easy for law enforcement and other government forces to identify the source of an attack and then arrest the perpetrator, Anonymous members may have recognized a need to have more advanced tools that offered a lesser degree of exposure. They recently claimed to have developed and possibly employed several new cyber attack tools for use in their self-proclaimed 'internet civil disobedience' campaigns. The NCCIC, coordinating with several of its partners, believes there are at least four new tools being shared among and employed by Anonymous members: #RefRef, Apache Killer, Anonware, and Universal Rapid Gamma Emitter (URGE).

(U//FOUO) Anonymous has stated that they are possibly going to use one of their new tools for 'OpBritain' on October 15, 2011, targeting Barclays, Vodafone, Lockheed Martin, and Atos. Other future targets announced by Anonymous may include FaceBook (OpFB) on November 5th, and the Fullerton, CA Police Department on a date to be determined. The tools would also be candidates for use during the upcoming 17 September, 2011 'Day of Rage' and 'OccupyWallStreet' protests that Anonymous has been widely advertising their planned participation in. Due to Anonymous' vague leadership structure and use of denial and deception, an actual attack may come with little warning or the threat could be a feint. Additionally, it may be difficult for government, law enforcement, and private sector entities to curb Anonymous actions, regardless of whether a warning is received. That being said, the NCCIC assesses with high confidence that Anonymous and associated groups will continue to use existing and newly created tools to exploit vulnerable web servers, web sites, computer networks and other digital information mediums, in spite of the fact that there are often indications of reconnaissance and penetration testing prior to an attack.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

BACKGROUND

(U//FOUO) LOIC has been popular with Anonymous because of its ease of use. It enables hackers with limited skill to engage in attacks by voluntarily joining a botnet and flooding a target server with network traffic; however, LOIC has a few drawbacks, the most important being the traceability of IP addresses involved. Network traffic records logged by the recipient of an attack can be identified if the attack was not routed through an anonymization network. Anyone with access to the logs, specifically law enforcement, could then trace the attack back to the individual computer used for conducting the attack. Thus, use of LOIC has been attributed by some members as the reason for the arrests of many alleged Anonymous members and associates over the last year. Those arrests led Anonymous members to clamor for a new tool that would provide better anonymity, and the purveyors of the '#RefRef' tool claim it offers that obfuscation. While '#RefRef' may have gotten the bulk of the attention lately, some security researchers believe another tool, 'Apache Killer' is a far greater source of concern. Below are descriptions and information for at least three probable new tools associated with or available for use by Anonymous and associated/sympathetic groups:

(U) #RefRef: originally claimed to be a platform neutral tool that leverages JavaScript to exploit a SQL vulnerability and allow unskilled users to launch DoS attacks against web sites.

(U//FOUO) A trusted Computer Network Defense partner has analyzed two separate, recently released scripts that can be used to carry out distributed denial-of-service (DDoS) attacks through slow-POST HTTP requests, slow-GET HTTP requests and SQL injection that are purported to be source code for #RefRef. They have assessed that neither script would likely perform DDoS attack attempts in the manner initially claimed by the tool's supposed creator. Though tools based on both scripts would likely be operable, it is unclear whether either has been used in Anonymous/AntiSec DDoS attacks, or whether either represents the #RefRef tool originally claimed to have been created by actor 'anonymousworldunited' and employed in attacks against pastebin.com.

(U//FOUO) The first variant was written in Perl and uses the target's own processing power against itself by uploading a JavaScript file to the target server and exploiting a SQL vulnerability, if present on the server. To exploit the vulnerability, the tool attempts to run a process that purportedly directs MySQL to execute the "benchmark" function to evaluate the expression "0x70726f62616e646f70726f62616e646f70726f62616e646f" 99,999,999,999 times, thus taxing the processor's resources and rendering it un-responsive. Also of note, "0x70726f62616e646f70726f62616e646f70726f62616e646f" is the ASCII string for "probandoprobandoprobando", the Latin word for "proving" strung together three times. Anonymous claimed the new tool would be made public in late August or early September.

(U//FOUO) The second variation, scripted in PHP, attempts to employ several DDoS attack methods commonly used by Anonymous activist groups, including slow-POST and slow-GET requests. The script's unnamed writers use multithreading and Keep-Alive mechanisms, attempting to maintain connections executing the various attack methods concurrently.

(U//FOUO) Other open source reports claiming to be based on interviews with the creators of #RefRef say it exploits a widespread SQL service by sending malformed SQL queries carrying a payload that forces the server to exhaust its resources. That reporting stream also mentions a user interface that has a field to input a refresh interval, thus combining http hammering with the SQL attack. If the scripts

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

described above actually are versions of the #RefRef tool, they would not present any 'new' attack vectors, though they do employ methods uncommon among Anonymous hackers and may pose threats to un-patched SQL servers and poorly configured web-server applications.

(U//FOUO) On September 9, 2011 a Twitter user, @AnonCMD, claimed to be associated with Anonymous and responsible for the almost universally derided August 31, 2011 denial of service attacks against WikiLeaks, Pastebin and 4Chan, sites commonly used by Anonymous members to post files and communicate with fellow hackers. AnonCMD repeatedly asserted that the attacks were 'field trials' for #RefRef and part of a personal vendetta with WikiLeaks founder Julian Assange over money. A post by @AnonCMD follows:

"As we returned from our days of hibernation, we have noticed that some may have took claim of developing #RefRef. We have seem the blatantly fake www.RefRef.org, and some more accounts that have taken claim to #RefRef – They are simply not true.

RefRef will be released to the public on September 17th. 2011, and any code you may have stumbled upon is strictly false. It is JavaScript, not Perl.

And to prove the fact that #RefRef is still in the works, we tested it again, not on(@Pastebin) – sorry we still owe you for that one, but on (@WikiLeaks)www.WikiLeaks.org . This was a #RefRef test, and again, it worked flawlessly."

(U) **Apache Killer:** on 25 August 2011, developers at the Apache open source project warned users of the popular web server software (more than two thirds of all web sites) about a new denial-of-service (DoS) tool called 'Apache Killer' that exploits a bug in the program and was confirmed to be circulating in the wild. According to Apache, all versions in the 1.3 and 2.0 lines are vulnerable to attack. Researchers who have examined copies of the malware say the vulnerability is trivial to exploit and causes an Apache web server to use up its memory and crash. The Apache Foundation update, Apache 2.2.20, fixes the issue and it's recommended that companies immediately patch their servers. Unfortunately, the group no longer supports the older Apache 1.3. and just over 5 percent of all Web servers are running revision 2.2.19. Apache has offered mitigation steps administrators with older versions can take to defend their web servers until a patch is available.

(U//FOUO) **Anonware:** a very basic tool. The source code itself is not very sophisticated and appears to be a framework from which a relatively inexperienced virus or malware writer can learn about and adapt malicious code. Researchers who have examined the source code stated that it essentially searches all available drives for .exe files, runs an .exe file supplied by the attacker, and then repackages the new .exe file so that it looks like nothing has happened. The "infected" file is created by using .net's run time CompileAssemblyFromSource method which allows a .net program to compile a new executable at run time. This is how the file "infection" is performed and is not considered a file infection in the true sense.

(U) **URGE:** tool claiming to be harmless while allowing an attacker to hijack Twitter trending topics and tweet messages within them. Anonymous claims it was created to 'better raise awareness of the real problems of the world' and used to get Twitter to 'trend topics that matter'. Reports state it may need Microsoft's .net Framework 4.0 to function.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

(U) TACTICS, TECHNIQUES, AND PROCEDURES

(U//FOUO) Anonymous utilizes the internet to recruit and train new personnel, conduct reconnaissance on potential targets, exploit vulnerabilities found in information systems, deny access to resources, alter information presented by organizations, and steal sensitive information. Though the Tactics, Techniques, and Procedures (TTPs) and tools employed by Anonymous are commonly referred to as being unsophisticated, their successes to date have gained them significant media attention. Though some media and blog attention has taken a negative sentiment towards the group and its activities, explicit condemnation of the group's activities has been mostly limited to the computer network defense community. Anonymous will likely continue to exploit weaknesses in system applications and network administration, thus allowing them to bypass network defenses and access sensitive data. Additionally, Anonymous and associated groups appear to be building upon recent successes to conduct their own and/or join in other highly visible messaging campaigns such as the September 17, 2011 'Worldwide Day of Rage'.

(U//FOUO) Anonymous and associated group's announcements on social media and other forums can provide computer network defenders an opportunity to pro-actively supplement their computer network defenses and provide awareness to management, employees, and partners. Anonymous members pride themselves on being 'social media' savvy, and routinely use forums such as Twitter^(USPER), YouTube^(USPER), FaceBook^(USPER), and public web pages to announce intended targets, ongoing attack results, and post files stolen from victim computer networks. Additionally, cybersecurity experts who have analyzed previous Anonymous attacks have noted there was a significant amount of reconnaissance prior to the attack. Other cybersecurity experts have recommended that public and private sector entities go through the same steps hackers would to determine the extent of attack surface available to a malicious actor. An example of this might entail using commercially available network security evaluation tools and internet search engines like Google^(USPER) to identify sensitive information and computer network vulnerabilities that have been cached as they catalogue the content of the WWW. Network defenders and managers should also bear in mind that claims made by Anonymous could be purposeful misdirection and possibly a distraction from the real (and undisclosed) attack Anonymous is planning or already engaged in.

(U//FOUO) To date, Anonymous has not demonstrated a capability to inflict damage to critical infrastructure, instead choosing to harass and embarrass its targets. However, some members of LulzSec, a group closely associated with Anonymous, have demonstrated moderately higher levels of skill and creativity, evidenced in attacks using combinations of methods and techniques to target multiple networks. To date, their attacks have largely resulted in the release of sensitive documents and personally identifiable information. This assessment does not take into account the possibility of a higher-level actor providing Anonymous or an associated group with more advanced capabilities.

(U//FOUO) The introduction of new tools such as Apache Killer, #RefRef, Anonware and Universal Rapid Gamma Emitter (URGE) clearly shows Anonymous' intention to not only continue their malicious activities, but improve their capabilities and provide a level of protection to anyone who participates. It is also likely to lead to changes in their tactics and techniques as they distribute new tools to members, those members become familiar with them, and new ways to employ them are then developed. Additionally, Anonymous has also increased the amount of physical 'protest' activity they either initiate or participate in, in conjunction with their cyber attacks, including the August 2011 attacks on the Bay Area Rapid Transit (BART) system and the upcoming 'Day of Rage'.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

ANTICIPATED FUTURE TARGETS

(U) Future attacks targeting both public and private sector entities, particularly in response to publicized events relating to civil liberties, cyber security, or allegations of censorship (online or otherwise) are likely to continue.

THE WAY AHEAD

(U//FOUO) Anonymous members have stated on several occasions that they engage in denial and deception activities. Therefore, network administrators, defenders, and security personnel should factor that in as they develop courses of action to counter the threat of an attack by Anonymous, an associated group, or person. Rigorous monitoring and analysis of logs and behaviors for indications of reconnaissance, probing, or ongoing attack targeting both internally and externally hosted resources may provide the key to successfully defending against an attack by Anonymous or any other malicious actor.

(U) The NCCIC recommends that U.S., Federal/State/local/Tribal/Territorial Departments and Agencies, and private sector partners ensure they have their internally hosted network resources, but also externally hosted ones updated and patched to the highest level possible. We also recommend, where applicable, personnel awareness and training programs be put in place to ensure employees are fully aware of potential threats and threat vectors. Processes should also be put in place to notify leadership, network operators, and security officials if an organization becomes a target by hackers or other malicious actors, and what notifications they are required or plan to make in the event of an attack.

(U) Should a cyber attack occur, ensure backup and recovery procedures are in place and enabled. Be prepared to execute a full spectrum defensive plan that includes contact information for external sources to draw on for assistance. Collect and centrally manage detailed aspects of the attack so you can provide accurate information to operations, security, and Law Enforcement personnel as necessary. Such a plan may also include materials identifying who to contact at your Internet service provider, possibly via alternate means, and at any time of day or night to minimize the duration and effect of a cyber attack. Similarly, have contact information readily available for public and private entities to draw on for assistance: the NCCIC, US-CERT, FBI Joint Terrorism Task Force, local FBI Field Office, applicable Information Sharing Analysis Center (ISAC), and Sector Specific Agency.

(U) For the situational awareness of F/S/L/T/T and CIKR partners, below are URLs to the National and Cyber Threat Levels the NCCIC monitors.

- National Terrorism Advisory System: <http://www.dhs.gov/alerts>
- NCRA: Contact NCCIC Watch & Warning: NCCIC@HQ.dhs.gov
- MS-ISAC: <http://www.msiscac.org/index.cfm>
- IT-ISAC: <https://www.it-isac.org/>
- ES-ISAC: <http://www.esisac.com/>
- FS-ISAC: <http://www.fsisac.com/>

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

POINTS OF CONTACT

(U) While the U.S. Government doesn't endorse a particular solution, identifying vendors with experience managing cyber incidents may reduce the time it takes to mitigate damage and restore service or operations. Additionally, the US-CERT web page offers a wide variety of technical and non-technical information to make use of both before and after an incident:

<http://www.us-cert.gov/nav/t01/>

(U) A variety of documents with information regarding defensive measures to combat a computer network attack are available at:

http://www.cert.gov/tech_tips/

(U) Many organizations can suffer financial loss as a result of a cyber attack and may wish to pursue criminal or civil charges against the intruder. For legal advice, we recommend that you consult with your legal counsel and law enforcement.

(U) Data breaches which involve a monetary loss or include a financial nexus such as a compromise to your financial, credit or debit accounts, or personal information can be reported to the U.S. Secret Service for criminal investigation. For more information contact your local Secret Service Field Office for assistance.

http://www.secretservice.gov/field_offices.shtml

(U) U.S. persons and companies interested in pursuing an investigation of a cyber attack can contact their local FBI field office for guidance and information. For contact information for your local FBI field office, please consult your local telephone directory or see the FBI's contact information web page:

<http://www.fbi.gov/contactus.htm>

(U) Non-U.S. entities may need to discuss malicious cyber activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

(U) U.S. Federal Government Departments and Agencies should report cyber attacks and incidents to US-CERT. Non-U.S. F/S/L/T/T Government Departments and Agencies interested in determining the source of certain types of cyber attacks may require the cooperation of your internet service provider and the administrator of the attacked networks. Tracking an intruder this way may not always be possible. If you are interested in trying to do so, contact your service provider directly. We do encourage you to report your experiences to US-CERT and the NCCIC, however. This helps the NCCIC and US-CERT understand the nature and scope of security incidents on the Internet, and we may be able to relate your report to other activity that has been reported to us.

TERMS OF REFERENCE

(U) **Anonymous** - (used as a mass noun) is an Internet meme originating 2003 on the imageboard 4chan, representing the concept of many online community users simultaneously existing as an anarchic, digitized global brain. It is also generally considered to be a blanket term for members of certain Internet subcultures, a way to refer to the actions of people in an environment where their actual identities are not known.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

(U) Lulz - often used to denote laughter at someone who is the victim of a prank, or a reason for performing an action. This variation is often used on the 'Oh Internet' wiki and '4chan' image boards.

(U) Distributed Denial of Service (DDoS) - an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary, it generally consists of the concerted efforts of person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

(U) Hacktivist - a portmanteau of hack and activism.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

CYBERDO

From: CYBERDO
Sent: October-28-11 2:00 PM
To: 'Lee Shields'
Cc: CYBERDO
Subject: [REDACTED] Re: Anonymous Threatens To Hack Toronto Stock Exchange Website - Canada-- [REDACTED]

Thank for the info.

Vireak Phlek
Cyber Duty Officer
Public Safety Canada
CCIRC

s.16(2)(c)
s.19(1)
s.20(1)(c)

www.publicsafety.gc.ca

-----Original Message-----

From: Lee Shields [mailto:Lee.Shields@rcmp-grc.gc.ca]
Sent: October 28, 2011 1:52 PM
To: CYBERDO
Subject: [REDACTED] Re: Anonymous Threatens To Hack Toronto Stock Exchange Website - Canada-- [REDACTED]

FYI...indication of some 'remediation' efforts at the ISP level.

Lee

>>> [REDACTED] 10/27/2011 12:35 PM >>>

Greetings.

AS | AS Name

[REDACTED] TSX-GROUP - The Toronto Stock Exchange

They have a [REDACTED] for their public IP Address allotments.

Since this "threat" is in the public domain, I'll reach out to their two upstream providers to give them the heads-up on this planned November 7th activity...

Thanks for the heads-up, eh?

-----Original Message-----

From: [REDACTED]
Sent: October-27-11 1:22 PM
To: [REDACTED]
Subject: [REDACTED] Anonymous Threatens To Hack Toronto Stock Exchange Website - Canada-- [REDACTED]

Importance: High

s.15(1) - Int'l

s.16(2)(c)

I know we have many Canadians on this list...

From: [REDACTED]
Sent: Thursday, October 27, 2011 11:28 AM

Any info on this????

[REDACTED]

From: [REDACTED]
Sent: Thursday, October 27, 2011 8:23 AM
Subject: Anonymous Threatens To Hack Toronto Stock Exchange Website - Canada-- [REDACTED]

For your insight and any information you may have on this situation (Threat) on the War against the Toronto Stock Exchange.

The hacking group's plan is to take down the web operations of TMX Group, which owns and operates the Toronto Stock Exchange, using Distributed Denial of Service (DDoS) attacks. The planned Toronto attack is called Operation #TMX.

[REDACTED]

-----Original Message-----

From: NOC Media Monitoring [<mailto:mmc@techopsolutions.net>]
Sent: Thursday, October 27, 2011 11:10 AM
To: Undisclosed recipients
Subject: Anonymous Threatens To Hack Toronto Stock Exchange Website - Canada-- [REDACTED]

Location: Toronto, Canada

* The hacker group Anonymous announced this week via a YouTube video posted to their account plans to disable the website of the Toronto Stock Exchange (TSX) on November 7

* It is the group's first major operation in Canada since "Occupy Toronto" started on October 15

* In the video message, Anonymous says: "The one percent has been putting their wealth in the Toronto Stock Exchange. This is why we choose to declare war against it"

* "On November 7, 2011, TSX shall be erased from the Internet. And this is just the beginning," the video says

* The hacking group's plan is to take down the web operations of TMX Group, which owns and operates the Toronto Stock Exchange, using Distributed Denial of Service (DDoS) attacks

* The planned Toronto attack is called Operation #TMX

s.15(1) - Int'l

New Media Sources (some page content may change or not be available over time):

- Twitter [NOW Toronto]

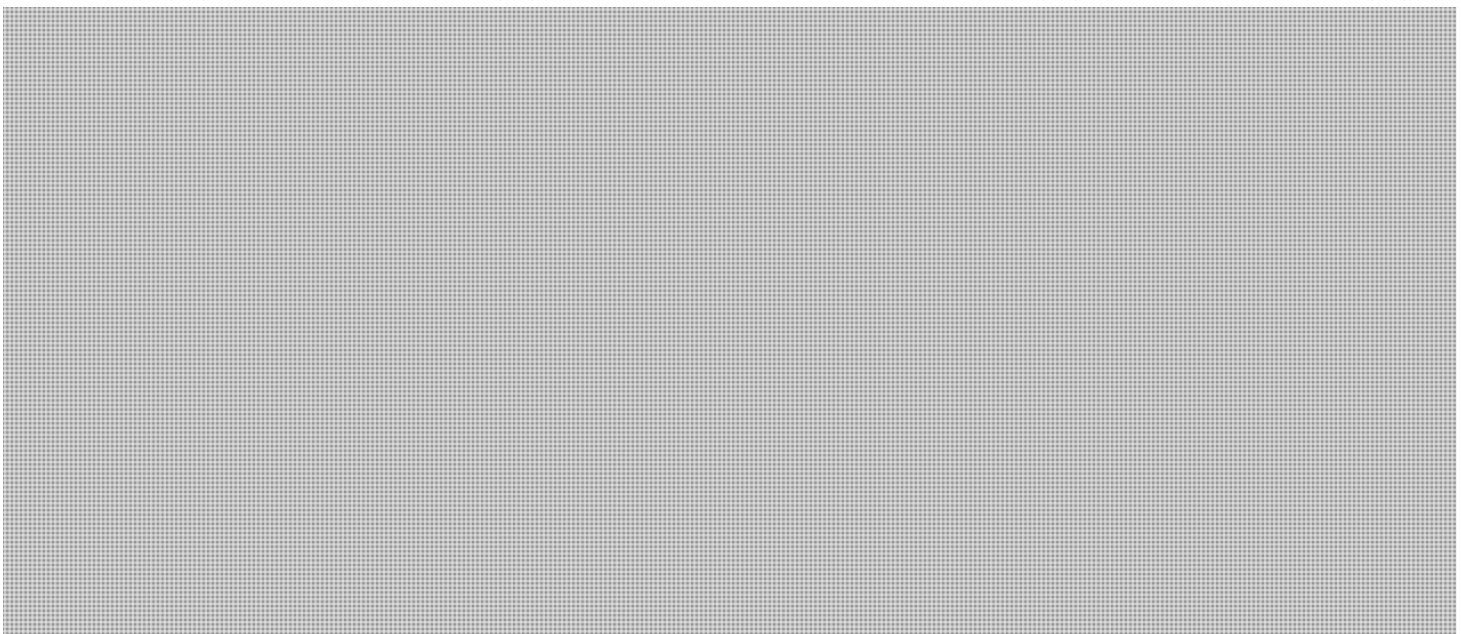
-- Expecting Anonymous at #TMX: <http://bit.ly/tScjBb> - 27 October, 0900

- Twitter

-- 'Anonymous' Promises to Hack Into TSX

<http://www.newstalk1010.com/News/localnews/blogentry.aspx?BlogEntryID=10305786> - 27 October, 0800

305786 - 27 October, 0800



CYBERDO


From: Beaudoin, Luc S s.19(1)
Sent: October-28-11 11:19 AM
To: 'Maurizio Rosa'; Ron Rimnyak
Cc: Dave Black; Gurb Singh; Lee Shields; RCMP_TCB_Operations@rcmp-grc.gc.ca; CYBERDO
Subject: RE: Anonymous threats to hack TSX (TMX Group)

Thanks. We will contact S/Sgt Ron RIMNYAK. At this time, we have been unsuccessful reaching TSX POC.

We have some mitigation advice we will send to [REDACTED] and advise them to monitor for network scanning activity. We have also identified public IP records for TMX to monitor our DDOS sources if something comes up.

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



From: Maurizio Rosa [<mailto:Maurizio.Rosa@rcmp-grc.gc.ca>]
Sent: October 28, 2011 10:35 AM
To: Beaudoin, Luc S; Ron Rimnyak
Cc: Dave Black; Gurb Singh; Lee Shields; RCMP_TCB_Operations@rcmp-grc.gc.ca
Subject: Anonymous threats to hack TSX (TMX Group)

Hi Luc,

As discussed earlier here is our position at this time regarding the above noted threat:

- The RCMP O Division Integrated Technological Crime Unit (ITCU) will generate an investigational file to track this issue.
- The O Div ITCU will liaise with: O Div Integrated Market Enforcement Team (IMET), CCIRC and the TMX Group, as required and monitor for future developments.
- The RCMP O Div ITCU will only become the lead agency if/when this becomes a Criminal Matter.

The contact at the O Div ITCU will be S/Sgt Ron RIMNYAK and can be reached at 519-640-7344 if needed.

Please keep him apprised of the mitigation steps taken by including him in any future correspondence.

Please let me know if you require any additional information or I can be of any assistance.

Thanks,

Moe

From: Maurizio Rosa [<mailto:Maurizio.Rosa@rcmp-grc.gc.ca>]
Sent: October 28, 2011 8:22 AM
To: Beaudoin, Luc S
Subject: RE: FW: Anonymous Threatens To Hack Toronto Stock Exchange Website - Canada--

Luc,

On that note can we (RCMP) have direct access to your source of information for the Money Mule file? Where is that source located? I just want to find the appropriate unit to follow-up on this information.
Thanks,

Moe

Sgt. Maurizio ROSA (46626)
Senior Forensic Investigator/A NCO i/c
Enquêteur judiciaire sénior/Sous.off. resp. intérimaire
Technological Crime Branch/Sous-direction de la criminalité technologique
Program and Operations Support Team/Équipe de soutien au programme et aux opérations
RCMP - GRC
1426 St. Joseph Blvd.
Ottawa, Ontario, Canada
K1A 0R2

s.15(1) - Int'l
s.16(2)(c)

Phone/Tél: (613) 993-9335
Fax: (613) 993-2963

Warning:

<<This document is the property of the RCMP. It is loaned to your agency/department in confidence and it is not to be reclassified or further disseminated without the consent of the originator.>>

Avis:

<<Ce document appartient à la GRC. Il est prêté à votre organisme en toute confidentialité et avec la compréhension qu'il ne sera ni reclassifié, ni diffusé plus largement sans le consentement de l'auteur.>>

>>> "Beaudoin, Luc S" <Luc.Beaudoin@ps-sp.gc.ca> 10/28/2011 7:30 AM >>>

tx Moe. I think the issue with the Money Mule would have been one of interest. These are time sensitive cases but it should be pretty straight forward to contact Google and get them to seize the account and under warrant provide responses.

We ll lead the TSX for now, from a mitigation end and we will cc you on all emails, OK ? If you guys come accross intel from [redacted] etc, let's share.

L

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

**Page 2143
is a duplicate
est un duplicata**

**Page 2144
is a duplicate
est un duplicata**

**Page 2145
is a duplicate
est un duplicata**

CYBERDO

From: [REDACTED]
Sent: October-28-11 10:16 AM
To: Beaudoin, Luc S s.19(1)
Cc: CYBERDO s.20(1)(c)
Subject: RE: TSX cyber contact

I thought so. [REDACTED] had sent me a note. I suggested he contact you.

I will pass on your thanks to [REDACTED]

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: October 28, 2011 9:50 AM
To: [REDACTED]
Cc: CYBERDO
Subject: RE: TSX cyber contact

Thanks and please pass our thanks to [REDACTED] as well. To give you some context, this is related to Anonymous recent public claims.

cheers

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]
Sent: October 28, 2011 9:37 AM
To: Beaudoin, Luc S
Cc: CYBERDO
Subject: RE: TSX cyber contact

Luc,

[REDACTED]

The contact was from [REDACTED]



From: Beaudoin, Luc S [<mailto:Luc.Beaudoin@ps-sp.gc.ca>]
Sent: October 28, 2011 8:22 AM
To: [REDACTED]
Cc: CYBERDO
Subject: TSX cyber contact

s.19(1)

Sorry to bother you. Quick question:

Would you guys have a trusted cyber security contact over at TSX ?

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

Handwritten signature

CYBERDO

From: Beaudoin, Luc S
Sent: October-28-11 9:26 AM
To: 'Maurizio Rosa'
Cc: CYBERDO
Subject: RE: Anonymous Threatens To Hack Toronto Stock Exchange Website - Canada-- [REDACTED]

I will ask the source but researchers don't like to come in the open typically....

Note that the way these things work is spam email sent to 1000s, answers within a few minutes are kept and redirected to another site, and another etc until a deal is made and trust is built. The original account is not used at all after a few minutes. From an investigation perspective, I guess you would need access to the email account to see who responded within the first couple of minutes. The info should all be there to do that. I was hoping the antifraud folks would have taken this on with their Google mail relationships....we haven't heard anything from them.

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

s.15(1) - Int'l
s.16(2)(c)

From: Maurizio Rosa [<mailto:Maurizio.Rosa@rcmp-grc.gc.ca>]
Sent: October 28, 2011 8:22 AM
To: Beaudoin, Luc S
Subject: RE: FW: Anonymous Threatens To Hack Toronto Stock Exchange Website - Canada-- [REDACTED]

Luc,

On that note can we (RCMP) have direct access to your source of information for the Money Mule file? Where is that source located? I just want to find the appropriate unit to follow-up on this information. Thanks,

Moe

>>> "Beaudoin, Luc S" <Luc.Beaudoin@ps-sp.gc.ca> 10/28/2011 7:30 AM >>>
tx Moe. I think the issue with the Money Mule would have been one of interest. These are time sensitive cases but it should be pretty straight forward to contact Google and get them to seize the account and under warrant provide responses.

We'll lead the TSX for now, from a mitigation end and we will cc you on all emails, OK? If you guys come across intel from [REDACTED] etc, let's share.

RCMP



**Page 2150
is a duplicate
est un duplicata**

**Page 2151
is a duplicate
est un duplicata**

Dvorkin, Corey

From: Barr, Corri <Corri.Barr@tbs-sct.gc.ca>
Sent: October-26-11 1:53 PM
To: Dvorkin, Corey
Subject: FW: LASER 11/234 - "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day / Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes
Attachments: Laser11234-E.pdf; Laser11234-F.pdf

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



Treasury Board of Canada
Secretariat

Secrétariat du Conseil du Trésor
du Canada

Canada

Better government: with partners, for Canadians | Un meilleur gouvernement : avec nos partenaires, pour les Canadiens

From: Guénette, Maxime
Sent: October 25, 2011 4:17 PM
To: Hutchison, Michael; Zwanenburg, Susan; Bujold, Luc; Lacroix, Daniel; McMahon, William; Hooper, Shawn; Lymburner, Jean-François; Côté, Alain
Cc: Lebel-Ducharme, Monique; Vignola, Lucie; Barr, Corri; Dussault, Nathalie; Hébert, Julie; Hébert, Stephanie; Girard, Paul; Gales, Geneviève; Rouleau, Pascale; 'Mark.McLaughlin@pco-bcp.gc.ca'; Eskibashian, Sevac
Subject: Fw: LASER 11/234 - "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day / Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes

Guys,

Pls see below and attached. A group has called on its members to undertake disruptive activities, including a call to deface government and media websites and taking over Twitter feeds ([REDACTED])

Please pay special attention to our Web sites over the coming days and flag any suspicious activity to our IMTD colleagues.

Thanks

Max

Typed with my thumbs using a device whose brand name must not be mentioned... // Rédigé avec mes pouces à l'aide d'un appareil dont la marque ne doit pas être mentionnée...

From: Girard, Paul
Sent: Tuesday, October 25, 2011 03:55 PM
To: Guénette, Maxime; Morrow, Rob
Subject: Fw: LASER 11/234 - "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day / Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes

Both of you should be aware of this.

Executive Director and Chief Information Officer | Directeur exécutif et Dirigeant principal de l'information

Information Management and Technology Directorate | Direction générale de la gestion d'information et de la technologie

Corporate Services Sector | Secteur des services ministériels

Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Ottawa, Canada K1A 0R5

Paul.Girard@tbs-sct.gc.ca

Telephone | Téléphone 613-992-4306 / Facsimile | Télécopieur 613-943-2077 / Teletypewriter | Tél'imprimeur 613-957-9090

Government of Canada | Gouvernement du Canada

From: Murphy, Larry
Sent: Tuesday, October 25, 2011 03:50 PM
To: Parson, Luc; Brouillard, Marc; Johnston, Philippe

Cc: Girard, Paul; Walker, Christine (CFO)

Subject: FW: LASER 11/234 - "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day / Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes

FYI

s.15(1) - Subv

From: [REDACTED]
Sent: October 25, 2011 2:57 PM
To: [REDACTED]
Subject: LASER 11/234 - "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day / Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes

Laser 11/234 - "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day

This document is UNCLASSIFIED and is the property of the Integrated Terrorism Assessment Centre (ITAC). Prepared by ITAC, it is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to those with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed via email to ITAC at [REDACTED] or to ITAC Partnerships at [REDACTED]

ITAC is a community resource of the Canadian government's Security and Intelligence Community. It is comprised of secondees from a wide range of federal agencies and produces integrated, comprehensive and timely threat assessments for all levels of government with security responsibilities and, as appropriate, critical infrastructure stakeholders in the private sector.

ITAC would like to express its gratitude to all agencies and departments of Canada's Security and Intelligence Community for the contributions they have made to this product, and invites those agencies and departments to provide feedback on the content of this threat assessment product.

Laser 11/234 - Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes


Le présent document est coté NON CLASSIFIÉ et est la propriété du Centre intégré d'évaluation du terrorisme (CIET) et a été préparé par celui-ci. Il s'appuie sur des informations qui proviennent de diverses sources et qui sont valables à la date de publication. Il est fourni à votre organisme ou ministère à titre confidentiel et peut être communiqué directement par votre organisme ou ministère à d'autres personnes selon le principe du besoin de savoir. Il ne doit pas être réutilisé, de quelque manière que ce soit, en tout ou en partie, sans le consentement de l'expéditeur. Pour tout commentaire, veuillez envoyer un courriel au CIET, à [REDACTED] ou communiquer avec la Sous-section des partenariats du CIET, au [REDACTED]

Le CIET est un membre de l'appareil canadien de la sécurité et du renseignement, composé d'employés en détachement provenant de divers organismes fédéraux. Il produit à point nommé des évaluations intégrées et détaillées de la menace pour tous les ordres de gouvernement responsables de la sécurité ainsi que pour les intervenants du secteur privé responsables de l'infrastructure essentielle.

Le CIET tient à remercier tous les organismes et les ministères de l'appareil canadien de la sécurité et du renseignement de leur contribution au présent document, et les invite à formuler des commentaires sur son contenu.

Thanks / merci,

s.15(1) - Subv


Dissemination Officer
ITAC





Integrated Terrorism Assessment Centre

Centre intégré d'évaluation du terrorisme

THREAT

L A S E R

ALERT

11 / 234-E
2011 10 25

UNCLASSIFIED -
See Handling Instructions

“Anonymous” calls for nuisance activities to coincide with Guy Fawkes Day

KEY POINTS

- On 2011 10 16, the international *hacktivist* group “Anonymous” posted a message online urging sympathizers to participate in a range of nuisance activities targeting governments and media on 2011 11 05 to coincide with Guy Fawkes Day. Dubbed “Operation Injustice Awareness” the call encourages sympathizers to deface web sites and redirect the traffic they receive to “Anonymous” *Twitter* feeds, in keeping with the group’s traditional *modus operandi*. The call also encourages sympathizers to take to the streets, wearing Guy Fawkes’ masks, to deface their cities with graffiti, to engage anyone who questions them, and to photograph and upload their stories to social media.
- [REDACTED]
- ITAC is providing this report to first responders for situational awareness. [REDACTED]

s.15(1) - Subv

s.16(1)(a)(iii)

s.16(1)(c)

LASER 11 / 234-E

UNCLASSIFIED - See Handing Instructions

ANALYSIS

1) On 2011 10 16, the international *hactivist* group “Anonymous” posted a message online urging sympathizers to engage in a range of nuisance activities targeting governments and media on 2011 11 05 to coincide with Guy Fawkes Day (a misinterpreted reference to the British tradition of Guy Fawkes Night, which marks a foiled plot in AD 1605 to assassinate the King of England in which Londoners, rejoicing that their King was safe, joyfully lit bonfires). Dubbed “Operation Injustice Awareness”, the call encourages sympathizers to deface web sites and redirect the traffic they receive to “Anonymous” *Twitter* feeds, in keeping with the group’s traditional *modus operandi*. The call also encourages sympathizers to take to the streets, wearing Guy Fawkes’ masks, to deface their cities with graffiti, to engage anyone who questions them, and to photograph and upload their stories to social media. ■■■■

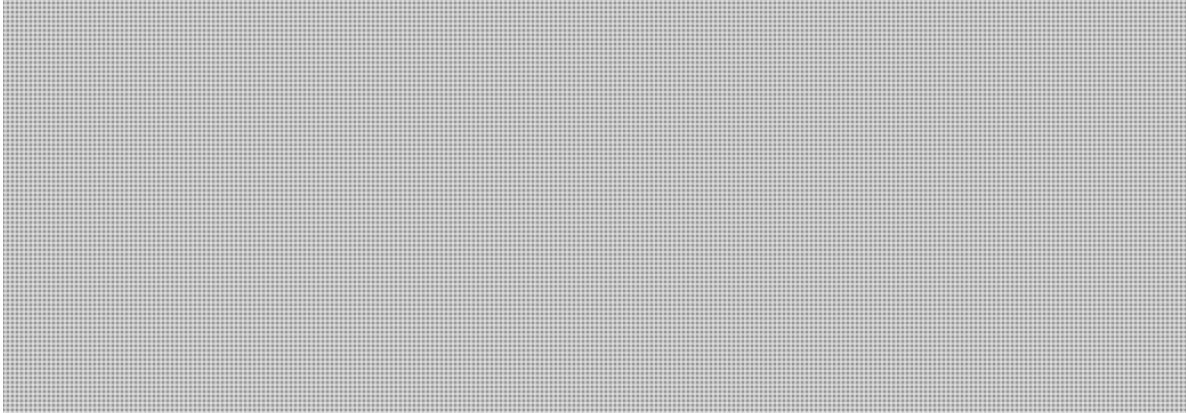
2) During the summer of 2011, dozens of “Anonymous” members were arrested in several countries for their attacks on corporate and sensitive government web sites. The group gained notoriety for taking down PayPal and Visa for ceasing to conduct business with *WikiLeaks* after it released thousands of US diplomatic cables. “Anonymous” also took down the web site of Monsanto, a major biotech company, accusing it of being “corrupt, unethical and downright evil”. The group has vowed to avenge the arrest of its members. ■■■■


3) According to open information, in most cyber attacks, “Anonymous” uses a method referred to as Distributed Denial of Service (DDoS), which consists of directing a large traffic surge to a web site until it becomes overwhelmed and cannot operate efficiently. Depending on the design and capacity of a web site, DDoS attack consequences can range from a slow-down, or speed-up to a potential crash of the site. “Anonymous” also uses a hacking tool known as SQL injection, which consists of exploiting a vulnerable code on a computer system. This allows the hacker to bypass security measures, obtain access to the network and steal information. ■■■■

4) On 2011 10 18, the US Department of Homeland Security (DHS), National Cyber-security and Communications Integration Center (NCCIC), was quoted as saying that the information available on “Anonymous” suggests they currently have a limited ability to conduct attacks targeting Industrial Control Systems (ICS). However, experienced and skilled members could develop capabilities to gain access and trespass on control system networks very quickly. Moreover, free educational opportunities (conferences, classes), presentations at hacker conferences and other high profile events / media coverage have raised awareness to ICS vulnerabilities and have likely shortened the time needed to develop sufficient tactics, techniques and procedures to disrupt ICS. ■■■■

LASER 11 / 234-E

UNCLASSIFIED - See Handing Instructions



7) ITAC continues to monitor the situation and will provide updates as necessary. 

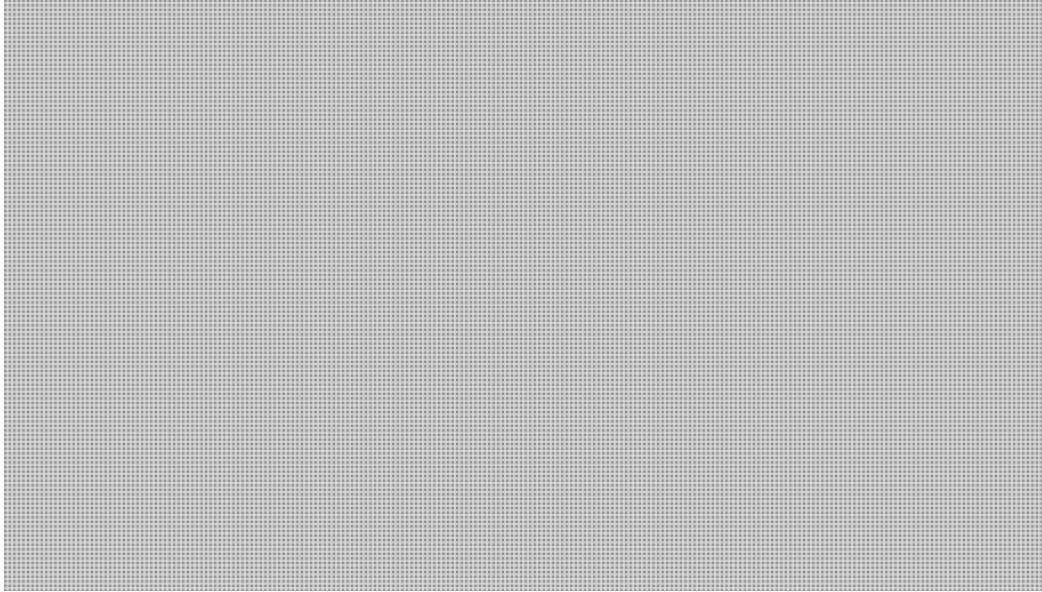
s.15(1) - Subv

s.16(1)(a)(iii)

s.16(1)(c)

LASER 11 / 234-E

UNCLASSIFIED - See Handling Instructions



HANDLING INSTRUCTIONS

This document is the property of the Integrated Terrorism Assessment Centre (ITAC). Prepared by ITAC, it is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to those with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed via email to ITAC at [REDACTED] or to ITAC Partnerships at [REDACTED].

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 ITAC.

s.15(1) - Subv



Centre intégré d'évaluation du terrorisme

Integrated Terrorism Assessment Centre

MENACE

L A S E R

ALERTE

11 / 234-F
2011 10 25

NON-CLASSIFIÉ -
Voir manipulation de renseignements

Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes

FAITS SAILLANTS

- Le 2011 10 16, le groupe international d'*hacktivistes* « Anonymous » a affiché un message en ligne incitant ses sympathisants à se livrer le 2011 11 05 à toute une série d'activités malveillantes prenant pour cible des organisations gouvernementales et des médias, et ce, afin de coïncider avec le Jour de Guy Fawkes. Conformément à ses façons de procéder habituelles, dans le cadre de cette « Opération de sensibilisation à l'injustice », le groupe encourage ses sympathisants à dégrader des sites Web et à rediriger les messages qui leur sont destinées vers le compte Twitter d'« Anonymous ». Il pousse également ses sympathisants à descendre dans la rue en portant des masques de Guy Fawkes, à recouvrir leur ville de graffitis, à prendre à partie quiconque les remet en question et à prendre des photos de leurs réalisations, puis à les afficher dans les médias sociaux. [REDACTED]
- [REDACTED]
- La présente évaluation du CIET s'adresse au personnel de première intervention afin de les tenir au courant de la situation. [REDACTED]

s.15(1) - Subv
s.16(1)(a)(iii)
s.16(1)(c)

LASER 11 / 234-F

NON-CLASSIFIÉ -
Voir manipulation de renseignements

ANALYSE

1) Le 2011 10 16, le groupe international d'*hacktivistes* « Anonymous » a affiché un message en ligne incitant ses sympathisants à se livrer le 2011 11 05 à toute une série d'activités malveillantes prenant pour cible des organisations gouvernementales et des médias, et ce, afin de coïncider avec le Jour de Guy Fawkes (il s'agit d'une référence erronée à la tradition britannique de la Nuit de Guy Fawkes, qui marque la mise en échec, en 1605, d'un complot visant à assassiner le roi d'Angleterre, à la suite de laquelle les Londoniens, se réjouissant que leur roi était sain et sauf, ont allumé des feux de joie). Conformément à ses façons de procéder habituelles, dans le cadre de cette « Opération de sensibilisation à l'injustice », le groupe encourage ses sympathisants à dégrader des sites Web et à rediriger les messages qui leur sont destinés vers le compte Twitter d'« Anonymous ». Il pousse également ses sympathisants à descendre dans la rue en portant des masques de Guy Fawkes, à recouvrir leur ville de graffitis, à prendre à partie quiconque les remet en question et à prendre des photos de leurs réalisations, puis à les afficher dans les médias sociaux. [REDACTED]

2) Au cours de l'été 2011, plusieurs dizaines de membres du groupe « Anonymous » ont été arrêtés dans plusieurs pays pour avoir piraté des sites Web d'entreprises et des sites Web sensibles gouvernementaux. Le groupe s'est fait connaître pour avoir réussi à mettre hors service les sites Web de PayPal et de Visa qui avaient décidé de cesser de faire des affaires avec *WikiLeaks* après la diffusion, par ce dernier, de milliers de câbles diplomatiques américains. Le groupe « Anonymous » a également mis hors service le site Web de Monsanto, une grande entreprise de biotechnologie, que le groupe accusait d'être « corrompue, sans éthique et purement et simplement malfaisante ». Le groupe a juré de venger l'arrestation de ses membres. [REDACTED]

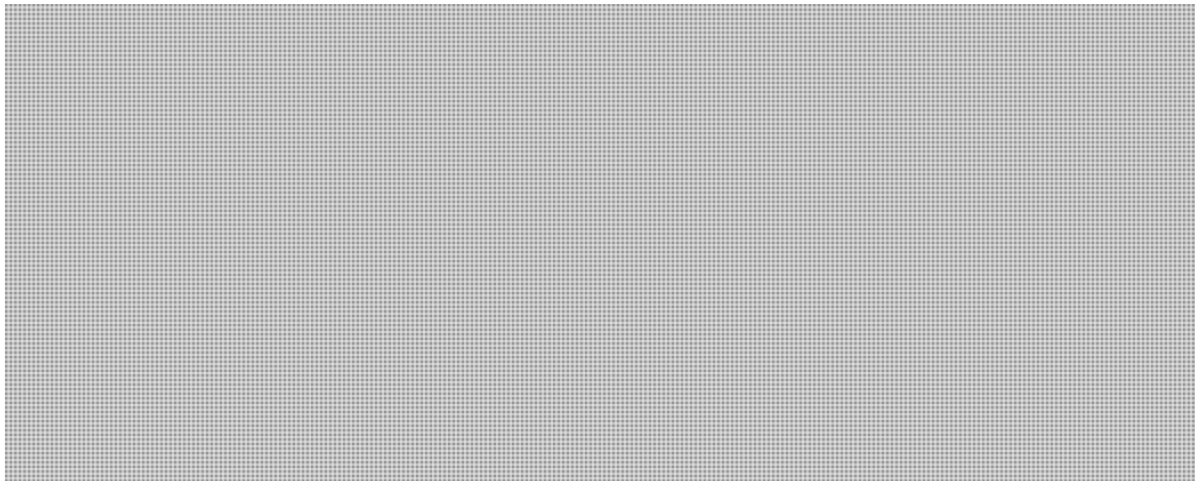
3) Selon des informations de sources ouvertes, le groupe « Anonymous » utilise pour la plupart de ses cyberattaques une méthode connue sous le nom de « déni de service distribué » (DDoS) qui consiste à diriger subitement un trafic très important vers un site Web jusqu'à ce qu'il soit submergé et ne puisse plus fonctionner efficacement. En fonction de la conception et de la capacité du site Web, les conséquences des attaques DDoS varient et peuvent provoquer soit un ralentissement soit, à l'inverse, une accélération des opérations du site jusqu'à la panne éventuelle de ce dernier. Le groupe « Anonymous » se sert également d'un outil de piratage appelé « injection SQL », qui consiste à exploiter un code vulnérable dans un système informatique. Le pirate est alors en mesure de contourner les mesures de sécurité en place, d'accéder au réseau et de voler l'information. [REDACTED]

4) Le 2011 10 18, le National Cyber-security and Communications Integration Center (NCCIC) du département de la Sécurité intérieure (DHS) des États-Unis a indiqué que selon les informations en sa possession sur « Anonymous », le groupe possède une capacité limitée pour mener des attaques contre les systèmes industriels de contrôle (SIC). Cependant, des membres expérimentés et compétents du groupe pourraient perfectionner très rapidement leurs capacités dans le but d'accéder

LASER 11 / 234-F

**NON-CLASSIFIÉ -
Voir manipulation de renseignements**

et de s'introduire illégalement dans les réseaux de systèmes de contrôle. De plus, les faiblesses des SIC ont été mises en lumière dans le cadre d'occasions d'apprentissage gratuites (conférences, classes), d'exposés présentés lors de congrès de pirates informatiques et d'autres événements très médiatisés, et il est probable que certains individus risquent maintenant de mettre au point beaucoup plus rapidement que prévu des tactiques, des techniques et des procédures qui leur permettront de perturber les SIC. ()



7) Le CIET continue de surveiller la situation et fera le point au besoin. ()

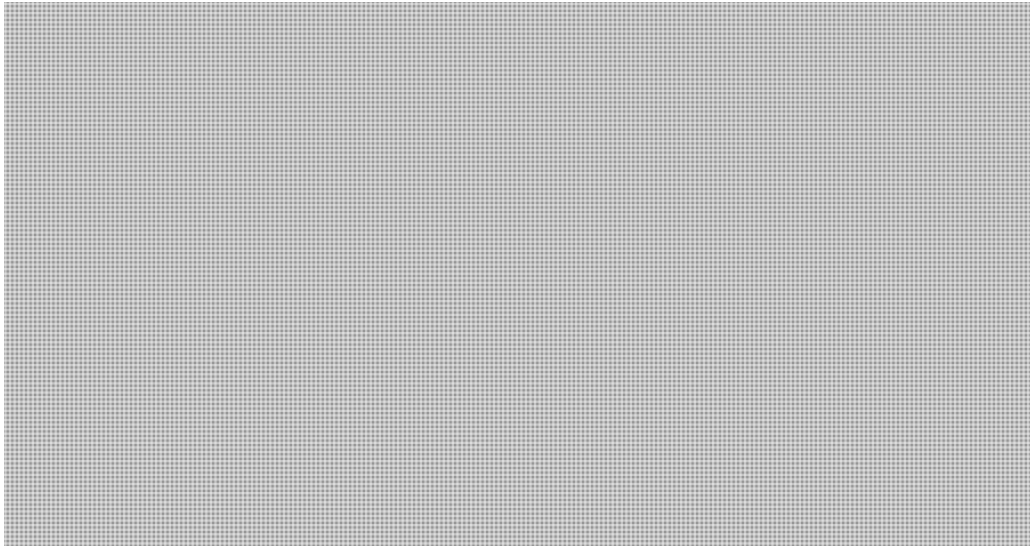
s.15(1) - Subv

s.16(1)(a)(iii)

s.16(1)(c)

LASER 11 / 234-F

**NON-CLASSIFIÉ -
Voir manipulation de renseignements**



MANIPULATION DE RENSEIGNEMENTS

Le présent document est la propriété du Centre intégré d'évaluation du terrorisme (CIET) et a été préparé par celui-ci. Il s'appuie sur des informations qui proviennent de diverses sources et qui sont valables à la date de publication. Il est fourni à votre organisme ou ministère à titre confidentiel et peut être communiqué directement par votre organisme ou ministère à d'autres personnes selon le principe du besoin de savoir. Il ne doit pas être réutilisé, de quelque manière que ce soit, en tout ou en partie, sans le consentement de l'expéditeur. Pour tout commentaire, veuillez envoyer un courriel au CIET, à [REDACTED] ou communiquer avec la Sous-section des partenariats du CIET, au [REDACTED].

Le présent document peut faire l'objet d'une exception aux termes de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*. On pourra également s'opposer à la communication des informations ou des renseignements qu'il contient en vertu de la *Loi sur la preuve au Canada*. Ces informations ou renseignements ne doivent être ni communiqués ni utilisés comme preuve sans consultation préalable du CIET.

s.15(1) - Subv

CYBERDO

From: CYBERDO
Sent: October-26-11 1:32 PM
To: 'Gurb Singh'
Cc: Beaudoin, Luc S; CYBERDO
Subject: RE: CE11-2428 [Antisec hack of police]

s.16(2)(c)

Hi Gurb,

Do you have any update for us?

Thank you,
Cyber Duty Officer
Public Safety Canada
CCIRC


www.publicsafety.gc.ca

-----Original Message-----

From: CYBERDO
Sent: October 24, 2011 9:22 AM
To: 'Maurizio Rosa'; 'Gurb Singh'
Cc: CYBERDO; Beaudoin, Luc S
Subject: CE11-2428 [Antisec hack of police]

Good day,

Here is the info that was on pastebin.com

The link : <http://pastebin.com/> : Content in txt and print out in pdf.

Thanks,

Vireak Phlek
Cyber Duty Officer
Public Safety Canada
CCIRC


www.publicsafety.gc.ca

-----Original Message-----

From: Beaudoin, Luc S
Sent: October 24, 2011 9:06 AM

To: 'Maurizio Rosa'; 'Gurb Singh'
Cc: Phlek, Vireak; CYBERDO
Subject: Antisec hack of police

Heads up of compromise. Details from pastebin will be sent to you in a few minutes.

<http://gawker.com/5852297/anonymous-hacks-police-websites-and-data-to-support-occupy-wall-street>
<<http://gawker.com/5852297/anonymous-hacks-police-websites-and-data-to-support-occupy-wall-street>>

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

Grigsby, Alexandre

From: Dvorkin, Corey
Sent: Tuesday, October 18, 2011 12:05 PM
To: Maillé, Marie Anick; Hatfield, Adam; McAllister, Andrew; Schramm, Kent; Campbell, Tom; Green, Amanda; Bradley, Kees; Vershinin, Sergey; Grigsby, Alexandre; Mohammed, Melanie; Bonvie, Jeff
Cc: 'Dave Black'; Gauthier, Darren
Subject: "Anonymous" and control systems



NCCIC-Anonym...

DHS: Anonymous Interested in Hacking Nation's Infrastructure

The hacker collective known as Anonymous has expressed interest in hacking industrial systems that control critical infrastructures, such as gas and oil pipelines, chemical plants and water and sewage treatment facilities, according to a Department of Homeland Security bulletin.

But DHS doubts the anarchic group has the necessary skills. At least for now.

Anonymous efforts to attack such systems could be thwarted by the lack of centralized leadership in the loosely collected group, the bulletin says, as well as a lack of "specific expertise" about how the systems work and how to attack them. However, the report notes, the latter could easily be overcome through study of publicly available information.

"The information available on Anonymous suggests they currently have a limited ability to conduct attacks targeting [industrial control systems]," according to DHS. "However, experienced and skilled members of Anonymous in hacking could be able to develop capabilities to gain access and trespass on control system networks very quickly."

The assessment comes in a bulletin issued recently (.pdf) by the Department of Homeland Security's National Cybersecurity and Communications Integration Center, and published Monday by the web site Public Intelligence. The bulletin was marked "For Official Use Only," a designation that means the data isn't classified but is meant only to be shared with government agencies and trusted outside sources.

The bulletin says that members of Anonymous have not yet demonstrated attacks on such systems, instead choosing to "harass and embarrass their targets using rudimentary attack methods." But the group's interest in attacking these systems could grow once they realize how poorly the systems are secured, and they figure out how to leverage information that is already publicly available about vulnerabilities in the systems.

NCCIC predicts a "moderate likelihood" that the group's protest activities could be accompanied by hacking attacks on core infrastructure in the future.

"[T]here are control systems that are currently accessible directly from the internet and easy to locate through internet search engine tools and applications," the bulletin notes. "These systems could be easily located and accessed with minimal skills in order to trespass, carry out nefarious activities, or conduct reconnaissance activities to be used in future operations."

As evidence of Anonymous' interest in control systems, the bulletin points to a July 11 post at Pastebin, a site where programmers and hackers post code and missives. The post discussed a denial-of-service attack against Monsanto and possible future plans against the company.

We blasted their web infrastructure to shit for 2 days straight, crippling all 3 of their mail servers as well as taking down their main websites world-wide. We dropped dox on 2500+ employees and associates, including full names, addresses, phone numbers, and exactly where they work. We are also in the process of setting up a wiki, to try and get all collected information in a more centralized and stable environment. Not bad for 2 months, I'd say.

What's next? Not sure... it might have something to do with that open 6666 IRC port on their nexus server though.

And on July 19, a known member of Anonymous tweeted the results of browsing the directory tree for Siemens SIMATIC software, the same industrial control system software that was exploited by the Stuxnet worm last year to sabotage uranium-enriching centrifuges at an Iranian nuclear plant.

Another Anonymous member subsequently pointed to XML and HTML code that could be used to query the SIMATIC system to find vulnerabilities in it, and also indicated he was already inside multiple control systems.

The posted xml and html code reveals that the individual understands the content of the code in relation to common hacking techniques to obtain elevated privileges. It does not indicate knowledge of ICS; rather, it indicates that the individual has interest in the application software used in control systems.

The posted xml and html contained administration code used to create password dump files for a human-machine interface control system software product from Siemens. The code also contained OLE for Process Control (OPC) foundation code that is used in server communication with control system devices such as programmable logic controllers, remote terminal units, intelligent-electronic devices, and industrial controllers.

While the latter information indicated the individual had an interest in control systems, NCCIC could find nothing to indicate that the person actually possessed the capabilities necessary to hack an ICS.

"There are no indications of knowledge or skill in control systems operations, design, or components," the bulletin notes. "The individual may possess the necessary skill to exploit elevated privileges by hijacking credentials of valid users of the ICS software product posted based on traditional exploitation methods, not anything ICS specific."

According to the NCCIC bulletin, oil and gas companies could become particularly attractive targets to Anonymous and its sympathizers, owing to the hacking collective's "green energy" agenda and its members' past opposition to pipeline projects.

"This targeting could likely extend beyond Anonymous to the broader [hacker activist] community, resulting in larger-scope actions against energy companies," DHS warns in the bulletin.

The security of industrial control systems, which are used in commercial manufacturing facilities and critical infrastructure systems around the world, was thrown into the spotlight over the last year, after the Stuxnet worm infected more than 100,000 computers in Iran and elsewhere. Although the worm was designed to target the SIMATIC industrial control system made by Siemens, it only released its destructive payload on a specific Simatic system – believed to be the system that controls centrifuges at Iran's uranium enrichment plant in Natanz.

The discovery of the worm helped bring attention to the serious security vulnerabilities that exist in the Siemens system. Researchers who have further examined Siemens systems, as well as industrial control systems made by other manufacturers, have found them all to share the same kinds of security vulnerabilities.

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 0P8
Tel: (613) 990-9608
corey.dvorkin@ps-sp.gc.ca

UNCLASSIFIED//FOR OFFICIAL USE ONLY



NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER BULLETIN

A-0020-NCCIC / ICS-CERT -120020110916

DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR MISION PARTNERS AT THE "FOR OFFICIAL USE ONLY" LEVEL, ACROSS THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE.

(U//FOUO) ASSESSMENT OF ANONYMOUS THREAT TO CONTROL SYSTEMS

EXECUTIVE SUMMARY

(U) The loosely organized hacking collective known as Anonymous has recently expressed an interest in targeting industrial control systems (ICS). This product characterizes Anonymous' capabilities and intent in this area, based on expert input from DHS's Control Systems Security Program/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in coordination with the other NCCIC components.

(U//FOUO) While Anonymous recently expressed intent to target ICS, they have not demonstrated a capability to inflict damage to these systems, instead choosing to harass and embarrass their targets using rudimentary attack methods, readily available to the research community. Anonymous does have the ability to impact aspects of critical infrastructure that run on common, internet accessible systems (such as web-based applications and windows systems) by employing tactics such as denial of service. Anonymous' increased interest may indicate intent to develop an offensive ICS capability in the future. ICS-CERT assesses that the *publically available information regarding exploitation of ICS could be leveraged to reduce the amount of time to develop offensive ICS capabilities. However, the lack of centralized leadership/coordination and specific expertise may pose challenges to this effort.*

DISCUSSION

(U//FOUO) Several racist, homophobic, hateful, and otherwise maliciously intolerant cyber and physical incidents throughout the past decade^a have been attributed to Anonymous, though recently, their targets and apparent motivations have evolved to what appears to be a hacktivist¹ agenda. The section below highlights a recent interest Anonymous has developed in exploiting ICS, which the NCCIC assesses is a new tactic, technique and/or procedure (TTP). For more information on Anonymous's background or motivations, please see the NCCIC Bulletins: "*Anonymous Upcoming US Operations, Impact, and Likelihood,*" and "*Anonymous and Associated Hacker Groups Developing New Cyber Attack Tools.*"

¹ Hacktivist – A cyber exploitation or attack actor whose intent is driven by a social, religious, political or cultural ideology.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Recent Examples of Anonymous' Interest in Control Systems

(U) On 11 July 2011 a suspected member of Anonymous, posted some materials to Pastebin^b. This posting describes its cyber attack on Monsanto's websites and e-mail servers. Anonymous reported exfiltrating personally identifiable information (PII) data on 2,500+ employees and associates, including full names, addresses, phone numbers, and exactly where they work. They reported it took about two months to accomplish this attack.

- (U) Monsanto is a U.S.-based global biotech seed company. Tom Helscher, the company director of corporate affairs, in an e-mail to msnbc.com confirmed that Monsanto "experienced a disruption to its website that appeared to be from an organized cyber group."^c

(U//FOUO) On 12 July 2011, Anonymous released a press report on a website titled "Anonymous Operation Green Rights \ Project Tarmaggedon."^d The report outlined Anonymous' hacktivists concerns with global warming and called for protests against the Alberta Tar Sands (Canada) project along Highway 12 in Montana. As quoted from its posting, "Anonymous Operation Green Rights calls your attention to an urgent situation in North America perpetuated by the boundless greed of the usual suspect: Exxon Mobil, ConocoPhillips, Canadian Oil Sands Ltd. Imperial Oil, the Royal Bank of Scotland and many others." On 13 July 2011, according to open source reporting, seventy protesters ascended on the Montana state capitol building to protest the Alberta Tar Sands project and the Keystone, XL 36 inch underground pipeline project.^e The NCCIC assesses that Anonymous' participation in peaceful protests carries a moderate likelihood of being accompanied by cyber attacks or exploitations, though no malicious cyber activity was reported in association with this protest.

(U) On 19 July 2011, a known Anonymous member posted to Twitter the results of browsing the directory tree for Siemens SIMATIC software. This is an indication in a shift toward interest in control systems by the hacktivist group.

(U) ICS-CERT Assessment of Capabilities^{f,g,h,i}

(U//FOUO) An anonymous individual provided an open source posting on twitter of xml and html code that queries the SIMATIC software. The individual alleged access to multiple control systems and referred to "Owning" them.² The Twitter posting does not identify any systems where privileged levels of access to control systems have been obtained.

(U//FOUO) The posted xml and html code reveals that the individual understands the content of the code in relation to common hacking techniques to obtain elevated privileges. It does not indicate knowledge of ICS; rather, it indicates that the individual has interest in the application software used in control systems. The posted xml and html contained administration code used to create password dump files for a human-machine interface control system software product from Siemens. The code also contained OLE for Process Control (OPC) foundation code that is used in server communication with control system devices such as programmable logic controllers, remote terminal units, intelligent-electronic devices, and industrial controllers. No indication of exploitation capability was observed by ICS-CERT. The information assessed indicates that the individual was able to recognize and post the portions of code that would ensure others knowledgeable in control systems would take notice.

(U//FOUO) The same individual also posted the directory browse history of the software application installation. In the twitter posting the server information was not identified. This does not indicate that

² "Owning" is a common term referring to having super-user or privileged access to a computer system.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

the individual was trespassing on an operational control system - the information could have been posted based on others work or a demonstration installation on the individual's personal systems.

(U//FOUO) The capability of the individual to recognize and post code that would gain the attention of those knowledgeable in control systems, as well as their claims to have access to multiple control systems, indicates the individual has an increased interest in control systems, but does not demonstrate capabilities. There are no indications of knowledge or skill in control systems operations, design, or components. The individual may possess the necessary skill to exploit elevated privileges by hijacking credentials of valid users of the ICS software product posted based on traditional exploitation methods, not anything ICS specific. No posting by the individual indicated direct malicious activity.

DHS/NCCIC ASSESSMENT

(U//FOUO) The information available on Anonymous suggests they currently have a limited ability to conduct attacks targeting ICS. However, experienced and skilled members of Anonymous in hacking could be able to develop capabilities to gain access and trespass on control system networks very quickly. Free educational opportunities (conferences, classes), presentations at hacker conferences, and other high profile events/media coverage have raised awareness to ICS vulnerabilities, and likely shortened the time needed to develop sufficient tactics, techniques, and procedures (TTPs) to disrupt ICS. Control system exploits are released in common penetration testing software such as Metasploit release 4.0 that can be directly used with novice level skills in hacking and little to no background in control systems. Common packet inspection tools such as WireShark and Netmon have improved to the point where industrial protocols are supported minimizing the effectiveness of security-by-obscurity.^{j,k,l,m} In addition, there are control systems that are currently accessible directly from the Internet and easy to locate through internet search engine tools and applications. These systems could be easily located and accessed with minimal skills in order to trespass, carry out nefarious activities, or conduct reconnaissance activities to be used in future operations.^{n,o,p}

(U//FOUO) Anonymous has recently called on their members to target energy companies based on "Green Energy" initiative performance. This targeting could likely extend beyond Anonymous to the broader hacktivist community, resulting in larger-scope actions against energy companies.^{q,r} Asset owners and operators of critical infrastructure control systems are encouraged to engage in addressing the security needs of their control system assets.

POINTS OF CONTACT

(U) This NCCIC Bulletin was produced by the NCCIC Analysis Group and the DHS Control Systems Security Program/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in coordination with the other NCCIC Functional Groups and Operational Components.

a (U) The New York Times, "Malwebolence, The World of Web Trolling," <http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html>, 3 August 2008, accessed 16 September 2011.

b. (U) PASTEBIN, "Untitled," <http://pastebin.com/vrDGwuUH>, accessed July 29, 2011.

c. (U) Suzanne Choney, "Anonymous hacks Monsanto computers; posts employee info," MSNBC, July 13, 2011. http://technolog.msnbc.msn.com/_news/2011/07/13/7076220-anonymous-hacks-monsanto-computers-posts-employee-info, accessed July 29, 2011.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

-
- d. (U) Anonnews.org, "Anonymous Operation Green Rights \ Project Tarmaggedon," <http://www.anonnews.org/?p=press&a=item&i=1021>, last accessed July 24, 2011.
- e. Adams, John S., "Pipeline protesters hit Montana governor's office", USA Today, http://www.usatoday.com/news/nation/2011-07-13-montana-oil-protest_n.htm, accessed September 12, 2011.
- f. (U) Pastie, "#2243211 – Pastie," <http://pastie.org/2243211>, last accessed July 20, 2011.
- g. (U) PasteBay, "PasteBay.com – Free uncensored text hosting," <http://pastebay.com/133000>, last accessed July 20, 2011.
- h. (U) PASTEBIN, "[Prolog]pr0f – Pastebin.com," <http://pastebin.com/DDbmJK90>, last accessed July 20, 2011.
- i. (U) PASTEBIN, "[HTML] pr0f – Pastebin.com," <http://pastebin.com/wY6XD97L>, last accessed July 21, 2011.
- j. WireShark, "Display Filter Reference: Common Industrial Protocol," <http://www.wireshark.org/docs/dfref/c/cip.html>, last accessed September 15, 2011.
- k. WireShark, "Display Filter Reference" EtherNet/IP (Industrial Protocol)" <http://www.wireshark.org/docs/dfref/e/enip.html>, last accessed September 15, 2011.
- l. Hulsebos, Rob, "Network Analysis and the challenge of Industrial Automation protocols," Industrial Ethernet Book, <http://www.iebmedia.com/index.php?id=5597&parentid=63&themeid=255&hft=41&showdetail=true&bb=1&PHPSESSID=rro01ah93rh2kkrjao3r01p152>, last accessed September 15, 2011.
- m. Morris, Jeff, "Re: [tcpdump-workers] request for DLT_WIHART for Wireless HART", SECLISTS.ORG, July 25, 2011, <http://seclists.org/wireshark/2011/Jul/511>, last accessed September 15, 2011.
- n. Mills, Elinor, "Researchers warn of SCADA equipment discoverable via Google" CNET, August 2, 2011, http://news.cnet.com/8301-27080_3-20087201-245/researchers-warn-of-scada-equipment-discoverable-via-google/, last accessed September 13, 2011.
- o. ICS-CERT, "ICS-ALERT-10-301-01 – Control System Internet Accessibility," October 28, 2010, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, last accessed September 13, 2011.
- p. Goodi, Dan, "Hackers tap SCADA Vuln Search Engine" theregister.co.uk, November 2, 2010, http://www.theregister.co.uk/2010/11/02/scada_search_engine_warning/, last accessed September 13, 2011.
- q. Vallance, Chris, "Activists turn 'hacktivists' on the web", BBC, March 16, 2010, <http://news.bbc.co.uk/2/hi/technology/8567934.stm>, last accessed September 12, 2011.
- r. (U) Lacey, Stephen, "In a Cable Released by WikiLeaks, State Department Officials Encourage Canada to Spin News Coverage of Tar Sands Pipeline" thinkprogress.org, July 13, 2011, <http://thinkprogress.org/romm/2011/07/13/268391/wikileaks-state-department-tar-sands-pipeline/>, last accessed September 12, 2011.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Dvorkin, Corey

From: Grigsby, Alexandre
Sent: September-09-11 9:19 AM
To: Mohammed, Melanie; Green, Amanda; Dvorkin, Corey
Subject: this reads like something out of criminal minds

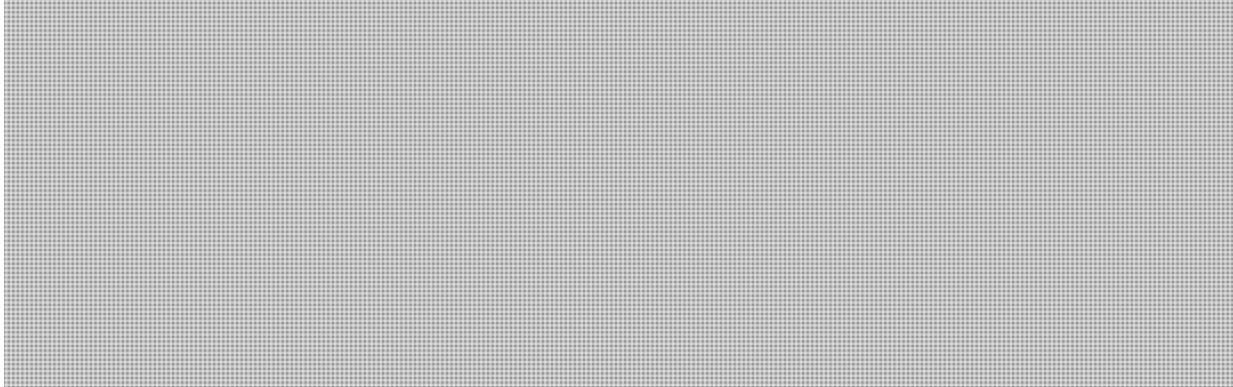
<http://arstechnica.com/tech-policy/news/2011/09/bisexual-money-grubber-with-aspergers-how-to-troll-anonymous.ars>

Alexandre Grigsby
Policy Analyst | Analyste des politiques
National Cyber Security Policy | Cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel: 613.949.4243

CYBERDO

From: Beaudoin, Luc S
Sent: September-06-11 3:26 PM
To: CYBERDO
Subject: anonymous activities against oil sands

s.15(1) - Int'l
s.16(2)(c)



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

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>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

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

CYBERDO

From: Gurb Singh <Gurbinder.Singh@rcmp-grc.gc.ca>
Sent: September-06-11 2:15 PM
To: CYBERDO s.15(1) - Subv
Cc: [REDACTED]
Subject: Anonymous Group
Attachments: page1.pdf

Good day,

We have received the following information regarding a continual and focused attack by Anonymous Group against the following:

- CNRL (Canadian Natural Resources Limited)
- CAPP (Canadian Association of Petroleum Producers)
- Trans Canada Corporation

All three Corporations have been identified in various Twitter, Pastebin, website postings as part of the focused effort against the Alberta Tarsands. RCMP ITCU in Alberta and Saskatchewan have been tracking much of the activity including the most recent postings of email addresses for various companies, including CAPP. We believe this may be seen as somewhat of an "invite" to start an email campaign against the companies, including a focused email "phishing" campaign to inject malware into their companies.

At the current time, We have no information to suggest that there has been any successful attempt to hack into any of the companies. There is however, significant concern by all Energy Stakeholders that they will fall victim to the repeated and continual efforts. The "attacks" we see today may simply be part of a reconnaissance to gather information about the companies (technical and resources).

Attached is an example of an Excel document we received this morning from CAPP with hostile network alerts.

Any assistance that can be provided would be greatly appreciative.

Gurb Singh

Gurb Singh (Cpl)
R.C.M.P - Royal Canadian Mounted Police

Technological Crime Branch
Operations Support Analyst
Operations Coordination and Liaison

T.P.O.F. - Technical and Protective Operations Facilities.
1426 St. Joseph Blvd.
Ottawa, Ontario K1A 0R2
PH:(613)949-2256

"This electronic mail message is intended only for the use of the party(ies) to whom it is addressed. This message may contain information that is privileged or confidential. Any use of the information by anyone other than the intended recipient(s) is prohibited. If you receive this message in error, please notify the sender immediately and delete both the original message and all copies. Thank you.

Ce courrier électronique est réservé à l'usage des personnes auxquelles il s'adresse. Ce message peut contenir de l'information protégée ou confidentielle. Toute utilisation de l'information par des personnes autres que celles auxquelles il s'adresse est interdite. Si vous avez reçu ce message par erreur, veuillez en aviser immédiatement l'expéditeur et détruisez le message original ainsi que les copies. Merci."

DATE	TIME	VECTOR	SOURCE IP	SOURCE	DESTINATION IP	DESTIN	PORT	LIST	REQ	ISP	APIN
2/9/2011	13:44:56.512	port scan detected									
2/9/2011	13:23:30.112	TCP FIN scan detected									
2/9/2011	13:23:28.848	port scan detected									
2/9/2011	13:21:00.624	port scan detected									
2/9/2011	11:50:58.928	TCP FIN scan detected									
2/9/2011	11:44:08.624	port scan detected									
2/9/2011	10:41:26.320	port scan detected									
2/9/2011	10:41:24.944	port scan detected									
2/9/2011	09:54:53.176	port scan detected									
2/9/2011	09:37:36.592	port scan detected									
2/9/2011	09:36:36.400	port scan detected									
2/9/2011	08:54:19.144	port scan detected									
2/9/2011	08:14:26.000	TCP FIN scan detected									
2/9/2011	08:00:02.464	port scan detected									
2/9/2011	06:28:44.464	port scan detected									
1/9/2011	16:08:30.816	XSS Generic Cross-Site									
1/9/2011	16:07:44.752	XSS Generic Cross-Site									

s.16(2)(c)