Lacroix, Lise: SBTMS-SMTPE

From: Phillips, James: SSC-SPC
Sent: Monday, January 28, 2013 15:20
To: Network Security - Securite De Reseau; IT Security
Subject: FW: [CE2013-1678] Possible 16(2)(c) infection(s) at IC

FYI ....

From: 15(1) [mailto: 15(1) @CSE-CST.GC.CA]
Sent: Monday, January 28, 2013 1:27 PM
To: Phillips, James: SSC-SPC; CTEC
Subject: RE: [CE2013-1678] Possible 16(2)(c) infection(s) at IC

Classification: UNCLASSIFIED

Hi James,
The information ultimately came from a victim. However, at this point it has been determined that the information is likely a false positive.
15(1)

15(1)
GC-CTEC Cyber Duty Officer

From: james.phillips@ssc-spc.gc.ca [mailto:james.phillips@ssc-spc.gc.ca]
Sent: January 28, 2013 12:15 PM
To: 15(1)
Cc: NSGSecurity-SecuriteGSR@ic.gc.ca
Subject: RE: [CE2013-1678] Possible 16(2)(c) infection(s) at IC

Hi 15(1),

What signature or detection technique are you using to classify the flow as " 16(2)(c) "?

James Phillips
Technical Specialist, Network Security | Spécialiste technique, sécurité du réseau
Shared Services Canada - Industry Canada | Services partagés Canada - Industrie Canada
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
James.Phillips@ic.gc.ca
Telephone | Téléphone 613-941-7874
Facsimile | Télécopieur 613-941-4615
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Edwards, Robert: SSC-SPC
Sent: Thursday, January 24, 2013 3:55 PM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR
Cc: IT Security
Subject: RE: [CE2013-1678] Possible 16(2)(c) infection(s) at IC

Denis, we will need to go back to CTEC for more details, specifically external targets which were impacted by a DDOS.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Thursday, January 24, 2013 3:32 PM
To: NSG Security - Securité GSR
Cc: IT Security
Subject: FW: [CE2013-1678] Possible 16(2)(c) infection(s) at IC
Importance: High

Hi,

An issue on the network was raised from CTEC. Can you please do the recommended checks and come back to us if there are concerns

Thank you

From: 15(1) [mailto: 15(1) @CSE-CST.GC.CA]
Sent: Thursday, January 24, 2013 3:21 PM
To: IT Security; CTEC
Subject: [CE2013-1678] Possible 16(2)(c) infection(s) at IC
Importance: High

Classification: UNCLASSIFIED

Hello,

GC-CTEC has received information from a trusted partner indicating that one or more hosts behind the 16(2)(c) may be infected with the 16(2)(c) There are indications that host 16(2)(c)

GC-CTEC recommends that 16(2)(c) 16(2)(c)

For more information on 16(2)(c) 16(2)(c)

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca. Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC.

http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf

Thanks,

15(1)

GC-CTEC Cyber Duty Officer

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, February 6, 2013 10:53
To: Gorman, Joseph: CIO-BI (NCR-RCN); Fournier, Denis: CIO-BI
Subject: FW: CE2013-1703

Fyi. I have given this Cyber Event IT Security Incident number ITSINC-2013-027.
Thanks,
Jen

-----Original Message-----
From: Fournier, Denis: CIO-BI
Sent: Wednesday, February 6, 2013 9:34 AM
To: Cullen, Jennifer: CIO-BI
Subject: FW: CE2013-1703

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, February 5, 2013 4:49 PM
To: Fournier, Denis: CIO-BI
Cc: CTEC
Subject: CE2013-1703

Classification: PROTECTED B

Hello Denis,

Please find attached tipper for your action as soon as possible.

Regards,

15(1)

15(1)
GC-CTEC - Incident Handler
15(1)

Lacroix, Lise: SBTMS-SMTPE

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 10:38
To: Fournier, Denis: CIO-BI
Subject: FW: Infected computer sending Spam

Hi Denis,

The message below was meant for you.

Elias

From: Begin, Denis: SSC-SPC (NCR-RCN)
Sent: Wednesday, January 23, 2013 10:36 AM
To: Farah, Elias: SSC-SPC; Fournier, Denis: CIO-BI
Subject: Re: Infected computer sending Spam

Sorry, which Denis.... Me or Fournier?

For me, I provided Denis Fournier with 16(2)(c) 16(2)(c)

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 10:28 AM
To: Fournier, Denis: CIO-BI; Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security
Subject: RE: Infected computer sending Spam

Hi Denis,

Can you please provide us with all the information you have regarding this incident? Including the ctec alert and timeline of events.

Thanks,

Elias

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:33 AM
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Rob, here are the 4 examples of emails that were sent with the account.

<< Message: 16(2)(c) >> << Message: 16(2)(c)
>> << Message: 16(2)(c) >> << Message: 16(2)(c) >>

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:29 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Can you provide an original message which went outbound? As well, within the mail logs, if enable, the ability to see originating IP address. You need to look deep.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:27 AM
To: NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: Infected computer sending Spam

Hi Guy's,

We have an internal computer that sent Spam on 16(2)(c)
We have the logs that show this was sent and we have the account sent items that show all the emails.

21(1)(a),21(1)(b)

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, February 13, 2013 11:44
To: 15(1)
Cc: CTEC; Fournier, Denis: CIO-BI
Subject: RE: CE2013-1602 - IC ITSINC-2013-003

Thank you for the update 15(1)
Jennifer

From: 15(1) [mailto: 15(1) @CSE-CST.GC.CA]
Sent: Wednesday, February 13, 2013 11:39 AM
To: Cullen, Jennifer: CIO-BI
Cc: CTEC; Fournier, Denis: CIO-BI
Subject: RE: CE2013-1602 - IC ITSINC-2013-003

Classification: PROTECTED B

Hi Jennifer, analysis on 1602 is still ongoing. As soon as the forensics are complete a Technical Analysis Report (TAR) will be approved for release and I will be in touch re handover. I am sorry but I cannot promise an ETA for the TAR but assure you that as soon as it's released it will be issued.

15(1)
Cyber Threat Evaluation Centre
Communications Security Establishment Canada
Centre d'évaluation des cybermenaces
Centre de la sécurité des télécommunications Canada

15(1) FAX: 613.949.5377

15(1) [call 15(1) before sending a secure fax]
15(1)

Contactez/reach CTEC? ctec@cse-cst.gc.ca
CSEC : Among National Capital Region's Top Employers 2013 / CSTC : l'un des meilleurs employeurs de la région de la capitale nationale (RCN) pour 2013

From: Jennifer.Cullen@ic.gc.ca [mailto:Jennifer.Cullen@ic.gc.ca]
Sent: February 13, 2013 10:14 AM
To: 15(1)
Cc: CTEC; Denis.Fournier@ic.gc.ca
Subject: RE: CE2013-1602 - IC ITSINC-2013-003

Hi 15(1)

We are trying to update our files and, as such, would it be possible to get an update on CE2013-1602? In regards to response activities from a CSEC perspective, 16(2)(c) 16(2)(c)

Thank you,
Jennifer

From: 15(1) [mailto: 15(1) @CSE-CST.GC.CA]
Sent: Wednesday, January 16, 2013 3:19 PM
To: Fournier, Denis: CIO-BI
Cc: Cullen, Jennifer: CIO-BI
Subject: CE2013-1602

Classification: PROTECTED B

Denis,

Attached is a transmittal receipt for your records. I will deal with you on this file, as per Jennifer's instructions.

15(1)
Cyber Threat Evaluation Centre
Communications Security Establishment Canada
Centre d'évaluation des cybermenaces
Centre de la sécurité des télécommunications Canada

15(1) FAX: 613.949.5377

15(1) [call 15(1) before sending a secure fax]
15(1)

Contactez/reach CTEC? ctec@cse-cst.gc.ca

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Tuesday, April 17, 2012 16:13
To: CTEC
Subject: [CE2012-514]: Canada Post "Phishing" Email Leads to System Compromises

Classification: UNCLASSIFIED

A recent Pastebin posting describes a Canada Post "Phishing" email for a 16(2)(c). Those receiving this fake notice are prompted to visit a link in order to reschedule; but the link actually leads to an executable pif file that tries to install malware onto the visiting system. 16(2)(c)) The Pastebin posting can be found here: http://pastebin.com/pnBjzPMN

At least one system within your organization was observed visiting this link between 16(2)(c), 2012 and therefore your threat exposure is rated by GC-CTEC as very high . GCCTEC highly recommends

16(2)(c),21(1)(a)

Incidents affecting GC infrasturectures should be reported to GC-CTEC at ctec@cse-cst.gc.ca. Any government department suspecting cyber incidents should provide a written report to GC-CTEC (see below).

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

This email is for the purpose of protecting Government of Canada computer networks. It may be disseminated within your department for the protection of your networks. No further dissemination is permitted without approval from GC-CTEC.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, May 16, 2012 15:59
To: IT Security
Cc: CTEC
Subject: [CE2012-615]: University of New Brunswick Compromised - Information Posted to Public Forum

Classification: UNCLASSIFIED

Hello,

Earlier this week, it was revealed that a hacking group had broken into a computer system at the University of New Brunswick. This group then posted some of the stolen data onto a public website known as Pastebin.com. Details of this story can be found at the CBC link here:

http://www.cbc.ca/news/canada/new-brunswick/story/2012/05/15/nb-unb-hacked.html

Your agency is being contacted because someone working there has had their contact information as an employer and/or their user names and passwords posted on Pastebin and may be at risk.

Anyone who's login credentials were exposed should take the following precautions:

16(2)(c),21(1)(a)

Those whose contact information was exposed may be targeted by cyber criminals pretending to be from UNB or related agencies.

Contact Information Exposed:

<none>

Login Credentials Exposed:

19(1)

Should you require further information please contact us.

<---------->
15(1)
GC-CTEC Cyber Duty Officer
Cyber Threat Evaluation Centre
Tel# 15(1)

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal

response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems. 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

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, June 1, 2012 15:27
To: IT Security
Cc: CTEC
Subject: [CE2012-698]: Login Credentials Exposed on Public Website

Classification: UNCLASSIFIED

Hello,

Earlier this week, it was revealed that a hacking group had broken into a "Canada Email" website and posted some of the stolen data onto a public website known as Pastebin.com.

Your agency is being contacted because someone working there has had their user name and password from this website posted on Pastebin and may be at risk.

Anyone who's login credentials were exposed should take the following precautions:

16(2)(c),21(1)(a)

Login Credentials Exposed:

19(1)

Should you require further information please contact us.

15(1)
<------------>
15(1)
GC-CTEC - Cyber Duty Officer
15(1)
--
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems. 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

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Tuesday, November 20, 2012 8:15
To: IT Security
Cc: CTEC
Subject: [CE2012-1429]: Login Credentials Exposed in Online Posting

Classification: UNCLASSIFIED

Hello,

A hacking group has broken into an unknown website and posted information stolen from it to Pastebin.com.

Your agency is being contacted because someone working there has had their user name and password posted online and may be at risk. The following information was exposed:

Email : password

19(1)

GC-CTEC recommends the following precautions be taken:

16(2)(c),21(1)(a)

Should you require further information please contact us.

Thank you,

15(1)
<---------->
15(1)
GC-CTEC Cyber Duty Officer
Cyber Threat Evaluation Centre
CTEC@CSE-CST.GC.CA
15(1)
--

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems. To report incidents affecting GC infrastructures, please complete this form: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and contact GC-CTEC at ctec@cse-cst.gc.ca or (613)991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 16:49
To: CTEC
Subject: CECM-GC - Cybercapsule GCCF12-009: Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC

Classification: UNCLASSIFIED

==========
CECM-GC - Cybercapsule GCCF12-009
Date : 2 novembre 2012
==========

PUBLIC
======
Cette cybercapsule est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

TITRE
=====
Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC

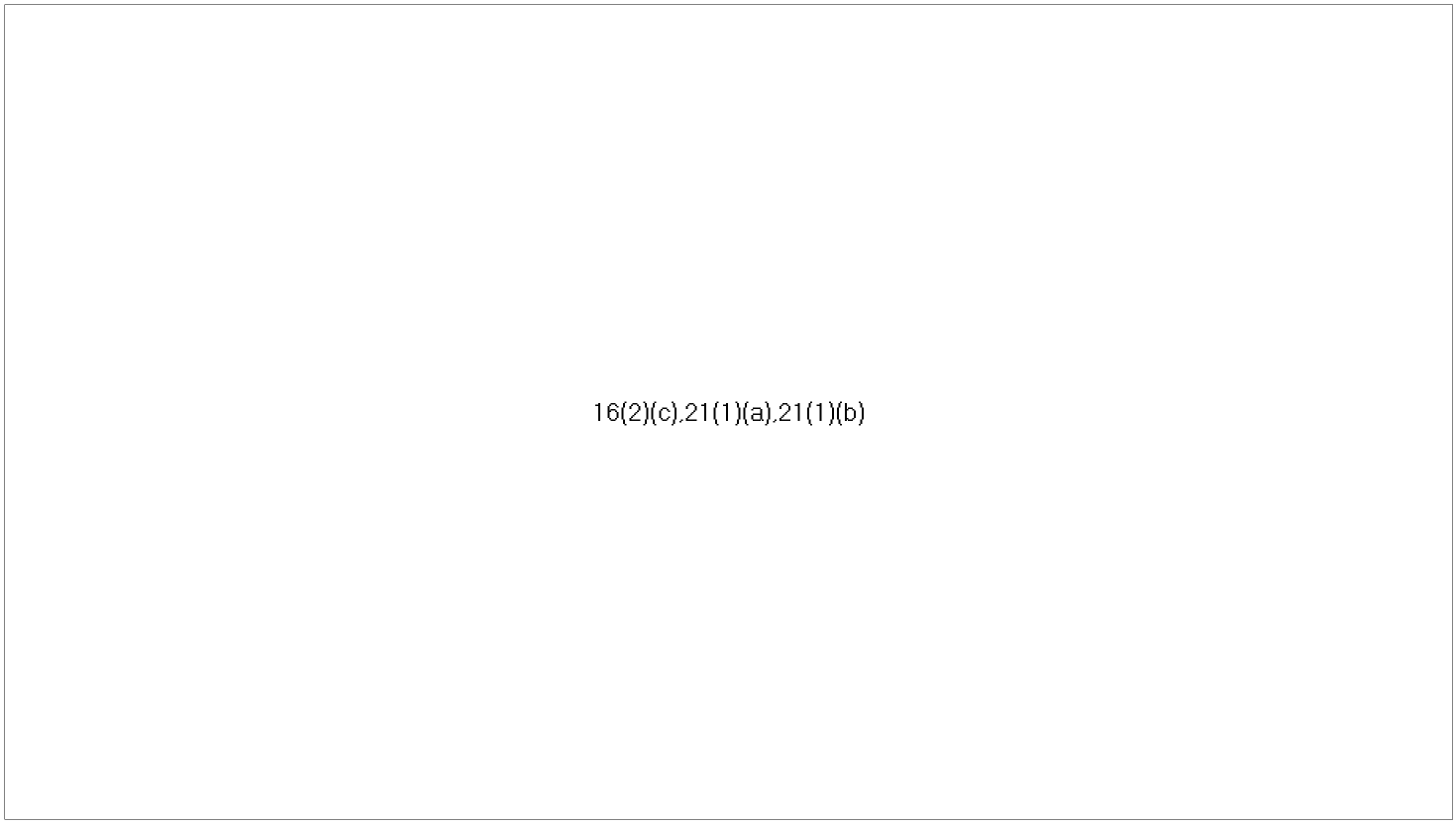
DÉTAILS
=======
Cette cybercapsule est liée à la note d'information IN12-002 intitulée « Anonymous – Attaque par déni de service distribué visant le GC » et aux mises à jour connexes.

High Orbit Ion Cannon (HOIC) est un outil multifil de déni de service distribué basé sur Windows qui transmet des demandes HTTP. En règle générale, c'est Anonymous qui utilise cet outil pour mener une attaque. Pour qu'il fonctionnement de manière efficace, HOIC repose sur un script d'appoint (booster script) configurable qui est souvent affiché publiquement. Les utilisateurs peuvent exploiter le script d'appoint de façon à ce qu'il précise une liste de rotation d'adresses URL pour les requêtes HTTP GET ou POST (données précisées par l'utilisateur). Les utilisateurs peuvent également définir l'agent-utilisateur de manière aléatoire (en fonction d'une liste définie par l'utilisateur) et créer des en-têtes personnalisés (composés de chaînes définies par l'utilisateur, annexées dans l'ordre de leur choix). L'utilisateur peut aussi régler le taux de requête (réglé par défaut à 2 fils).

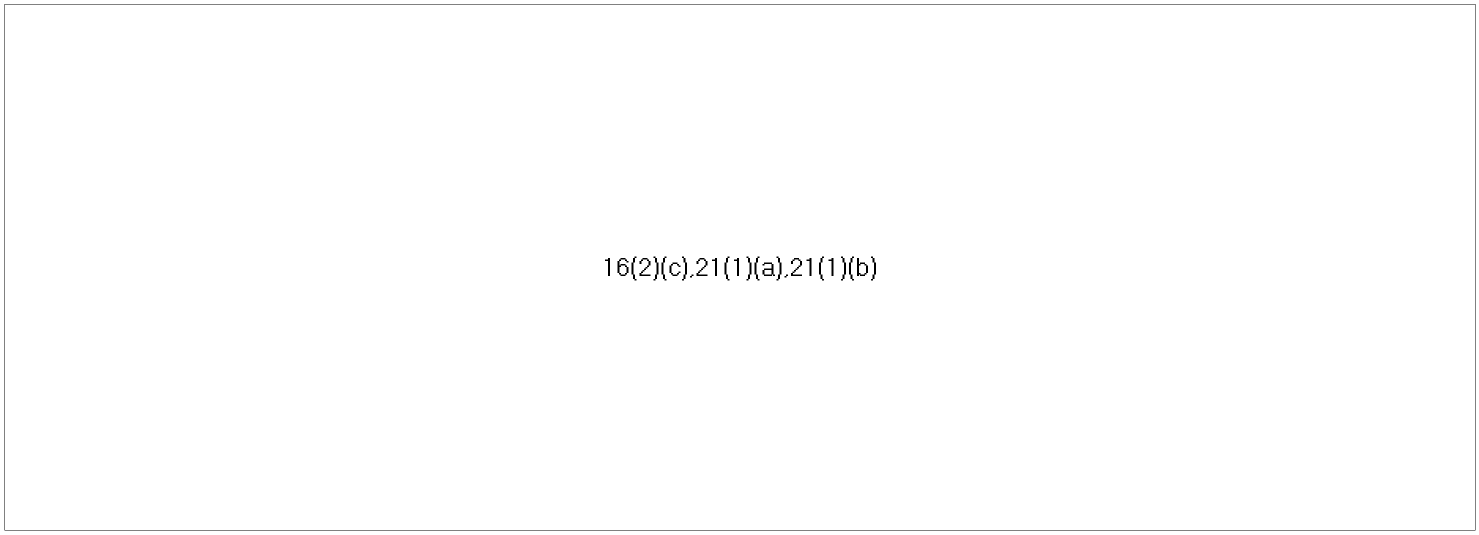
ATTÉNUATION
===========

Atténuation réseau

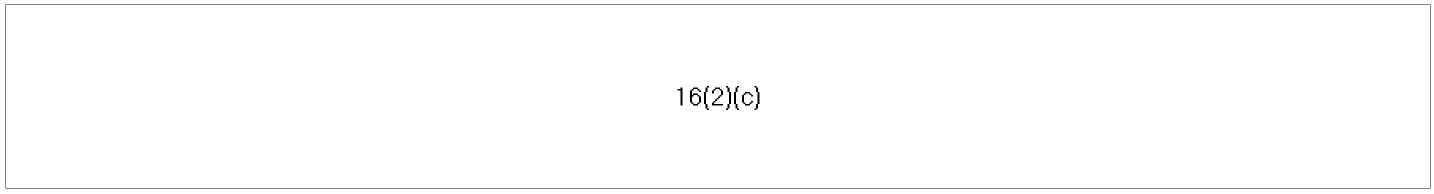
16(2)(c),21(1)(a),21(1)(b)



Afin de réduire au minimum les répercussions de cet outil d'attaque sur les sites Web, le CECM-GC recommande aux administrateurs Web du GC de mettre en œuvre les mesures d'atténuation suivantes, dans la mesure du possible :



Bien que les noms et le contenu des en-têtes de requête soient valides, l'ordre dans lequel les en-têtes sont définis dans la requête ne correspond pas à celui dans lequel les navigateurs Web normaux les enverraient. Voici la caractéristique la plus facile à remarquer : dans HOIC, l'en-tête de l'hôte apparaît toujours à la fin de la requête, mais ce n'est pas le cas pour les navigateurs Web légitimes.



16(2)(c),21(1)(a),21(1)(b)

Le trafic HOIC présente aussi la caractéristique suivante : le contenu des entêtes de requête a souvent deux espaces en début de ligne. 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Mesure d'atténuation tactique

En plus du trafic récurrent mentionné ci-dessus, 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Avertissement :
Le CECM-GC offre l'information et les conseils d'atténuation ci-dessus en fonction des menaces envers les réseaux du gouvernement du Canada et ne recommande pas que cette information soit utilisée à d'autres fins.
L'information contenue dans le présent message est fournie exclusivement aux fins de reconfiguration défensive des biens appartenant au destinataire.
Le destinataire ne doit en aucun cas participer à des activités de collecte d'information à l'extérieur de son propre périmètre réseau au moyen des renseignements contenus dans le présent document. Ces activités comprennent la vérification, le téléchargement, la navigation et le balayage des sites mentionnés dans le présent rapport.

SIGNALEMENT DES INCIDENTS
==========
Les ministères qui croient avoir été victimes d'un incident lié à l'activité décrite dans le présent document doivent soumettre un rapport écrit au CECM-GC. Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

AVIS : Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

Le présent message et ses pièces jointes contiennent des renseignements pouvant provenir de sources externes et dont le CECM-GC ne peut pas vérifier l'exactitude ni l'intégrité. Le CECM-GC ne sera pas responsable des conséquences négatives résultant de l'utilisation de ces renseignements.

Les liens vers les sites Web sur lesquels le gouvernement du Canada n'exerce aucun

contrôle sont fournis aux utilisateurs pour des raisons de commodité seulement. Le GC n'est pas responsable de l'exactitude, de l'actualité ni de la fiabilité du contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites ou leur contenu.

NOTE AUX LECTEURS
==========
Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.
Pour signaler les incidents touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC par courriel à ctec@cse-cst.gc.ca ou par téléphone au 613-991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 16:51
To: CTEC
Subject: CECM-GC - Cybercapsule GCCF12-010: Mesures d'atténuation pour la campagne visant les formulaires de sites Web du GC

Classification: UNCLASSIFIED

English version previously sent.

==========
CECM-GC - Cybercapsule GCCF12-010
Date : 2 novembre 2012
==========

PUBLIC
======
Cette cybercapsule est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

TITRE
=====
Mesures d'atténuation pour la campagne visant les formulaires de sites Web du GC

DÉTAILS
=======
Cette cypercapsule porte sur une campagne ciblant les formulaires de sites Web du GC. Des serveurs Web du GC ont reçu un grand nombre de formulaires contenant des entrées invalides. Bon nombre de ces formulaires sont soumis à l'aide de méthodes automatisées.

ATTÉNUATION
==========
Afin de réduire au minimum les répercussions de ces attaques, le CECMGC recommande aux administrateurs Web du GC de mettre en œuvre les mesures d'atténuation suivantes, dans la mesure du possible :

16(2)(c),21(1)(a),21(1)(b)

Avertissement :
Le CECM-GC offre l'information et les conseils d'atténuation ci-dessus en fonction des menaces envers les réseaux du gouvernement du Canada et ne recommande pas que cette information soit utilisée à d'autres fins.

L'information contenue dans le présent message est fournie exclusivement aux fins de reconfiguration défensive des biens appartenant au destinataire.

Le destinataire ne doit en aucun cas participer à des activités de collecte d'information à l'extérieur de son propre périmètre réseau au moyen des renseignements contenus dans le présent document. Ces activités comprennent la vérification, le téléchargement, la navigation et le balayage des sites mentionnés dans le présent rapport.

SIGNALEMENT DES INCIDENTS
==========
Les ministères qui croient avoir été victimes d'un incident lié à l'activité décrite dans le présent document doivent soumettre un rapport écrit au CECM-GC. Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

AVIS : Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

Le présent message et ses pièces jointes contiennent des renseignements pouvant provenir de sources externes et dont le CECM-GC ne peut pas vérifier l'exactitude ni l'intégrité. Le CECM-GC ne sera pas responsable des conséquences négatives résultant de l'utilisation de ces renseignements.

Les liens vers les sites Web sur lesquels le gouvernement du Canada n'exerce aucun contrôle sont fournis aux utilisateurs pour des raisons de commodité seulement. Le GC n'est pas responsable de l'exactitude, de l'actualité ni de la fiabilité du contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites ou leur contenu.

NOTE AUX LECTEURS
==========
Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Pour signaler les incidents touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC par courriel à ctec@cse-cst.gc.ca ou par téléphone au 613-991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Tuesday, October 30, 2012 16:00
To: CTEC
Subject: CORRECTION: Cyber Flash / Cybercapsule GCCF12-008: DDoS campaign against the GC

Importance: High

Classification: UNCLASSIFIED

This Cyber Flash was erroneously issued with the incorrect reference number of GCFC12-007. The correct reference number is GCCF12-008.

We apologise for any confusion this may have caused.

****

La version francaise suivra.

==========
GC-CTEC - Cyber Flash GCCF12-008
Date: 30 October 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal government.

TITLE
=====
DDoS campaign against the GC

DETAILS
=======
This Cyber Flash is related to 'Information Note IN12-002: Anonymous DDoS activity against GC' and all updates.

On 22 October, GC-CTEC was notified that some GC departments were experiencing degraded states or periods of being offline. Further investigation resulted in the discovery of DDoS related techniques that looks to be beyond what has been characteristically attributed to Anonymous or HOIC capabilities. 21(1)(b)

21(1)(b)

This campaign has had several characteristics that set it apart from a typical DDoS event which typically use SYN or HTTP Get flooding:

16(2)(c),21(1)(b)

16(2)(c).21(1)(b)

MITIGATION
==========

16(2)(c).21(1)(a).21(1)(b)

Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.
The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

REPORTING
=========
Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC. To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

NOTE TO READERS
==========
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.
To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca or (613)991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, November 2, 2012 16:15
To: CTEC
Subject: Cyber Flash / Cybercapsule GCCF12-009: Possible use of HOIC for DDoS campaign against the GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC-CTEC - Cyber Flash GCCF12-009
Date: 02 November 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal government.

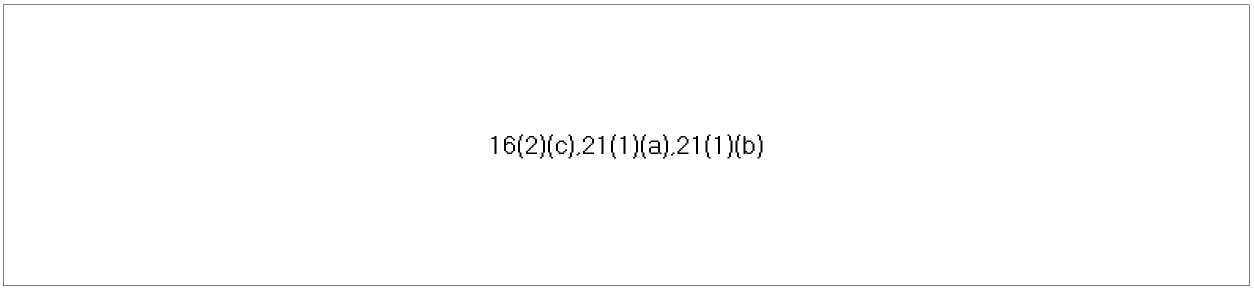
TITLE
=====
Possible use of HOIC for DDoS campaign against the GC

DETAILS
=======
This Cyber Flash is related to 'Information Note IN12-002: Anonymous DDoS activity against GC' and all updates.

The High Orbit Ion Cannon (HOIC) is a Windows-based DDoS tool characteristically attributed to Anonymous. HOIC is a multi-threaded DDoS tool that transmits HTTP requests. In order for it to work effectively, HOIC relies on a configurable "booster" script that is commonly posted publicly. Users may leverage the booster script to specify a list of rotating URLs for HTTP requests, using either the GET or POST (user-specified data) request methods. Users may also randomize the user-agent (based on a user-defined list) and create custom headers (composed of user-defined strings, appended in the order of their choice). The request rate can also be set (default is 2 threads).

MITIGATION
==========

Network-based mitigation



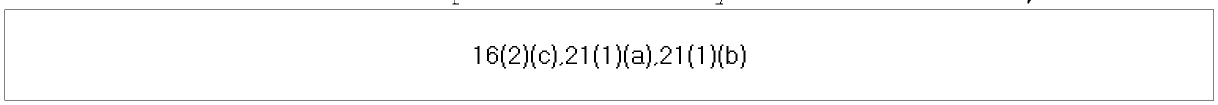
16(2)(c),21(1)(a),21(1)(b)

In order to help minimize the effect of this attack tool on websites, GC website administrators are advised to take the following mitigative actions where practical:

16(2)(c),21(1)(a),21(1)(b)

Tactical mitigation

In addition to the traffic patterns that may be observed above,



Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.
The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

REPORTING
=========
Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC. To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

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 GC CTEC cannot verify the accuracy and integrity. GC CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

NOTE TO READERS
==========
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.
To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca or (613)991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Tuesday, October 30, 2012 15:35
To: Hagarty, Richard: CIO-BI
Subject: FW: Cyber Flash / Cybercapsule GCCF12-007: DDoS campaign against the GC
Importance: High

Hi Richard,

FYI. There is nothing new here from an Anonymous activity point of view. This CF provides mitigation recommendations to departments. Tom will action it 19(1)

Thanks,
Jen

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, October 30, 2012 3:20 PM
To: CTEC
Subject: Cyber Flash / Cybercapsule GCCF12-007: DDoS campaign against the GC
Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC-CTEC - Cyber Flash GCCF12-007
Date: 30 October 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal government.

TITLE
=====
DDoS campaign against the GC

DETAILS
=======
This Cyber Flash is related to 'Information Note IN12-002: Anonymous DDoS activity against GC' and all updates.

On 22 October, GC-CTEC was notified that some GC departments were experiencing degraded states or periods of being offline. Further investigation resulted in the discovery of DDoS related techniques that looks to be beyond what has been characteristically attributed to Anonymous or HOIC capabilities. 21(1)(b)

21(1)(b)

This campaign has had several characteristics that set it apart from a typical DDoS event which typically use SYN or HTTP Get flooding:

16(2)(c),21(1)(a),21(1)(b)

MITIGATION
==========

16(2)(c),21(1)(a),21(1)(b)

Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.

The information contained in this message is provided strictly for the purpose of

defensive reconfiguration of assets owned by the recipient.

The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

REPORTING
=========
Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC. To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

NOTE TO READERS
===============
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca or (613)991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, October 26, 2012 16:22
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 2

Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 2: 26 October 2012
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

Limited traffic associated with a proposed Distributed Denial of Service (DDOS) attack was identified on GC networks commencing on 22 October 2012. This traffic was limited in volume and localized to specific departments. By 25 October 2012, at least 44 departments received traffic related to the DDOS. This activity is believed to be related to the Anonymous operation #OpPartyCrasher and related operations, which are scheduled to occur from 3 to 15 November 2012. 21(1)(b)

21(1)(b)

The departments receiving traffic related to this activity may be affected to varying degrees, from no observable effect to a successful DDOS. The way the network responds to this DDOS traffic depends on many factors, 16(2)(c)

16(2)(c)

GC-CTEC advises that the scope and level of activity may increase as the targeted date range approaches.

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both :

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 13:24
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========
On 20 October 2012, GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous was planning against the GC. The Anonymous activity is being distributed under the name of #OpPartyCrasher, but several other operations are also linked to this activity. The manifesto, schedule and the configuration files for the attack, are being posted to public file sharing sites. The tool being used for this campaign is the High Orbit Ion Cannon (HOIC). The goal appears to be disruption of GC sites and services.

According to the publicly posted schedule, the operation is scheduled to run 3 to 15 November 2012. Traffic that is related to this DDOS attack has been observed as early as 22 October 2012. The level of activity appears to be increasing on each subsequent day. 16(2)(c) 16(2)(c) GC-CTEC advises that the scope and level of activity may increase as we move into the targeted date range. 21(1)(b) 21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider.

To report any outages or suspicious network activities that require

mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@tpsgc-pwgsc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 16:55
To: CTEC
Subject: Mise à jour no 1: CECM-GC - Cybercapsule GCCF12-009: Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC

Classification: UNCLASSIFIED

English version previously sent.

CECM-GC - Cybercapsule GCCF12-009
Date : 2 novembre 2012
==========

AVIS : Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

==========
Mise à jour no 1 : 5 novembre 2012
- Mise à jour de la section sur l'atténuation
- Vérification du référent avec les domaines de moteurs de recherche
- Utilisation de termes de recherche invraisemblables, y compris « http:// » en tant qu'URI
==========

PUBLIC
======
Cette cybercapsule est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

TITRE
=====
Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC

DÉTAILS
=======
Cette cybercapsule est liée à la note d'information IN12-002 intitulée « Anonymous – Attaque par déni de service distribué visant le GC » et à toutes les mises à jour connexes.

High Orbit Ion Cannon (HOIC) est un outil multifil de déni de service distribué basé sur Windows qui transmet des demandes HTTP. Anonymous est généralement l'auteur des attaques menées à l'aide de cet outil. Pour qu'il fonctionne de manière efficace, HOIC repose sur un script d'appoint (booster script) configurable qui est souvent affiché publiquement. Les utilisateurs peuvent exploiter le script d'appoint de façon à ce qu'il précise une liste de rotation d'adresses URL pour les requêtes HTTP, au moyen des méthodes de requête GET ou POST (données précisées par l'utilisateur). Ils peuvent également définir l'agent-utilisateur de manière aléatoire (en fonction d'une liste définie par l'utilisateur) et créer des en-têtes personnalisés (composés de chaînes définies par l'utilisateur, annexées dans l'ordre de leur choix). Les utilisateurs peuvent aussi régler le taux de requête (réglé par défaut à 2 fils).

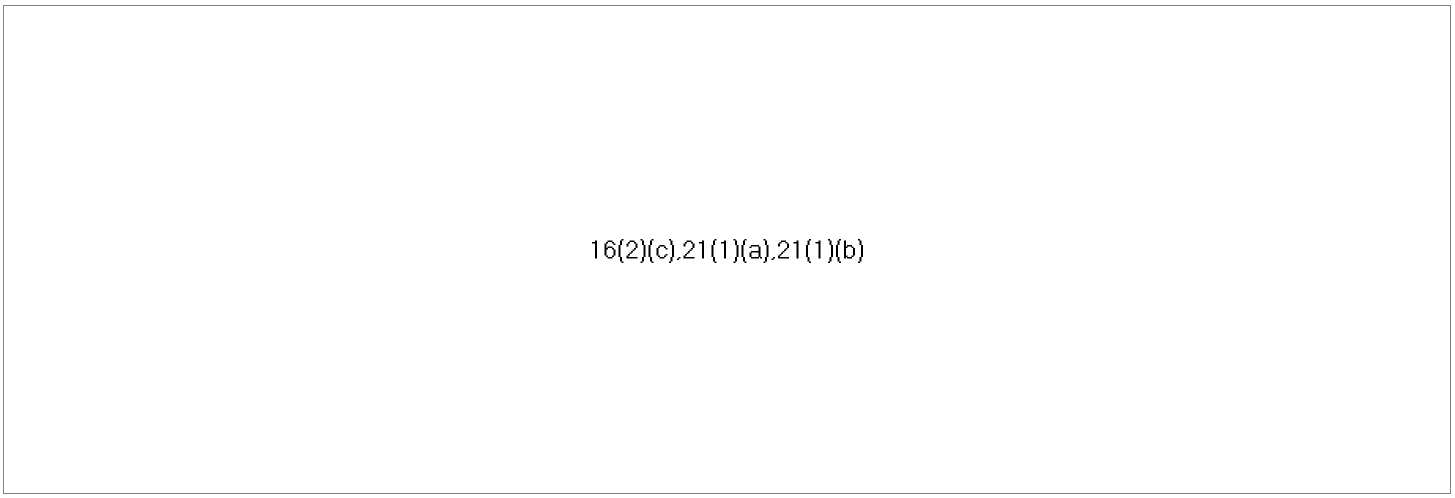
ATTÉNUATION
==========

Atténuation réseau

16(2)(c).21(1)(a).21(1)(b)

Afin de réduire au minimum les répercussions de cet outil d'attaque sur les sites Web, le CECM-GC recommande aux administrateurs Web du GC de mettre en œuvre les mesures d'atténuation suivantes, dans la mesure du possible :

16(2)(c).21(1)(a).21(1)(b)



Bien que les noms et les données utiles des en-têtes de requête soient valides, l'ordre dans lequel les en-têtes sont définis dans la requête ne correspond pas à celui dans lequel les navigateurs Web normaux les enverraient. Voici la caractéristique la plus facile à remarquer : dans HOIC, l'en-tête de l'hôte apparaît toujours à la fin de la requête, mais ce n'est pas le cas pour les navigateurs Web légitimes.

Atténuation tactique

En plus du trafic récurrent mentionné ci-dessus, 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Avertissement :
Le CECM-GC offre l'information et les conseils d'atténuation ci-dessus en fonction des menaces envers les réseaux du gouvernement du Canada et ne recommande pas que cette information soit utilisée à d'autres fins.

L'information contenue dans le présent message est fournie exclusivement aux fins de reconfiguration défensive des biens appartenant au destinataire.
Le destinataire ne doit en aucun cas participer à des activités de collecte d'information à l'extérieur de son propre périmètre réseau au moyen des renseignements contenus dans le présent document. Ces activités comprennent la vérification, le téléchargement, la navigation et le balayage des sites mentionnés dans le présent rapport.

SIGNALEMENT DES INCIDENTS
==========
Les ministères qui croient avoir été victimes d'un incident lié à l'activité décrite dans le présent document doivent soumettre un rapport écrit au CECM-GC. Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

AVIS : Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

Le présent message et ses pièces jointes contiennent des renseignements pouvant provenir de sources externes et dont le CECM-GC ne peut pas vérifier l'exactitude ni l'intégrité. Le CECM-GC ne sera pas responsable des conséquences négatives résultant de l'utilisation de ces renseignements.

Les liens vers les sites Web sur lesquels le gouvernement du Canada n'exerce aucun contrôle sont fournis aux utilisateurs pour des raisons de commodité seulement. Le GC n'est pas responsable de l'exactitude, de l'actualité ni de la fiabilité du contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites ou leur contenu.

NOTE AUX LECTEURS
==========
Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avantgarde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.
Pour signaler les incidents touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC par courriel à ctec@cse-cst.gc.ca ou par téléphone au 613-991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, October 31, 2012 10:12
To: CTEC
Subject: Mise à jour no 2: Note d'information IN12-002: Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: NON CLASSIFIÉ

==========
CECM-GC – Note d'information IN12-002
Date : 25 octobre 2012
==========

==========
Mise à jour n° 2 : 26 octobre 2012
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======
Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

ÉVALUATION
==========

Dès le 22 octobre 2012, le CECM-GC a découvert sur des réseaux ministériels précis du GC un volume restreint de trafic lié à une attaque suggérée par déni de service distribué. Le 25 octobre 2012, plus de 44 ministères avaient reçu du trafic afférent, lequel serait lié à l'opération #OpPartyCrasher et à d'autres opérations connexes d'Anonymous devant se dérouler du 3 au 15 novembre 2012. Pour l'instant, 21(1)(b)

21(1)(b)

La gravité de l'attaque pourrait varier d'un ministère à un autre, allant d'aucun effet observable à un déni de service distribué. De nombreux facteurs expliquent la façon dont le réseau répond au trafic, 16(2)(c)

16(2)(c)

Le CECM-GC prévient les ministères que la portée et le niveau d'activité risquent d'augmenter à mesure que les dates prévues de l'opération approchent.

MESURES RECOMMANDÉES

==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur de services.

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux entités suivantes :

- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@csecst.gc.ca.

==========

Note aux lecteurs
==========
Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire

part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 15:46
To: CTEC
Subject: Mise à jour no 9: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

English version previously sent.

==========
CECM-GC – Note d'information IN12-002
Date : 2 novembre 2012
==========

==========
Mise à jour no 9 : 2 novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de la campagne de déni de service distribué visant le GC planifiée par Anonymous. Cette compagne, regroupant #OpPartyCrasher et d'autres opérations connexes, est prévue du 3 au 15 novembre 2012.

ÉVALUATION
==========

Anonymous a affiché un horaire des attaques sur pastebay[.]net (no 1151488) et a annoncé qu'il allait fournir une liste révisée des cibles et des scripts d'appoint une heure avant les heures d'attaque suivantes :

Samedi	3 novembre	De 12 h à 18 h
Dimanche	4 novembre	De 12 h à 18 h
Mardi	6 novembre	De 18 h à 22 h
Mercredi	7 novembre	De 18 h à 22 h
Jeudi	8 novembre	De 18 h à 22 h
Vendredi	9 novembre	De 18 h à 22 h

Ces heures pourraient changer, et il est impossible de les vérifier puisqu'il s'agit de la seule liste disponible.

Depuis le 25 octobre, un grand nombre de ministères ont signalé des activités comparables à des tentatives de déni de service distribué, mais aucun lien direct n'a pu être établi avec la campagne planifiée d'Anonymous. Le CECM-GC prévient les ministères

que la portée et le niveau d'activité malveillante pourraient augmenter à mesure que les dates prévues de la campagne approchent, et que les techniques d'attaque pourraient varier de celles dont se sert habituellement Anonymous. Il convient toutefois de noter que les activités observées à ce jour n'ont eu aucune incidence majeure sur le GC.

Jusqu'ici, les activités pertinentes comprennent :

16(2)(c),21(1)(a),21(1)(b)

À mesure qu'il découvrira des activités malveillantes touchant le GC, le CECM-GC diffusera des cybercapsules contenant des conseils d'atténuation technique connexes.

Depuis la diffusion de la première note d'information IN12-002, le CECM-GC a publié les documents suivants :

- GCCF12-008 : « Campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre au

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-009 : « Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-010 : « Mesures d'atténuation pour la campagne visant les formulaires de sites Web du GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

Des membres du personnel du CECM-GC et de SPC surveilleront la situation au cours de la fin de semaine, pendant les heures d'attaque annoncées, et fourniront des conseils généraux d'atténuation, dont de nouvelles cybercapsules ou mises à jour, au besoin. Le CECM-GC diffusera également au besoin des mises à jour de la note d'information IN12-002 pour informer les ministères du GC des changements concernant l'horaire des attaques et des tendances dans les activités observées de déni de service distribué.

On vous recommande de mettre en œuvre les conseils d'atténuation énoncés dans les cybercapsules susmentionnées et dans celles qui seront diffusées ultérieurement.

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :

- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 16:42
To: CTEC
Subject: Mise à jour no 10: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

English version previously sent.

==========
CECM-GC – Note d'information IN12-002
Date : 25 octobre 2012
==========

==========
Mise à jour no 10: 3 novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de la campagne de déni de service distribué visant le GC planifiée par Anonymous. Cette compagne, regroupant #OpPartyCrasher et d'autres opérations connexes, est prévue du 3 au 15 novembre 2012.

ÉVALUATION
==========

En date de la présente publication, il n'y a pas lieu de croire que les sites Web gc.ca sont perturbés. Les scripts d'appoint diffusés le 3 novembre n'ont pas présenté de changements considérables.

Les 2 et 3 novembre, un ministère du GC a signalé une tentative de déni de service distribué 16(2)(c) Cette attaque a eu toutefois très peu, voire aucune incidence sur le site Web.

Anonymous a affiché un horaire des attaques sur pastebay[.]net (no 1151488) et a annoncé qu'il allait fournir une liste révisée des cibles et des scripts d'appoint une heure avant les heures d'attaque suivantes :

Samedi	3 novembre	De 12 h à 18 h
Dimanche	4 novembre	De 12 h à 18 h
Mardi	6 novembre	De 18 h à 22 h
Mercredi	7 novembre	De 18 h à 22 h
Jeudi	8 novembre	De 18 h à 22 h

Vendredi 9 novembre De 18 h à 22 h

Ces heures pourraient changer, et il est impossible de les vérifier puisqu'il s'agit de la seule liste disponible.

Depuis le 25 octobre, un grand nombre de ministères ont signalé des activités comparables à des tentatives de déni de service distribué, mais aucun lien direct n'a pu être établi avec la campagne planifiée d'Anonymous. Le CECM-GC prévient les ministères que la portée et le niveau d'activité malveillante pourraient augmenter à mesure que les dates prévues de la campagne approchent, et que les techniques d'attaque pourraient varier de celles dont se sert habituellement Anonymous. Il convient toutefois de noter que les activités observées à ce jour n'ont eu aucune incidence majeure sur le GC.

Jusqu'ici, les activités pertinentes comprennent :

16(2)(c),21(1)(a),21(1)(b)

À mesure qu'il découvrira des activités malveillantes touchant le GC, le CECM-GC diffusera des cybercapsules contenant des conseils d'atténuation technique connexes.

Depuis la diffusion de la première note d'information IN12-002, le CECM-GC a publié les documents suivants :

- GCCF12-008 : « Campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre au

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-009 : « Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-010 : « Mesures d'atténuation pour la campagne visant les formulaires de sites Web du GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

Des membres du personnel du CECM-GC et de SPC surveilleront la situation au cours de la fin de semaine, pendant les heures d'attaque annoncées, et fourniront des conseils généraux d'atténuation, dont de nouvelles cybercapsules ou mises à jour, au besoin. Le CECM-GC diffusera également au besoin des mises à jour de la note d'information IN12-002 pour informer les ministères du GC des changements concernant l'horaire des attaques et des tendances dans les activités observées de déni de service distribué.

On vous recommande de mettre en œuvre les conseils d'atténuation énoncés dans les

cybercapsules susmentionnées et dans celles qui seront diffusées ultérieurement.

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 16:45
To: CTEC
Subject: Mise à jour no 11: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

==========
CECM-GC – Note d'information IN12-002
Date : 25 octobre 2012
==========

==========
Mise à jour no 11 : 4 novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de la campagne de déni de service distribué visant le GC planifiée par Anonymous. Cette compagne, regroupant #OpPartyCrasher et d'autres opérations connexes, est prévue du 3 au 15 novembre 2012.

ÉVALUATION
==========

Le 4 novembre, Le Droit a publié un article intitulé « Le gouvernement canadien menacé d'une cyberattaque » sur la page d'accueil de son site Web. L'article porte sur de l'information semblable à celle que l'on retrouve dans la note d'information IN12-002.

Plusieurs copies d'un nouveau script d'appoint ont été diffusées le 4 novembre, lesquelles ciblaient un site Web non gouvernemental. Il n'y a pas lieu de croire que les sites Web gc.ca sont perturbés.

Selon une source sûre, les tentatives de déni de service distribué pourraient se poursuivre jusqu'au 30 novembre.

En date de la présente publication, il n'y a pas lieu de croire que les sites Web gc.ca sont perturbés. Les scripts d'appoint diffusés le 4 novembre n'ont pas présenté de changements considérables.

Les 2 et 3 novembre, un ministère du GC a signalé une tentative de déni de service distribué 16(2)(c). Cette attaque a eu toutefois très peu, voire

aucune incidence sur le site Web.

Le 4 novembre, aucun ministère n'a signalé de tentative de déni de service distribué.

Anonymous a affiché un horaire des attaques sur pastebay[.]net (no 1151488) et a annoncé qu'il allait fournir une liste révisée des cibles et des scripts d'appoint une heure avant les heures d'attaque suivantes :

Samedi	3 novembre	De 12 h à 18 h
Dimanche	4 novembre	De 12 h à 18 h
Mardi	6 novembre	De 18 h à 22 h
Mercredi	7 novembre	De 18 h à 22 h
Jeudi	8 novembre	De 18 h à 22 h
Vendredi	9 novembre	De 18 h à 22 h

Ces heures pourraient changer, et il est impossible de les vérifier puisqu'il s'agit de la seule liste disponible.

Depuis le 25 octobre, un grand nombre de ministères ont signalé des activités comparables à des tentatives de déni de service distribué, mais on a pu établir aucun lien direct avec la campagne planifiée d'Anonymous. Le CECM-GC prévient les ministères que la portée et le niveau d'activité malveillante pourraient augmenter à mesure que les dates prévues de la campagne approchent, et que les techniques d'attaque pourraient varier de celles dont se sert habituellement Anonymous. Il convient toutefois de noter que les activités observées à ce jour n'ont eu aucune incidence majeure sur le GC.

Jusqu'ici, les activités pertinentes comprennent :

16(2)(c),21(1)(a),21(1)(b)

À mesure qu'il découvrira des activités malveillantes touchant le GC, le CECM-GC diffusera des cybercapsules contenant des conseils d'atténuation technique connexes.

Depuis la diffusion de la première note d'information IN12-002, le CECM-GC a publié les documents suivants :

- GCCF12-008 : « Campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre au

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-009 : « Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-010 : « Mesures d'atténuation pour la campagne visant les formulaires de sites Web du GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier.

Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

Des membres du personnel du CECM-GC et de SPC surveilleront la situation au cours de la fin de semaine, pendant les heures d'attaque annoncées, et fourniront des conseils généraux d'atténuation, dont de nouvelles cybercapsules ou mises à jour, au besoin. Le CECM-GC diffusera également au besoin des mises à jour de la note d'information IN12-002 pour informer les ministères du GC des changements concernant l'horaire des attaques et des tendances dans les activités observées de déni de service distribué.

On vous recommande de mettre en œuvre les conseils d'atténuation énoncés dans les cybercapsules susmentionnées et dans celles qui seront diffusées ultérieurement.

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs

préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Thursday, November 8, 2012 11:49
To: CTEC
Subject: Mise à jour no 12: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

English version previously sent.

==========
CECM-GC – Note d'information IN12-002
Date : 25 octobre 2012
==========

==========
Mise à jour no 12 : 5 novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de l'opération de déni de service distribué #OpPartyCrasher d'Anonymous qui a pour cible le GC.

ÉVALUATION
==========

Depuis le 2 novembre, de nombreux scripts d'appoint de déni de service distribué ont été affichés quotidiennement. Cependant, rien n'indique que les sites Web gc.ca ont été perturbés.

Anonymous a affiché un horaire des attaques sur pastebay[.]net (no 1151488) et a annoncé qu'il allait fournir une liste révisée des cibles et des scripts d'appoint une heure avant les heures d'attaque précisées suivantes :

Samedi	3 novembre	de 12 h à 18 h
Dimanche	4 novembre	de 12 h à 18 h

Lundi	5 novembre	Jour de Guy Fawkes, aucune activité prévue
Mardi	6 novembre	de 18 h à 22 h
Mercredi	7 novembre	de 18 h à 22 h
Jeudi	8 novembre	de 18 h à 22 h
Vendredi	9 novembre	de 18 h à 22 h

Ces heures peuvent faire l'objet de modifications et ne peuvent être confirmées puisque cette liste est la seule disponible.
Depuis le 25 octobre, un grand nombre de ministères ont signalé des activités comparables à des tentatives de déni de service distribué, mais aucun lien direct n'a pu être établi avec la campagne planifiée d'Anonymous. Le CECM-GC prévient les ministères que la portée et le niveau d'activité malveillante pourraient augmenter d'ici la date de fin prévue de la campagne, et que les techniques d'attaque pourraient varier de celles dont se sert habituellement Anonymous. Il convient toutefois de noter que les activités observées à ce jour n'ont eu aucune incidence majeure sur le GC.

Jusqu'ici, les activités pertinentes comprennent :

16(2)(c),21(1)(a),21(1)(b)

À mesure qu'il découvrira des activités malveillantes touchant le GC, le CECM-GC diffusera des cybercapsules contenant des conseils techniques d'atténuation connexes.

Depuis la diffusion de la première note d'information IN12-002, le CECMGC a publié les documents suivants :
- GCCF12-008 : « Campagne de déni de service distribué contre le GC ». Cette cybercapsule fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-009 : « Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC ». Cette cybercapsule fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-010 : « Mesures d'atténuation pour la campagne visant les formulaires de sites Web du GC ». Cette cybercapsule fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Les prochaines mises à jour seront présentées dans un nouveau format axé sur les événements actuels, le calendrier des événements et les prévisions d'événements futurs en lien avec la campagne de déni de service distribué d'Anonymous.

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

Des membres du personnel du CECM-GC et de SPC surveilleront la situation au cours de la fin de semaine, pendant les heures d'attaque annoncées, et fourniront des conseils généraux d'atténuation au besoin, dont de nouvelles cybercapsules ou des mises à jour de cybercapsules. Le CECM-GC diffusera également au besoin des mises à jour de la note

d'information IN12-002 pour informer les ministères du GC des changements concernant l'horaire des attaques et des tendances dans les activités observées de déni de service distribué.

On vous recommande de mettre en œuvre les conseils d'atténuation énoncés dans les cybercapsules susmentionnées et dans celles qui seront diffusées ultérieurement.

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :

- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@csecst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 16:58
To: CTEC
Subject: Mise à jour no 13: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

English version previously sent.

==========

CECM-GC - Note d'information IN12-002
Date : 6 novembre 2012
==========

AVIS :
Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

==========
Mise à jour n° 13 : 6 novembre 2012
- Remaniement de la section sur l'évaluation
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous - Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de l'opération de déni de service distribué #OpPartyCrasher d'Anonymous, laquelle a pour cible le GC.

ÉVALUATION
==========

Selon les tendances actuelles, les scripts d'appoint pour l'outil HOIC sont affichés une heure avant une attaque prévue.

3 novembre
Cible prévue : Parti conservateur du Canada
Cible du script d'appoint : victoews.com
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant quatre heures. Des utilisateurs ont indiqué que des pages d'erreur se sont affichées pendant une brève période.

Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

4 novembre
Cible prévue : Site Web du premier ministre du Canada
Cible du script d'appoint : jimflaheretymp.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant trois heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

5 novembre
Cible prévue : Jour de Guy Fawkes, aucune activité prévue
Cible du script d'appoint : Surrey.ca
Répercussions sur la cible : Anonymous prétend que le site Web était en panne pendant deux heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

6 novembre
Cible prévue : Conservateurs du Québec
Cible du script d'appoint : petermackay.ca
Répercussions sur la cible : Aucune répercussion pour l'instant
Répercussions sur le GC : Aucune répercussion pour l'instant

7 novembre
Cible prévue : Conservateurs de l'Ontario

8 novembre
Cible prévue : Conservateurs de l'Île-du-Prince-Édouard

9 novembre
Cible prévue : Conservateurs de la Nouvelle-Écosse

10 novembre
Cible prévue : Conservateurs du Nouveau-Brunswick

11 novembre
Cible prévue : Jour du Souvenir, aucune activité prévue

12 novembre
Cible prévue : Conservateurs de Terre-Neuve-et-Labrador

13 novembre
Cible prévue : Conservateurs du Manitoba

14 novembre

Cible prévue : Conservateurs de l'Alberta

15 novembre
Cible prévue : Conservateurs de la Colombie-Britannique

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

On vous recommande de continuer à mettre en œuvre les mesures d'atténuation énoncées dans les cybercapsules.

Si votre ministère est aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :

- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@csecst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux

cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avantgarde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Thursday, November 8, 2012 11:52
To: CTEC
Subject: Mise à jour no 14: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

English version sent previously.

==========
CECM-GC - Note d'information IN12-002
Date : 7 novembre 2012
==========

AVIS :
Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

==========
Mise à jour n° 14 : 7 novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous - Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de l'opération de déni de service distribué #OpPartyCrasher d'Anonymous qui a pour cible le GC.

ÉVALUATION
==========

Selon les tendances actuelles, les scripts d'appoint pour l'outil HOIC sont

affichés une heure avant une attaque prévue.

3 novembre
Cible prévue : Parti conservateur du Canada
Cible du script d'appoint : victoews.com
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant quatre heures. Des utilisateurs ont indiqué que des pages d'erreur se sont affichées pendant une courte période.

Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

4 novembre
Cible prévue : Site Web du premier ministre du Canada
Cible du script d'appoint : jimflaheretymp.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant trois heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

5 novembre
Cible prévue : Jour de Guy Fawkes, aucune activité prévue
Cible du script d'appoint : Surrey.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant deux heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

6 novembre
Cible prévue : Conservateurs du Québec
Cible du script d'appoint : petermackay.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant sept heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

7 novembre
Cible prévue : Conservateurs de l'Ontario
Cible du script d'appoint : blakerichards.ca
Répercussions sur la cible : Aucune répercussion signalée.
Répercussions sur le GC : Aucune répercussion pour l'instant.

8 novembre
Cible prévue : Conservateurs de l'Île-du-Prince-Édouard

9 novembre
Cible prévue : Conservateurs de la Nouvelle-Écosse

10 novembre
Cible prévue : Conservateurs du Nouveau-Brunswick

11 novembre
Cible prévue : Jour du Souvenir, aucune activité prévue

12 novembre
Cible prévue : Conservateurs de Terre-Neuve-et-Labrador

13 novembre
Cible prévue : Conservateurs du Manitoba

14 novembre
Cible prévue : Conservateurs de l'Alberta

15 novembre
Cible prévue : Conservateurs de la Colombie-Britannique

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

On vous recommande de continuer à mettre en œuvre les mesures d'atténuation énoncées dans les cybercapsules.

Si votre ministère est aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :

- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@csecst.gc.ca.

==========

Note aux lecteurs

==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, November 9, 2012 12:21
To: CTEC
Subject: Mise à jour no 15: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

==========
CECM-GC – Note d'information IN12-002
Date : 8 novembre 2012
==========

AVIS :
Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

==========
Mise à jour no 15 : 8 novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de l'opération de déni de service distribué #OpPartyCrasher d'Anonymous qui a pour cible le GC.

ÉVALUATION
==========

Selon les tendances actuelles, les scripts d'appoint pour l'outil HOIC sont affichés une heure avant une attaque prévue.

3 novembre
Cible prévue : Parti conservateur du Canada
Cible du script d'appoint : victoews.com
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant quatre heures. Des utilisateurs ont indiqué que des pages d'erreur se sont affichées pendant une courte période.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

4 novembre
Cible prévue : Site Web du premier ministre du Canada
Cible du script d'appoint : jimflaheretymp.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant trois heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

5 novembre
Cible prévue : Jour de Guy Fawkes, aucune activité prévue
Cible du script d'appoint : Surrey.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant deux heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

6 novembre
Cible prévue : Conservateurs du Québec
Cible du script d'appoint : petermackay.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant sept heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

7 novembre
Cible prévue : Conservateurs de l'Ontario
Cible du script d'appoint : blakerichards.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant cinq heures.
Répercussions sur le GC : Le CECM-GC a observé des activités de déni de service distribué dans 18 ministères, mais un seul ministère a été victime d'une panne mineure. Des analyses sont en cours afin de déterminer si ces activités sont liées à la campagne actuelle d'Anonymous.

8 novembre
Cible prévue : Conservateurs de l'Île-du-Prince-Édouard
Cible du script d'appoint : www.pm.gc.ca
Répercussions sur la cible : Aucune répercussion pour l'instant.
Répercussions sur le GC : Aucune répercussion pour l'instant.

9 novembre
Cible prévue : Conservateurs de la Nouvelle-Écosse

10 novembre
Cible prévue : Conservateurs du Nouveau-Brunswick

11 novembre
Cible prévue : Jour du Souvenir, aucune activité prévue

12 novembre
Cible prévue : Conservateurs de Terre-Neuve-et-Labrador

13 novembre
Cible prévue : Conservateurs du Manitoba

14 novembre
Cible prévue : Conservateurs de l'Alberta

15 novembre
Cible prévue : Conservateurs de la Colombie-Britannique

MESURES RECOMMANDÉES

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier.

Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

On vous recommande de continuer à mettre en œuvre les mesures d'atténuation énoncées dans les cybercapsules.

Si votre ministère est aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse cst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Tuesday, November 13, 2012 11:37
To: CTEC
Subject: Mise à jour no 16: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

==========
CECM-GC – Note d'information IN12-002
Date : 9 novembre 2012
==========

AVIS :
Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

Aucune mise à jour de la présente note d'information ne sera diffusée pendant la longue fin de semaine du 10 au 12 novembre, à moins que des événements ne l'exigent.

==========
Mise à jour no 16 : 9 novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de l'opération de déni de service distribué #OpPartyCrasher d'Anonymous qui a pour cible le GC.

ÉVALUATION
==========

Selon les tendances actuelles, les scripts d'appoint pour l'outil HOIC sont affichés une heure avant une attaque prévue.

3 novembre
Cible prévue : Parti conservateur du Canada
Cible du script d'appoint : victoews.com
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant quatre heures. Des utilisateurs ont indiqué que des pages d'erreur se sont affichées

pendant une courte période.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

4 novembre
Cible prévue : Site Web du premier ministre du Canada
Cible du script d'appoint : jimflaheretymp.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant trois heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

5 novembre
Cible prévue : Jour de Guy Fawkes, aucune activité prévue
Cible du script d'appoint : Surrey.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant deux heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

6 novembre
Cible prévue : Conservateurs du Québec
Cible du script d'appoint : petermackay.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant sept heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

7 novembre
Cible prévue : Conservateurs de l'Ontario
Cible du script d'appoint : blakerichards.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant cinq heures.
Répercussions sur le GC : Le CECM-GC a observé des activités de déni de service distribué dans 18 ministères, mais un seul ministère a été victime d'une panne mineure. Des analyses sont en cours afin de déterminer si ces activités sont liées à la campagne actuelle d'Anonymous.

8 novembre
Cible prévue : Conservateurs de l'Île-du-Prince-Édouard
Cible du script d'appoint : www.pm.gc.ca
Répercussions sur la cible : Anonymous affirme que la version anglaise du site Web www.pm.gc.ca était en panne pendant 2 heures et que la version française était en panne pendant 3 heures.
Répercussions sur le GC : Des activités de déni de service distribué ont été détectées, mais aucune panne n'a été observée ou signalée.

9 novembre
Cible prévue : Conservateurs de la Nouvelle-Écosse
Cible du script d'appoint : www.conservative.ca
Répercussions sur la cible : Anonymous aurait affiché des micromessages (tweets) contenant des liens conçus en vue d'exploiter une faille mineure du site Web www.conservative.ca. Bien que ce site n'ait été compromis d'aucune façon, les personnes y accédant à l'aide des liens conçus verront ce qui semble être une version modifiée du site Web.
Répercussions sur le GC : Aucune répercussion pour l'instant.

10 novembre
Cible prévue : Conservateurs du Nouveau-Brunswick

11 novembre
Cible prévue : Jour du Souvenir, aucune activité prévue

12 novembre
Cible prévue : Conservateurs de Terre-Neuve-et-Labrador

13 novembre

Cible prévue : Conservateurs du Manitoba

14 novembre
Cible prévue : Conservateurs de l'Alberta

15 novembre
Cible prévue : Conservateurs de la Colombie-Britannique

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c).

On vous recommande de continuer à mettre en œuvre les mesures d'atténuation énoncées dans les cybercapsules.

Si votre ministère est aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse cst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 14, 2012 11:50
To: CTEC
Subject: Mise à jour no 17: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

English sent previously.

==========
CECM-GC – Note d'information IN12-002
Date : 13 novembre 2012
==========

AVIS :
Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

==========
Mise à jour no 17 : 13 novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de l'opération de déni de service distribué #OpPartyCrasher d'Anonymous qui a pour cible le GC.

ÉVALUATION
==========

Selon les tendances actuelles, les scripts d'appoint pour l'outil HOIC sont affichés une heure avant une attaque prévue.

Le calendrier suivant est fondé sur celui qu'Anonymous a affiché à l'origine. Anonymous semble y avoir dévié quelque peu au cours de la campagne et devrait s'y écartera davantage puisqu'il a déclaré qu'il allait détourner son attention des systèmes du GC.

3 novembre

Cible prévue : Parti conservateur du Canada
Cible du script d'appoint : victoews.com
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant quatre heures. Des utilisateurs ont indiqué que des pages d'erreur se sont affichées pendant une courte période.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

4 novembre
Cible prévue : Site Web du premier ministre du Canada
Cible du script d'appoint : jimflaheretymp.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant trois heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

5 novembre
Cible prévue : Jour de Guy Fawkes, aucune activité prévue
Cible du script d'appoint : Surrey.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant deux heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

6 novembre
Cible prévue : Conservateurs du Québec
Cible du script d'appoint : petermackay.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant sept heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

7 novembre
Cible prévue : Conservateurs de l'Ontario
Cible du script d'appoint : blakerichards.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant cinq heures.
Répercussions sur le GC : Le CECM-GC a observé des activités de déni de service distribué dans 18 ministères, mais un seul ministère a été victime d'une panne mineure. Des analyses sont en cours afin de déterminer si ces activités sont liées à la campagne actuelle d'Anonymous.

8 novembre
Cible prévue : Conservateurs de l'Île-du-Prince-Édouard
Cible du script d'appoint : www.pm.gc.ca
Répercussions sur la cible : Anonymous affirme que la version anglaise du site Web www.pm.gc.ca était en panne pendant 2 heures et que la version française était en panne pendant 3 heures.
Répercussions sur le GC : Des activités de déni de service distribué ont été détectées, mais aucune panne n'a été observée ou signalée.

9 novembre
Cible prévue : Conservateurs de la Nouvelle-Écosse
Cible du script d'appoint : www.conservative.ca
Répercussions sur la cible : Anonymous aurait affiché des micromessages (tweets) contenant des liens conçus en vue d'exploiter une faille mineure du site Web www.conservative.ca. Bien que ce site n'ait été compromis d'aucune façon, les personnes y accédant à l'aide des liens conçus verront ce qui semble être une version modifiée du site Web.
Répercussions sur le GC : Aucune répercussion pour l'instant.

10 novembre
Cible prévue : Conservateurs du Nouveau-Brunswick
Cible du script d'appoint : Aucun
Répercussions sur la cible : Aucune

Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

11 novembre
Cible prévue : Jour du Souvenir, aucune activité prévue
Cible du script d'appoint : Aucun
Répercussions sur la cible : Aucune
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

12 novembre
Cible prévue : Conservateurs de Terre-Neuve-et-Labrador
Cible du script d'appoint : Aucun
Répercussions sur la cible : Aucune
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

13 novembre
Cible prévue : Conservateurs du Manitoba
Cible du script d'appoint : Aucun
Répercussions sur la cible : Aucune
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

14 novembre
Cible prévue : Conservateurs de l'Alberta

15 novembre
Cible prévue : Conservateurs de la Colombie-Britannique

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c).

On vous recommande de continuer à mettre en œuvre les mesures d'atténuation énoncées dans les cybercapsules.

Si votre ministère est aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse cst.gc.ca.

==========

contrôle sont fournis aux utilisateurs pour des raisons de commodité seulement. Le GC n'est pas responsable de l'exactitude, de l'actualité ni de la fiabilité du contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites ou leur contenu.

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 14, 2012 15:11
To: CTEC
Subject: Mise à jour no 18: CECM-GC – Note d'information IN12-002: Anonymous – Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

English version sent previously.

==========
CECM-GC – Note d'information IN12-002
Date : 14 novembre 2012
==========

==========
Mise à jour no 18 : 14 novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de l'opération de déni de service distribué #OpPartyCrasher d'Anonymous qui a pour cible le GC.

ÉVALUATION
==========

Selon les tendances actuelles, les scripts d'appoint pour l'outil HOIC sont affichés une heure avant une attaque prévue.

Le calendrier suivant est fondé sur celui qu'Anonymous a affiché à l'origine. Anonymous semble y avoir dévié quelque peu au cours de la campagne et devrait s'y écartera davantage puisqu'il a déclaré qu'il allait détourner son attention des systèmes du GC.

3 novembre
Cible prévue : Parti conservateur du Canada
Cible du script d'appoint : victoews.com
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant quatre heures. Des utilisateurs ont indiqué que des pages d'erreur se sont affichées pendant une courte période.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

4 novembre
Cible prévue : Site Web du premier ministre du Canada
Cible du script d'appoint : jimflaheretymp.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant trois heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

5 novembre
Cible prévue : Jour de Guy Fawkes, aucune activité prévue
Cible du script d'appoint : Surrey.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant deux heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

6 novembre
Cible prévue : Conservateurs du Québec
Cible du script d'appoint : petermackay.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant sept heures.
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

7 novembre
Cible prévue : Conservateurs de l'Ontario
Cible du script d'appoint : blakerichards.ca
Répercussions sur la cible : Anonymous affirme que le site Web était en panne pendant cinq heures.
Répercussions sur le GC : Le CECM-GC a observé des activités de déni de service distribué dans 18 ministères, mais un seul ministère a été victime d'une panne mineure. Des analyses sont en cours afin de déterminer si ces activités sont liées à la campagne actuelle d'Anonymous.

8 novembre
Cible prévue : Conservateurs de l'Île-du-Prince-Édouard
Cible du script d'appoint : www.pm.gc.ca
Répercussions sur la cible : Anonymous affirme que la version anglaise du site Web www.pm.gc.ca était en panne pendant 2 heures et que la version française était en panne pendant 3 heures.
Répercussions sur le GC : Des activités de déni de service distribué ont été détectées, mais aucune panne n'a été observée ou signalée.

9 novembre
Cible prévue : Conservateurs de la Nouvelle-Écosse
Cible du script d'appoint : www.conservative.ca
Répercussions sur la cible : Anonymous aurait affiché des micromessages (tweets) contenant des liens conçus en vue d'exploiter une faille mineure du site Web www.conservative.ca. Bien que ce site n'ait été compromis d'aucune façon, les personnes y accédant à l'aide des liens conçus verront ce qui semble être une version modifiée du site Web.
Répercussions sur le GC : Aucune répercussion pour l'instant.

10 novembre
Cible prévue : Conservateurs du Nouveau-Brunswick
Cible du script d'appoint : Aucun
Répercussions sur la cible : Aucune
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

11 novembre
Cible prévue : Jour du Souvenir, aucune activité prévue
Cible du script d'appoint : Aucun
Répercussions sur la cible : Aucune
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

12 novembre
Cible prévue : Conservateurs de Terre-Neuve-et-Labrador
Cible du script d'appoint : Aucun
Répercussions sur la cible : Aucune
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

13 novembre
Cible prévue : Conservateurs du Manitoba
Cible du script d'appoint : Aucun
Répercussions sur la cible : Aucune
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

14 novembre
Cible prévue : Conservateurs de l'Alberta
Cible du script d'appoint : Aucun
Répercussions sur la cible : Aucune
Répercussions sur le GC : Les ministères du GC n'ont signalé aucune répercussion.

15 novembre
Cible prévue : Conservateurs de la Colombie-Britannique

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c).

On vous recommande de continuer à mettre en œuvre les mesures d'atténuation énoncées dans les cybercapsules.

Si votre ministère est aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse cst.gc.ca.

==========

Le présent message et ses pièces jointes contiennent des renseignements pouvant provenir de sources externes et dont le CECM-GC ne peut pas vérifier l'exactitude ni l'intégrité. Le CECM-GC ne sera pas responsable des conséquences négatives résultant de l'utilisation de ces renseignements.

Les liens vers les sites Web sur lesquels le gouvernement du Canada n'exerce aucun contrôle sont fournis aux utilisateurs pour des raisons de commodité seulement. Le GC n'est pas responsable de l'exactitude, de l'actualité ni de la fiabilité du contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites ou leur contenu.

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, November 16, 2012 12:12
To: CTEC
Subject: Mise à jour no 19: CECM-GC - Note d'information IN12-002: Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

English version sent previously.

==========
CECM-GC - Note d'information IN12-002
Date : 15 novembre 2012
==========

AVIS :
Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

==========
Mise à jour no 19 : 15 novembre 2012
- Mise à jour de l'information sur l'évaluation et des mesures recommandées
==========

==========
Anonymous - Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de l'opération de déni de service distribué #OpPartyCrasher d'Anonymous qui a pour cible le GC.

ÉVALUATION
==========

Le 15 novembre 2012 marque la dernière journée de la campagne #OpPartyCrasher. La présente mise à jour résume les activités et les répercussions recensées au cours de la campagne.

Aujourd'hui, 16(2)(c) ministères ont signalé des activités mineures de déni de service distribué qui ne sont pas suffisamment importantes pour causer une détérioration des services.

Le CECM-GC a évalué les répercussions de la campagne sur les ministères du GC comme étant minimales : seulement deux pannes temporaires et très brèves ont été décelées. On ignore toutefois si ces pannes sont liées à la campagne d'Anonymous ou à d'autres activités en marge du calendrier de l'opération #OpPartyCrasher.

La campagne n'a pas réellement nui aux services du GC. Elle a surtout forcé le GC à mettre en place des ressources supplémentaires pour assurer la surveillance des réseaux.

En général, les ministères ont signalé les événements au CECM-GC et aux Opérations de SPC en temps opportun et ils ont fourni suffisamment d'information pour permettre de faire enquête et de mettre en place des mesures d'atténuation subséquentes.

MESURES RECOMMANDÉES
==========

Le CECM-GC a coordonné l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) a dirigé l'atténuation avec les fournisseurs de services.

On recommande aux ministères de s'assurer que leurs plans de continuité des activités sont à jour.

Si votre ministère est aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant garde et des conseils stratégiques, et en coordonnant l'intervention

fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Tuesday, June 12, 2012 14:40
To: IT Security
Cc: CTEC
Subject: RE: [CE2012-766]: Login Credentials Exposed in Online Posting

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED

Hello,

Recently, it was revealed that a hacking group had broken into the website www.intelconsumerelectronics.com and posted some stolen client data onto another public website known as Pastebin.com.

Your agency is being contacted because someone working there has had their email address posted on Pastebin. The following data was exposed:

19(1)

GC-CTEC recommends that the affected employee be notified and that the employee should exercise heightened caution when opening unrecognized or suspicious emails.

Should you require further information please contact us.

CTEC

15(1)
GC-CTEC Cyber Duty Officer

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 16:55
To: CTEC
Subject: Mise à jour no 1: CECM-GC - Cybercapsule GCCF12-009: Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC

Classification: UNCLASSIFIED

English version previously sent.

CECM-GC - Cybercapsule GCCF12-009
Date : 2 novembre 2012
==========

AVIS : Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

==========
Mise à jour no 1 : 5 novembre 2012
- Mise à jour de la section sur l'atténuation

16(2)(c)

==========

PUBLIC
======
Cette cybercapsule est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

TITRE
=====
Utilisation possible de l'outil HOIC dans le cadre de la campagne de déni de service distribué contre le GC

DÉTAILS
=======
Cette cybercapsule est liée à la note d'information IN12-002 intitulée « Anonymous – Attaque par déni de service distribué visant le GC » et à toutes les mises à jour connexes.

High Orbit Ion Cannon (HOIC) est un outil multifil de déni de service distribué basé sur Windows qui transmet des demandes HTTP. Anonymous est généralement l'auteur des attaques menées à l'aide de cet outil. Pour qu'il fonctionne de manière efficace, HOIC repose sur un script d'appoint (booster script) configurable qui est souvent affiché publiquement. Les utilisateurs peuvent exploiter le script d'appoint de façon à ce qu'il précise une liste de rotation d'adresses URL pour les requêtes HTTP, au moyen des méthodes de requête GET ou POST (données précisées par l'utilisateur). Ils peuvent également définir l'agent-utilisateur de manière aléatoire (en fonction d'une liste définie par l'utilisateur) et créer des en-têtes personnalisés (composés de chaînes définies par l'utilisateur, annexées dans l'ordre de leur choix). Les utilisateurs peuvent aussi régler le taux de requête (réglé par défaut à 2 fils).

ATTÉNUATION
==========

Atténuation réseau

16(2)(c),21(1)(a),21(1)(b)

Afin de réduire au minimum les répercussions de cet outil d'attaque sur les sites Web, le CECM-GC recommande aux administrateurs Web du GC de mettre en œuvre les mesures d'atténuation suivantes, dans la mesure du possible :

16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Bien que les noms et les données utiles des en-têtes de requête soient valides, l'ordre dans lequel les en-têtes sont définis dans la requête ne correspond pas à celui dans lequel les navigateurs Web normaux les enverraient. Voici la caractéristique la plus facile à remarquer : dans HOIC, l'en-tête de l'hôte apparaît toujours à la fin de la requête, mais ce n'est pas le cas pour les navigateurs Web légitimes.

16(2)(c),21(1)(a),21(1)(b)

Le trafic HOIC présente aussi la caractéristique suivante : les données utiles des en-têtes de requête contiennent souvent deux espaces en début de ligne. 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Atténuation tactique

En plus du trafic récurrent mentionné ci-dessus, 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Avertissement :
Le CECM-GC offre l'information et les conseils d'atténuation ci-dessus en fonction des menaces envers les réseaux du gouvernement du Canada et ne recommande pas que cette information soit utilisée à d'autres fins.

L'information contenue dans le présent message est fournie exclusivement aux fins de reconfiguration défensive des biens appartenant au destinataire.
Le destinataire ne doit en aucun cas participer à des activités de collecte d'information à l'extérieur de son propre périmètre réseau au moyen des renseignements contenus dans le présent document. Ces activités comprennent la vérification, le téléchargement, la navigation et le balayage des sites mentionnés dans le présent rapport.

SIGNALEMENT DES INCIDENTS
==========
Les ministères qui croient avoir été victimes d'un incident lié à l'activité décrite dans le présent document doivent soumettre un rapport écrit au CECM-GC. Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

AVIS : Le présent message et ses pièces jointes sont réservés à la personne ou à l'entité à qui ils ont été adressés. Il est strictement interdit à toute personne autre que le destinataire prévu de diffuser, de distribuer ou de copier leur contenu, ou de prendre des mesures sur la foi de ce contenu. Si vous avez reçu ce message par erreur, veuillez en aviser l'expéditeur à l'adresse indiquée ci-dessus et supprimer ce courriel.

Le présent message et ses pièces jointes contiennent des renseignements pouvant provenir de sources externes et dont le CECM-GC ne peut pas vérifier l'exactitude ni l'intégrité. Le CECM-GC ne sera pas responsable des conséquences négatives résultant de l'utilisation de ces renseignements.

Les liens vers les sites Web sur lesquels le gouvernement du Canada n'exerce aucun contrôle sont fournis aux utilisateurs pour des raisons de commodité seulement. Le GC n'est pas responsable de l'exactitude, de l'actualité ni de la fiabilité du contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites ou leur contenu.

NOTE AUX LECTEURS
==========
Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avantgarde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.
Pour signaler les incidents touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC par courriel à ctec@cse-cst.gc.ca ou par téléphone au 613-991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Monday, November 5, 2012 16:27
To: CTEC
Subject: Update 1: Cyber Flash GCCF12-009: Possible use of HOIC for DDoS campaign against the GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC-CTEC - Cyber Flash GCCF12-009
Date: 02 November 2012
==========

==========
Update 1: 05 November 2012
- Updated mitigation section

16(2)(c)

==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal government.

TITLE
=====
Possible use of HOIC for DDoS campaign against the GC

DETAILS
=======
This Cyber Flash is related to 'Information Note IN12-002: Anonymous DDoS activity against GC' and all updates.

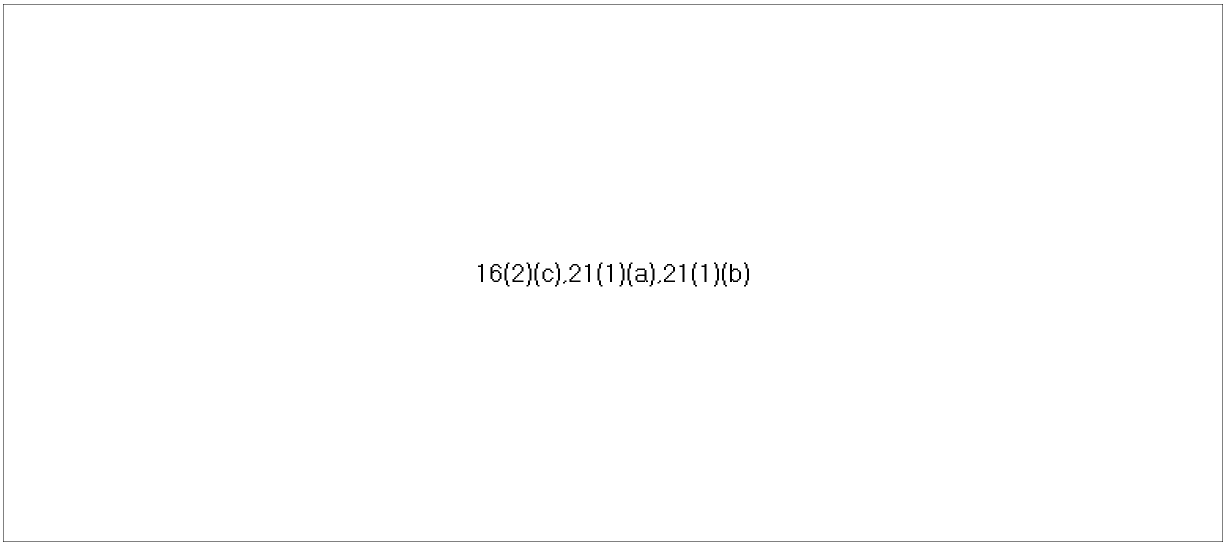
The High Orbit Ion Cannon (HOIC) is a Windows-based DDoS tool characteristically attributed to Anonymous. HOIC is a multi-threaded DDoS tool that transmits HTTP requests. In order for it to work effectively, HOIC relies on a configurable "booster" script that is commonly posted publicly. Users may leverage the booster script to specify a list of rotating URLs for HTTP requests, using either the GET or POST (user-specified data) request methods. Users may also randomize the user-agent (based on a user-defined list) and create custom headers (composed of user-defined strings, appended in the order of their choice). The request rate can also be set (default is 2 threads).

MITIGATION
==========

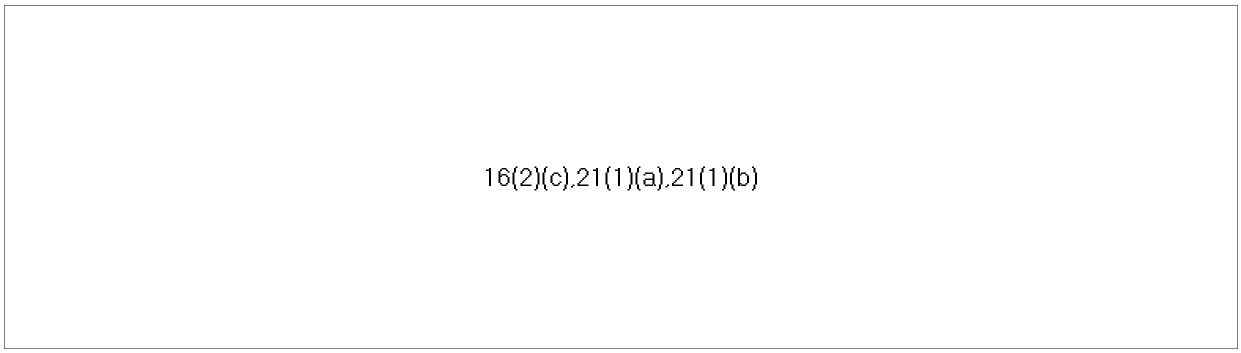
Network-based mitigation

In order to help minimize the effect of this attack tool on websites, GC website administrators are advised to take the following mitigative actions where practical:

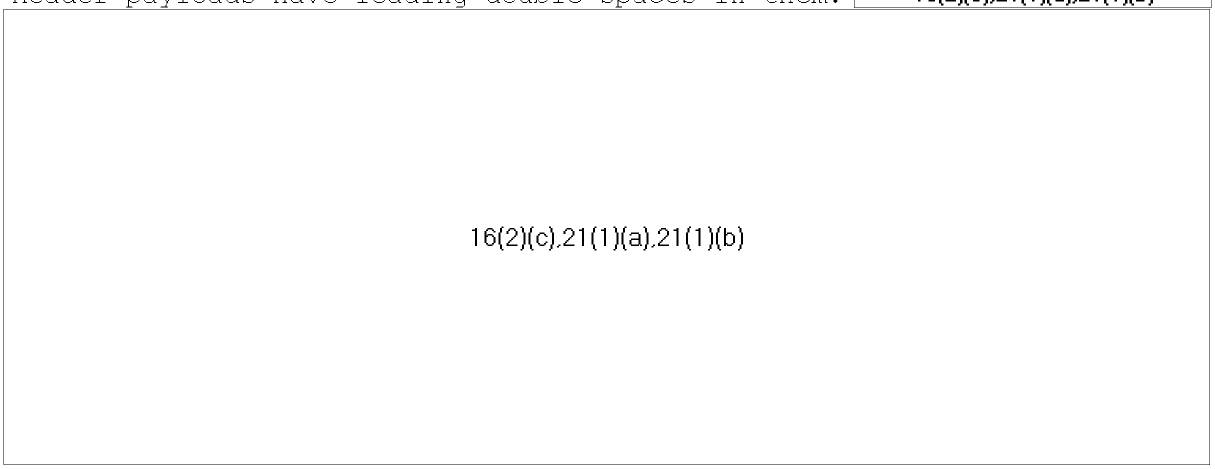
16(2)(c),21(1)(a),21(1)(b)



While the request header names and payloads are valid, the order in which they are defined in the request do not match what normal web browsers would send. The easiest characteristic to notice is that, in HOIC, the Host header is always listed last in the header order while this is not the case in any legitimate browsers.

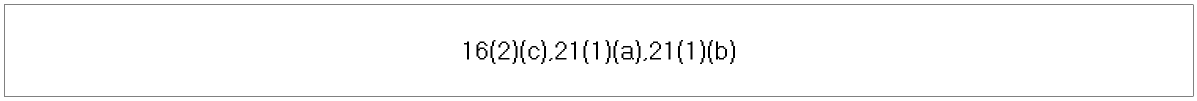


Another characteristic of HOIC traffic is that many of the Request Header payloads have leading double-spaces in them. 16(2)(c),21(1)(a),21(1)(b)



Tactical mitigation

In addition to the traffic patterns that may be observed above,



Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.
The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

REPORTING
=========
Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC. To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

NOTE TO READERS
===============
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.
To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca or (613)991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Monday, October 29, 2012 16:28
To: CTEC
Subject: Update 5: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 29 October 2012
==========

==========
Update 5: 29 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

As of 29 October, activity related to this Information Note appears to be dimishing significantly compared to the previous Update. This activity is still believed to be related to the Anonymous operation #OpPartyCrasher and related operations, which is scheduled to occur from 3 to 15 November 2012. At this stage 21(1)(b)
21(1)(b)

The remaining activity is still consistent with this Information Note Update

16(2)(c),21(1)(a),21(1)(b)

The drop-off in activity is not indicative that the operation has completed.

Caution is recommended as the decrease in activity may be temporary.

GC-CTEC advises that the scope and level of activity may fluctuate between now and the targeted date range specified, and that it may not follow typical Anonymous techniques.

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:

- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring

threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Tuesday, October 30, 2012 17:29
To: CTEC
Subject: Update 6: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 30 October 2012
==========

==========
Update 6: 30 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

As of 30 October 2012, activity related to this Information Note still appears to be diminished compared to the levels reported 25 to 28 October 2012. This activity is still believed to be linked to the Anonymous operation #OpPartyCrasher and related operations, which are scheduled to occur from 3 to 15 November 2012. At this stage 21(1)(b)

21(1)(b)

The remaining activity is still consistent with previous updates. Some observed activity

16(2)(c),21(1)(a),21(1)(b)

GC-CTEC has released "GCCF12-008: DDoS campaign against the GC" that provides mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

GC-CTEC advises that the scope and level of activity may fluctuate between now and the targeted date range specified, and that it may not follow typical Anonymous techniques.

SUGGESTED ACTION

==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

Departments should implement the mitigation advice in GCCF12-008: DDoS campaign against the GC.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, October 31, 2012 16:02
To: CTEC
Subject: Update 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 31 October 2012
==========

==========
Update 7: 31 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC . The operation, #OpPartyCrasher and related operations, is scheduled to occur from 3 to 15 November 2012.

Since 25 October 2012, there have been multiple departments reporting activity consistent with DDOS attempts, however no direct link has been made with the planned Anonymous campaign. GC-CTEC advises that the scope and level of malicious activity may fluctuate between now and the targeted date range specified, and that it may not follow typical Anonymous techniques.

To date observed DDOS activities include:

16(2)(c)

As GC-CTEC identifies mitigation actions a Cyber Flash product will be disseminated to provide the technical mitigation advice.

To date GC-CTEC has released:
- GCCF12-008: DDoS campaign against the GC - which provided mitigation recommendations that can be implemented 16(2)(c).21(1)(a).21(1)(b)
16(2)(c).21(1)(a).21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

Departments should implement the mitigation advice in GCCF12-008: DDoS campaign against the GC.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, November 2, 2012 16:37
To: CTEC
Subject: Update 9: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 2 November 2012
==========

==========
Update 9: 2 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC . The operation, #OpPartyCrasher and related operations, is scheduled to occur from 3 to 15 November 2012.

ASSESSMENT
==========

Anonymous has posted a schedule of attacks on pastebay[.]net (paste 1151488) and has announced that they will provide a revised list of targets and boosters one hour before the designated attack times. The listed times are as follows:

```
Saturday        November 3      12:00-18:00
Sunday  November 4      12:00-18:00
Tuesday November 6      18:00-22:00
Wednesday       November 7      18:00-22:00
Thursday        November 8      18:00-22:00
Friday  November 9      18:00-22:00
```

These times may be subject to change and cannot be verified as the only list that exists.

Since 25 October 2012, there have been multiple departments reporting activity consistent with DDOS attempts, however no direct link has been made with the planned Anonymous campaign. GC-CTEC advises that the scope and level of malicious activity may fluctuate between now and the targeted date range specified, and that it may not follow typical Anonymous techniques. There has been no major impact on the GC by any of the observed activity to date.

To date, observed DDOS-related activities include:

16(2)(c),21(1)(a),21(1)(b)

As GC-CTEC identifies malicious activity impacting the GC, Cyber Flash products will be disseminated to provide the associated technical mitigation advice.

Since IN12-002 was first issued, GC-CTEC has released:

- GCCF12-008: DDoS campaign against the GC - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-009: Possible use of HOIC for DDoS campaign against the GC - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-010: Mitigation for campaign against GC Website forms - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

GC-CTEC and SSC will have staff in place this weekend, during the announced attack times, monitoring the situation and providing general mitigation advice including new or updated Cyber Flashes as required. Information note updates will be released as required in order to inform the GC of any changes of attack schedule as well as any trending in DDoS activity observed.

Departments should implement the mitigation advice in above listed Cyber Flashes as well as any other Cyber Flashes that are released.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen

the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Saturday, November 3, 2012 16:17
To: CTEC
Subject: Update 10: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 10: 3 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC. The operation, #OpPartyCrasher and related operations, is scheduled to occur from 3 to 15 November 2012.

ASSESSMENT
==========

As of the time of this release, there is no evidence of disruption to gc.ca departments. Booster scripts released on November 3 did not exhibit any significant change.

On November 2 and November 3, one GC department reported a DDoS attempt - targeting a 16(2)(c) This resulted in little or no effect on the site.

Anonymous has posted a schedule of attacks on pastebay[.]net (paste 1151488) and has announced that they will provide a revised list of targets and boosters one hour before the designated attack times. The listed times are as follows:

Saturday	November 3	12:00-18:00
Sunday	November 4	12:00-18:00
Tuesday	November 6	18:00-22:00
Wednesday	November 7	18:00-22:00
Thursday	November 8	18:00-22:00

Friday November 9 18:00-22:00

These times may be subject to change and cannot be verified as the only list that exists.

Since 25 October 2012, there have been multiple departments reporting activity consistent with DDOS attempts, however no direct link has been made with the planned Anonymous campaign. GC-CTEC advises that the scope and level of malicious activity may fluctuate between now and the targeted date range specified, and that it may not follow typical Anonymous techniques. There has been no major impact on the GC by any of the observed activity to date.

To date, observed DDOS-related activities include:

16(2)(c),21(1)(a),21(1)(b)

As GC-CTEC identifies malicious activity impacting the GC, Cyber Flash products will be disseminated to provide the associated technical mitigation advice.

Since IN12-002 was first issued, GC-CTEC has released:
- GCCF12-008: DDoS campaign against the GC - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-009: Possible use of HOIC for DDoS campaign against the GC - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-010: Mitigation for campaign against GC Website forms - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

GC-CTEC and SSC will have staff in place this weekend, during the announced attack times, monitoring the situation and providing general mitigation advice including new or updated Cyber Flashes as required. Information note updates will be released as required in order to inform the GC of any changes of attack schedule as well as any trending in DDoS activity observed.

Departments should implement the mitigation advice in above listed Cyber Flashes as well as any other Cyber Flashes that are released.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires

further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here:
http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf
and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Sunday, November 4, 2012 15:27
To: CTEC
Subject: Update 11: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 11: 4 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC. The operation, #OpPartyCrasher and related operations, is scheduled to occur from 3 to 15 November 2012.

ASSESSMENT
==========

Le Droit published (November 4), on its website's main page, an article entitled "The Canadian government threatened cyber attack". The article discusses information similar to what was disclosed in the IN12-002.

Multiple copies of a new booster script was released November 4, targeting a non-GC website. There is no evidence of disruption to gc.ca departments.

A trusted source has indicated that the DDoS attempts may continue until November 30.

As of the time of this release, there is no evidence of disruption to gc.ca departments. Booster scripts released on November 4 did not exhibit any significant change.

On November 2 and November 3, one GC department reported a DDoS attempt - targeting a 16(2)(c) This resulted in little or no effect on the site.

On November 4, there were no reports of any DDoS attempts.

Anonymous has posted a schedule of attacks on pastebay[.]net (paste 1151488) and has announced that they will provide a revised list of targets and boosters one hour before the designated attack times. The listed times are as follows:

Saturday	November 3	12:00-18:00
Sunday	November 4	12:00-18:00
Tuesday	November 6	18:00-22:00
Wednesday	November 7	18:00-22:00
Thursday	November 8	18:00-22:00
Friday	November 9	18:00-22:00

These times may be subject to change and cannot be verified as the only list that exists.

Since 25 October 2012, there have been multiple departments reporting activity consistent with DDOS attempts, however no direct link has been made with the planned Anonymous campaign. GC-CTEC advises that the scope and level of malicious activity may fluctuate between now and the targeted date range specified, and that it may not follow typical Anonymous techniques. There has been no major impact on the GC by any of the observed activity to date.

To date, observed DDOS-related activities include:

16(2)(c),21(1)(a),21(1)(b)

As GC-CTEC identifies malicious activity impacting the GC, Cyber Flash products will be disseminated to provide the associated technical mitigation advice.

Since IN12-002 was first issued, GC-CTEC has released:

- GCCF12-008: DDoS campaign against the GC - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-009: Possible use of HOIC for DDoS campaign against the GC - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-010: Mitigation for campaign against GC Website forms - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

GC-CTEC and SSC will have staff in place this weekend, during the announced attack times, monitoring the situation and providing general mitigation advice including new or updated Cyber Flashes as required. Information note updates will be released as required in order to inform the GC of any changes of attack schedule as well as any trending in

DDoS activity observed.

Departments should implement the mitigation advice in above listed Cyber Flashes as well as any other Cyber Flashes that are released.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here:
http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf
and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Monday, November 5, 2012 17:53
To: CTEC
Subject: Update 12: Information Note IN12-002: Anonymous DDoS activity against GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

==========
Update 12: 5 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Since November 2, numerous DDoS booster scripts have been posted daily, however, there has been no evidence of disruption to gc.ca departments, to date.

Anonymous has posted a schedule of attacks on pastebay[.]net (paste 1151488) and has announced that they will provide a revised list of

targets and boosters one hour before the designated attack times. The listed times are as follows:

Saturday	November 3	12:00-18:00
Sunday	November 4	12:00-18:00
Monday	November 5	Guy Fawkes Day - nothing scheduled
Tuesday	November 6	18:00-22:00
Wednesday	November 7	18:00-22:00
Thursday	November 8	18:00-22:00
Friday	November 9	18:00-22:00

These times may be subject to change and cannot be verified as the only list that exists.

Since 25 October 2012, there have been multiple departments reporting activity consistent with DDoS attempts, however no direct link has been made with the planned Anonymous campaign. GC-CTEC advises that the scope and level of malicious activity may fluctuate between now and the targeted date range specified, and that it may not follow typical Anonymous techniques. There has been no major impact on the GC by any of the observed activity to date.

To date, observed DDoS-related activities include:

16(2)(c),21(1)(a),21(1)(b)

Since IN12-002 was first issued, GC-CTEC has released:
- GCCF12-008: DDoS campaign against the GC - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-009: Possible use of HOIC for DDoS campaign against the GC - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

- GCCF12-010: Mitigation for campaign against GC Website forms - which provided mitigation recommendations that can be implemented 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Future updates will follow a new format aimed at documenting current events, timelines, and forecasting of future events specific to the Anonymous DDoS campaign.

SUGGESTED ACTION

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

GC-CTEC and SSC will have staff in place this weekend, during the announced attack times, monitoring the situation and providing general

mitigation advice including new or updated Cyber Flashes as required. Information note updates will be released as required in order to inform the GC of any changes of attack schedule as well as any trending in DDoS activity observed.

Departments should implement the mitigation advice in above listed Cyber Flashes as well as any other Cyber Flashes that are released.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
 - SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
 - GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Tuesday, November 6, 2012 16:25
To: CTEC
Subject: Update 13: Information Note IN12-002: Anonymous DDoS activity against GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 6 November 2012
==========

==========
Update 13: 6 November 2012
- Restructured assessment section
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Current trends show that booster scripts for HOIC are posted 1 hour before a scheduled attack.

Nov. 3
Planned target: Conservative Party of Canada.
Booster target: victoews.com
Target impact: Anonymous claims the website was down for 4 hours.

Reports of error pages being presented for a short period of time.
 GC impact: No impact reported by GC departments.

Nov. 4
 Planned target: Prime Minister Of Canada website.
 Booster target: jimflaheretymp.ca
 Target impact: Anonymous claims the website was down for 3 hours.
 GC impact: No impact reported by GC departments.

Nov. 5
 Planned target: Guy Fawkes Day, nothing planned
 Booster target: Surrey.ca
 Target impact: Anonymous claims the website was down for 2 hours.
 GC impact: No impact reported by GC departments.

Nov. 6
 Planned target: Quebec Conservatives
 Booster target: petermackay.ca
 Target impact: None reported at time of update.
 GC impact: None reported at time of update.

Nov. 7
 Planned target: Ontario Conservatives

Nov. 8
 Planned target: PEI Conservatives

Nov. 9
 Planned target: Nova Scotia Conservatives

Nov. 10
 Planned target: New Brunswick Conservatives

Nov. 11
 Planned target: Remembrance Day, nothing planned

Nov. 12
 Planned target: Newfoundland and Labrador Conservatives

Nov. 13
 Planned target: Manitoba Conservatives

Nov. 14
 Planned target: Alberta Conservatives

Nov. 15
 Planned target: BC Conservatives

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider, 16(2)(c).

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
 - SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and

- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 16:39
To: CTEC
Subject: Update 14: Information Note IN12-002: Anonymous DDoS activity against GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 7 November 2012
==========

==========
Update 14: 7 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Current trends show that booster scripts for HOIC are posted 1 hour before a scheduled attack.

Nov. 3
Planned target: Conservative Party of Canada.
Booster target: victoews.com
Target impact: Anonymous claims the website was down for 4 hours.

Reports of error pages being presented for a short period of time.
 GC impact: No impact reported by GC departments.

Nov. 4
 Planned target: Prime Minister Of Canada website.
 Booster target: jimflaheretymp.ca
 Target impact: Anonymous claims the website was down for 3 hours.
 GC impact: No impact reported by GC departments.

Nov. 5
 Planned target: Guy Fawkes Day, nothing planned
 Booster target: Surrey.ca
 Target impact: Anonymous claims the website was down for 2 hours.
 GC impact: No impact reported by GC departments.

Nov. 6
 Planned target: Quebec Conservatives
 Booster target: petermackay.ca
 Target impact: Anonymous claims the website was down for 7 hours.
 GC impact: No impact reported by GC departments.

Nov. 7
 Planned target: Ontario Conservatives
 Booster target: blakerichards.ca
 Target impact: None reported.
 GC impact: None reported at time of update.

Nov. 8
 Planned target: PEI Conservatives

Nov. 9
 Planned target: Nova Scotia Conservatives

Nov. 10
 Planned target: New Brunswick Conservatives

Nov. 11
 Planned target: Remembrance Day, nothing planned

Nov. 12
 Planned target: Newfoundland and Labrador Conservatives

Nov. 13
 Planned target: Manitoba Conservatives

Nov. 14
 Planned target: Alberta Conservatives

Nov. 15
 Planned target: BC Conservatives

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider, 16(2)(c)

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
 - SSC Operations Duty Analyst 819-956-1006 or
RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
 - GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here:
http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Thursday, November 8, 2012 15:29
To: CTEC
Subject: Update 15: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 8 November 2012
==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

==========
Update 15: 8 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Current trends show that booster scripts for HOIC are posted 1 hour before a scheduled attack.

Nov. 3
Planned target: Conservative Party of Canada.

Booster target: victoews.com
Target impact: Anonymous claims the website was down for 4 hours. Reports of error pages being presented for a short period of time.
GC impact: No impact reported by GC departments.

Nov. 4
Planned target: Prime Minister Of Canada website.
Booster target: jimflahertymp.ca
Target impact: Anonymous claims the website was down for 3 hours.
GC impact: No impact reported by GC departments.

Nov. 5
Planned target: Guy Fawkes Day, nothing planned
Booster target: surrey.ca
Target impact: Anonymous claims the website was down for 2 hours.
GC impact: No impact reported by GC departments.

Nov. 6
Planned target: Quebec Conservatives
Booster target: petermackay.ca
Target impact: Anonymous claims the website was down for 7 hours.
GC impact: No impact reported by GC departments.

Nov. 7
Planned target: Ontario Conservatives
Booster target: blakerichards.ca
Target impact: Anonymous claims the website was down for 5 hours.
GC impact: Some DDoS activity was observed at 18 GC departments, resulting in a minor outage at one department. Analysis is on-going to determine if this is linked to the current Anonymous campaign.

Nov. 8
Planned target: PEI Conservatives
Booster target: www.pm.gc.ca
Target impact: None reported at time of update.
GC impact: None reported at time of update.

Nov. 9
Planned target: Nova Scotia Conservatives

Nov. 10
Planned target: New Brunswick Conservatives

Nov. 11
Planned target: Remembrance Day, nothing planned

Nov. 12
Planned target: Newfoundland and Labrador Conservatives

Nov. 13
Planned target: Manitoba Conservatives

Nov. 14
Planned target: Alberta Conservatives

Nov. 15
Planned target: BC Conservatives

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider, 16(2)(c).

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
 - SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
 - GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, November 9, 2012 15:32
To: CTEC
Subject: Update 16: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 9 November 2012
==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

Long Weekend updates, for November 10, 11 and 12, to this Information Note will not be issued unless required.

==========
Update 16: 9 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Current trends show that booster scripts for HOIC are posted 1 hour before a scheduled attack.

Nov. 3
Planned target: Conservative Party of Canada.

Booster target: victoews.com
Target impact: Anonymous claims the website was down for 4 hours. Reports of error pages being presented for a short period of time.
GC impact: No impact reported by GC departments.

Nov. 4
Planned target: Prime Minister Of Canada website.
Booster target: jimflahertymp.ca
Target impact: Anonymous claims the website was down for 3 hours.
GC impact: No impact reported by GC departments.

Nov. 5
Planned target: Guy Fawkes Day, nothing planned
Booster target: surrey.ca
Target impact: Anonymous claims the website was down for 2 hours.
GC impact: No impact reported by GC departments.

Nov. 6
Planned target: Quebec Conservatives
Booster target: petermackay.ca
Target impact: Anonymous claims the website was down for 7 hours.
GC impact: No impact reported by GC departments.

Nov. 7
Planned target: Ontario Conservatives
Booster target: blakerichards.ca
Target impact: Anonymous claims the website was down for 5 hours.
GC impact: Some DDoS activity was observed at 18 GC departments, resulting in a minor outage at one department. Analysis is on-going to determine if this is linked to the current Anonymous campaign.

Nov. 8
Planned target: PEI Conservatives
Booster target: www.pm.gc.ca
Target impact: Anonymous claims the english version of the website www.pm.gc.ca was down for 2 hours and the french version of the same website for 3 hours.
GC impact: Some DDoS activity was detected, but no outage was observed or reported.

Nov. 9
Planned target: Nova Scotia Conservatives
Booster target: www.conservative.ca
Target impact: Tweets containing crafted links that take advantage of a minor flaw in the www.conservative.ca website have been posted, purportedly by Anonymous. Although no compromise has taken place on the website, those visiting using these crafted links will see what appears to be a modified version of the website.
GC impact: None reported at time of update.

Nov. 10
Planned target: New Brunswick Conservatives

Nov. 11
Planned target: Remembrance Day, nothing planned

Nov. 12
Planned target: Newfoundland and Labrador Conservatives

Nov. 13
Planned target: Manitoba Conservatives

Nov. 14

Planned target: Alberta Conservatives

Nov. 15
Planned target: BC Conservatives

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider, 16(2)(c)

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 14, 2012 14:44
To: CTEC
Subject: Update 18: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 14 November 2012
==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

==========
Update 18: 14 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Current trends show that booster scripts for HOIC are posted 1 hour before a scheduled attack.

The below schedule is based on one originally posted by Anonymous. Some deviation from the schedule has been observed through the course of the campaign, and more is anticipated as Anonymous has stated they will be

directing their attention away from GC systems.

Nov. 3
 Planned target: Conservative Party of Canada.
 Booster target: victoews.com
 Target impact: Anonymous claims the website was down for 4 hours. Reports of error pages being presented for a short period of time.
 GC impact: No impact reported by GC departments.

Nov. 4
 Planned target: Prime Minister Of Canada website.
 Booster target: jimflahertymp.ca
 Target impact: Anonymous claims the website was down for 3 hours.
 GC impact: No impact reported by GC departments.

Nov. 5
 Planned target: Guy Fawkes Day, nothing planned
 Booster target: surrey.ca
 Target impact: Anonymous claims the website was down for 2 hours.
 GC impact: No impact reported by GC departments.

Nov. 6
 Planned target: Quebec Conservatives
 Booster target: petermackay.ca
 Target impact: Anonymous claims the website was down for 7 hours.
 GC impact: No impact reported by GC departments.

Nov. 7
 Planned target: Ontario Conservatives
 Booster target: blakerichards.ca
 Target impact: Anonymous claims the website was down for 5 hours.
 GC impact: Some DDoS activity was observed at 18 GC departments, resulting in a minor outage at one department. Analysis is on-going to determine if this is linked to the current Anonymous campaign.

Nov. 8
 Planned target: PEI Conservatives
 Booster target: www.pm.gc.ca
 Target impact: Anonymous claims the english version of the website www.pm.gc.ca was down for 2 hours and the french version of the same website for 3 hours.
 GC impact: Some DDoS activity was detected, but no outage was observed or reported.

Nov. 9
 Planned target: Nova Scotia Conservatives
 Booster target: www.conservative.ca
 Target impact: Tweets containing crafted links that take advantage of a minor flaw in the www.conservative.ca website have been posted, purportedly by Anonymous. Although no compromise has taken place on the website, those visiting using these crafted links will see what appears to be a modified version of the website.
 GC impact: No impact reported by GC departments.

Nov. 10
 Planned target: New Brunswick Conservatives
 Booster target: None
 Target impact: None
 GC impact: No impact reported by GC departments.

Nov. 11
 Planned target: Remembrance Day, nothing planned
 Booster target: None

Target impact: None
GC impact: No impact reported by GC departments.

Nov. 12
Planned target: Newfoundland and Labrador Conservatives
Booster target: None
Target impact: None
GC impact: No impact reported by GC departments.

Nov. 13
Planned target: Manitoba Conservatives
Booster target: None
Target impact: None
GC impact: No impact reported by GC departments.

Nov. 14
Planned target: Alberta Conservatives
Booster target: None
Target impact: None
GC impact: No impact reported by GC departments.

Nov. 15
Planned target: BC Conservatives

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider, 16(2)(c)

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Thursday, November 15, 2012 14:50
To: CTEC
Subject: Update 19: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC
Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 15 November 2012
==========

==========
Update 19: 15 November 2012
- Updated assessment information and suggested action
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

15 November 2012 is the last day of the published #OpPartyCrasher campaign.

This update summarizes the activities and impacts that occurred over the course of the campaign.

Minor amounts of DDoS activity were reported today 15(1),16(2)(c) but not at the levels required to cause any degradation in services.

Over the course of the campaign, impact to GC departments was assessed as minimal, with two reports of very short and temporary disruptions. It has not been confirmed if these outages are associated with the Anonymous campaign or with other activity outside of the #OpPartyCrasher schedule.

The main impact on the GC was the requirement for additional resources for monitoring, rather than a degradation in services.

The timeliness of reporting to GC CTEC and SSC Operations was generally fast and provided enough information for investigation and subsequent mitigation actions to take place.

SUGGESTED ACTION
==========

GC-CTEC coordinated the incident response and the threat evaluation for this event. Shared Services Canada led the mitigation effort with the service providers.

Departments should ensure that their Business Continuity Plans are updated and current.

If a department is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

through these links, nor does it endorse the sites and their content.

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, November 2, 2012 17:05
To: CTEC
Subject: Update/Mise à jour no 5: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

English version sent previously.

==========
CECM-GC - Note d'information IN12-002
Date : 29 octobre 2012
==========

==========
Mise à jour no 5 : 29 octobre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous - Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

ÉVALUATION
==========

Le 29 octobre 2012, l'activité liée à cette note d'information semble avoir diminué considérablement comparativement à la dernière mise à jour. Cette activité se rapporterait toujours à l'opération #OpPartyCrasher et à d'autres opérations connexes d'Anonymous devant se dérouler du 3 au 15 novembre 2012. Pour l'instant, 21(1)(b)

21(1)(b)

L'activité observée est toujours conforme à celle énoncée dans la mise à jour no 4. 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

La baisse d'activité ne signifie pas que la campagne a pris fin; il est bien probable qu'elle soit temporaire. On recommande donc aux ministères de rester vigilants.

Le CECM-GC prévient les ministères que la portée et le niveau d'activité pourraient augmenter à mesure que les dates prévues de la campagne approchent, et que les techniques d'attaque pourraient varier de celles dont se sert habituellement Anonymous.

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :

- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@csecst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, November 2, 2012 17:05
To: CTEC
Subject: Update/Mise à jour no 6: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous – Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

English version sent previously.

==========
CECM-GC – Note d'information IN12-002
Date : 30 octobre 2012
==========

==========
Mise à jour no 6 : 30 octobre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

ÉVALUATION
==========

Le 30 octobre 2012, l'activité liée à cette note d'information semble encore avoir diminué comparativement aux niveaux d'activité détectés du 25 au 28 octobre. Cette activité se rapporterait toujours à l'opération #OpPartyCrasher et à d'autres opérations connexes d'Anonymous devant se dérouler du 3 au 15 novembre 2012. Pour l'instant, on

21(1)(b)

L'activité observée est toujours conforme à celle des mises à jour précédentes. 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Le CECM-GC a diffusé la cybercapsule GCCF12-008 intitulée « Campagne de déni de service distribué contre le GC » afin de fournir aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Le CECM-GC prévient les ministères que la portée et le niveau d'activité pourraient

augmenter à mesure que les dates prévues de la campagne approchent, et que les techniques d'attaque pourraient varier de celles dont se sert habituellement Anonymous.

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

On vous recommande fortement de mettre en œuvre les conseils d'atténuation énoncés dans la cybercapsule GCCF12-008.

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est

important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, November 2, 2012 17:05
To: CTEC
Subject: Update/Mise à jour no 7: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous – Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

English version sent previously.

==========
CECM-GC – Note d'information IN12-002
Date : 31 octobre 2012
==========

==========
Mise à jour no 7 : 31 octobre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

ÉVALUATION
==========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de la campagne de déni de service distribué visant le GC planifiée par Anonymous. Cette compagne, regroupant #OpPartyCrasher et d'autres opérations connexes, est prévue du 3 au 15 novembre 2012.

Depuis le 25 octobre, un grand nombre de ministères ont signalé des activités comparables à des tentatives de déni de service distribué, mais aucun lien direct n'a pu être établi avec la campagne planifiée d'Anonymous. Le CECM-GC prévient les ministères que la portée et le niveau d'activité malveillante pourraient augmenter à mesure que les dates prévues de la campagne approchent, et que les techniques d'attaque pourraient varier de celles dont se sert habituellement Anonymous.

Jusqu'ici, les activités connexes observées comprennent :

16(2)(c),21(1)(a),21(1)(b)

Le CECM-GC diffusera des cybercapsules à mesure qu'il cernera les mesures d'atténuation technique requises.

À ce jour, le CECM-GC a publié la cybercapsule suivante :

- GCCF12-008 : « Campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

On vous recommande fortement de mettre en œuvre les conseils d'atténuation énoncés dans la cybercapsule GCCF12-008.

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
- l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse-cst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est

important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, November 2, 2012 17:14
To: CTEC
Subject: Update/Mise à jour no 8: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous – Attaque par déni de service distribué visant le GC

Importance: High

Classification: UNCLASSIFIED

(La version française suit)

==========
GC CTEC - Information Note IN12-002
Date: 1 November 2012
==========

==========
Update 8: 1 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the planned Anonymous DDOS operation against the GC . The operation, #OpPartyCrasher and related operations, is scheduled to occur from 3 to 15 November 2012.

NEW HIGHLIGHTS
==========
Potential traces of HOIC activity have been detected.

ASSESSMENT
==========

Since 25 October 2012, there have been multiple departments reporting activity consistent with DDOS attempts, however no direct link has been made with the planned Anonymous campaign. GC-CTEC advises that the scope and level of malicious activity may fluctuate between now and the targeted date range specified, and that it may not follow typical Anonymous techniques. There has been no major impact on the GC by any of the observed activity to date.

To date, observed DDOS-related activities include:

16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

As GC-CTEC identifies malicious activity impacting the GC, Cyber Flash products will be disseminated to provide the associated technical mitigation advice.

To date, GC-CTEC has released:
- GCCF12-008: DDoS campaign against the GC - which provided mitigation recommendations

16(2)(c),21(1)(a),21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

Departments should implement the mitigation advice in GCCF12-008: DDoS campaign against the GC.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here:
http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf
and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats;

providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

==========

==========
CECM-GC – Note d'information IN12-002
Date : 1er novembre 2012
==========

==========
Mise à jour no 8 : 1er novembre 2012
- Mise à jour de l'information sur l'évaluation
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

OBJECTIF
========

La présente note d'information vise à vous tenir au courant de la situation dans le cadre de la campagne de déni de service distribué visant le GC planifiée par Anonymous. Cette compagne, regroupant #OpPartyCrasher et d'autres opérations connexes, est prévue du 3 au 15 novembre 2012.

ÉVALUATION
==========

Depuis le 25 octobre, un grand nombre de ministères ont signalé des activités comparables à des tentatives de déni de service distribué, mais aucun lien direct n'a pu être établi avec la campagne planifiée d'Anonymous. Le CECM-GC prévient les ministères que la portée et le niveau d'activité malveillante pourraient augmenter à mesure que les dates prévues de la campagne approchent, et que les techniques d'attaque pourraient varier de celles dont se sert habituellement Anonymous. Il convient toutefois de noter que les activités observées à ce jour n'ont eu aucune incidence majeure sur le GC.

Jusqu'ici, les activités pertinentes comprennent :

16(2)(c),21(1)(a),21(1)(b)

À mesure qu'il découvrira des activités malveillantes touchant le GC, le CECM-GC diffusera des cybercapsules contenant des conseils d'atténuation technique connexes. À ce jour, le CECM-GC a publié la cybercapsule suivante :
 - GCCF12-008 : « Campagne de déni de service distribué contre le GC », laquelle fournit aux ministères des mesures d'atténuation recommandées qu'ils peuvent mettre en œuvre au

16(2)(c),21(1)(a),21(1)(b)

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur du Réseau 16(2)(c)

On vous recommande fortement de mettre en œuvre les conseils d'atténuation énoncés dans la cybercapsule GCCF12-008.

Si vous découvrez du trafic lié à cette attaque par déni de service distribué au sein de votre ministère ou si vous êtes aux prises avec une interruption de service, veuillez communiquer avec les deux personnes suivantes :
 - l'agent de service des Opérations de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;
 - l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour de plus amples renseignements sur la présente note d'information, veuillez envoyer un courriel à CTEC@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse cst.gc.ca.

==========

Note aux lecteurs
==========

Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des

infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:54
To: Sargent, Rob: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Rob are still sending?

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:51 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line 16(2)(c) only 2 such emails were sent out since 16(2)(c)

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:45 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Here's a list of emails with the following characteristics:

- Taken from tracking logs on both 16(2)(c) and 16(2)(c) .. i.e. results are combined.
- subject line: 16(2)(c)

This is similar to what I see being generated on 16(2)(c)
16(2)(c)
Emails started on 16(2)(c) and continued through this morning.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:31 PM
To: Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

I'm working on a list of emails … there were many, and sent to multiple recipients. Will get that to everyone in the next 15 minutes I hope.

16(2)(c)

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:09 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

On 16(2)(c) ...give or take 5 minutes.

rob

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:07 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: Phishing investigation

Rob, please search the 16(2)(c) for a subject line " 16(2)(c) " from the 16(2)(c)

Cheers,

rob

Robert Edwards
Manager Network Security Services | Gestionnaire du Réseau des services de sécurité
Shared Services Canada - Services partagés Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@spc-ssc.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Hagarty, Richard: CIO-BI
Sent: Wednesday, January 30, 2013 13:21
To: Cullen, Jennifer: CIO-BI
Cc: Fournier, Denis: CIO-BI
Subject: FW: 16(2)(c) - Recommendations from SSC - EP

I will need some detail on the last incident that should be reviewed by SSC. I'm unsure at this point if we are actually talking about the same case.

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 30, 2013 9:20 AM
To: Hagarty, Richard: CIO-BI
Subject: RE: 16(2)(c) - Recommendations from SSC - EP

Richard, we have one confirmed, the second incident is under review which looks like the same situation.

16(2)(c).21(1)(b)

Cheers,

Rob

From: Hagarty, Richard: CIO-BI
Sent: Wednesday, January 30, 2013 9:08 AM
To: Edwards, Robert: SSC-SPC
Subject: FW: 16(2)(c) - Recommendations from SSC - EP

Hi again Rob,

I need to brief our DSO and wanted to clarify the following statements from Neelam where she states that:

16(2)(c)

16(2)(c)

The statements suggest that several accounts were compromised, yet to my understanding from our last discussion, only one was actually found to be compromised.

Can you let me know what we are looking at one or many?

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

From: Pradhan, Neelam: SSC-SPC
Sent: Tuesday, January 29, 2013 4:53 PM
To: Acton, Kelly: CIO-BI
Cc: Gravel, Pierre: SSC-SPC; Campbell, Sandy: SSC; Moffett, Cameron: SSC; Crockett, Dave: SSC; Kasiri, Mehrdad: SSC-SPC (NCR-RCN); Fillion, Marc: SSC-SPC; Micucci, Nathalie: SSC-SPC; Edwards, Robert: SSC-SPC; Bernard, Mario: CIO-BI; Hagarty, Richard: CIO-BI; Cloutier, Christine: SSC-SPC; Beauchamp, Manon: SSC-SPC
Subject: FW: 16(2)(c) - Recommendations from SSC - EP

Hi Kelly,

Attached are the SSC - EP recommendations for 16(2)(c) If you are OK with this, we can start to work together for a planned implementation:

Background: 16(2)(c) is a service provided by Industry Canada (IC) to its users to 16(2)(c) 16(2)(c)

16(2)(c)

Other similar incidents have happened in the past few months making this service 16(2)(c) 16(2)(c)

In an effort to mitigate the risks for Industry Canada, it was decided, on 16(2)(c) 16(2)(c) and to examine the logs for determining the future course of action.

Analysis: On further analysis of the logs, there is a distinct pattern 16(2)(c) 16(2)(c) yet, the risk 16(2)(c). As a result, options and solutions need to be further discussed and put in place.

Option 1: 16(2)(c),21(1)(a)

16(2)(c),21(1)(a)

16(2)(c),21(1)(a)

Option 2: 16(2)(c),21(1)(a)

16(2)(c),21(1)(a)

16(2)(c),21(1)(a),21(1)(b)

Also, IC is to provide estimated number of users that will require access on priority basis. We will need a process to manage accordingly (users setup, training, assignment of tokens, etc.)

Recommendations:

SSC recommends 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Neelam Pradhan
A/Senior Director, Data Centre and Email | Directrice principale par intérim, centre de données et courriel
Economic Portfolio | Portefeuille économique
Shared Services Canada | Services partagés Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Neelam.Pradhan@ssc-spc.gc.ca
Telephone | Téléphone : 613-946-7506
Fax / Télécopieur: 613-941-4615
Government of Canada | Gouvernement du Canada

Shared Services Canada | Services partagés Canada

Lacroix, Lise: SBTMS-SMTPE

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:49
To: IT Security
Subject: FW: Phishing investigation

Attachments: 16(2)(c)

We've got several different email threads going as we address this issue … here's a copy of what I just sent to the network group…

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:45 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Here's a list of emails with the following characteristics:

- Taken from tracking logs on both 16(2)(c) and 16(2)(c) .. i.e. results are combined.
- subject line: 16(2)(c)

This is similar to what I see being generated on 16(2)(c)
16(2)(c)
16(2)(c) and continued through this morning.

16(2)(c)

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:31 PM
To: Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

I'm working on a list of emails … there were many, and sent to multiple recipients. Will get that to everyone in the next 15 minutes I hope.

16(2)(c),21(1)(a),21(1)(b)

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:09 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

On 16(2)(c) ..give or take 5 minutes.

rob

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:07 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: Phishing investigation

Rob, please search the 16(2)(c) for a subject line " 16(2)(c) " from the 16(2)(c)

Cheers,

rob

Robert Edwards
Manager Network Security Services | Gestionnaire du Réseau des services de sécurité
Shared Services Canada - Services partagés Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@spc-ssc.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Tennian, Frank: SSC-SPC
Sent: Wednesday, January 23, 2013 13:43
To: Farah, Elias: SSC-SPC; Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: Re: Phishing investigation

Hi.

Denis Begin did that earlier this morning.

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 01:39 PM Eastern Standard Time
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Hi Rob,

One more thing. Did you 16(2)(c)

Rob E asked that 16(2)(c) if not done yet.

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:37 PM
To: Farah, Elias: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

16(2)(c) can't indicate originating IP.

I'm looking through the 16(2)(c) on the server, which logs successful logons, and I don't see anything yet in terms of accessing this mailbox

---

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 1:32 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation
Importance: High

Hi Rob S,

Is there any indication in the mail server logs where those connections are coming from? Do we see connections from internal IP addresses? Do you have that information?

That would be very helpful as to whether we have any compromised machines or not.

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:02 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line '' 16(2)(c) '', here is the list of emails.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:51 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line 16(2)(c) only 2 such emails were sent out since 16(2)(c) 16(2)(c)

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:45 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Here's a list of emails with the following characteristics:

- Taken from tracking logs on both 16(2)(c) and 16(2)(c) .. i.e. results are combined.
- subject line: 16(2)(c)

This is similar to what I see being generated on 16(2)(c) 16(2)(c)

Emails started on 16(2)(c) and continued through this morning.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:31 PM
To: Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

I'm working on a list of emails ... there were many, and sent to multiple recipients. Will get that to everyone in the next 15 minutes I hope.

16(2)(c).21(1)(a).21(1)(b)

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:09 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

On 16(2)(c) ..give or take 5 minutes.

rob

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:07 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: Phishing investigation

Rob, please search the 16(2)(c) for a subject line " 16(2)(c) " from the 16(2)(c)

Cheers,

rob

Robert Edwards
Manager Network Security Services | Gestionnaire du Réseau des services de sécurité
Shared Services Canada - Services partagés Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@spc-ssc.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 13:42
To: Farah, Elias: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Yes, our team 16(2)(c)

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 1:40 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Hi Rob,

One more thing. Did you 16(2)(c)

Rob E asked that 16(2)(c) if not done yet.

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:37 PM
To: Farah, Elias: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

16(2)(c) can't indicate originating IP.

I'm looking through the 16(2)(c) on the server, which logs successful logons, and I don't see anything yet in terms of accessing this mailbox

---

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 1:32 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation
Importance: High

Hi Rob S,

Is there any indication in the mail server logs where those connections are coming from? Do we see connections from internal IP addresses? Do you have that information?

That would be very helpful as to whether we have any compromised machines or not.

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:02 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering

Subject: RE: Phishing investigation

FYI For the subject line '16(2)(c)', here is the list of emails.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:51 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line 16(2)(c) only 2 such emails were sent out since 16(2)(c)

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:45 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Here's a list of emails with the following characteristics:

- Taken from tracking logs on both 16(2)(c) and 16(2)(c) .. i.e. results are combined.
- subject line: 16(2)(c)

This is similar to what I see being generated on 16(2)(c)
16(2)(c)
Emails started on 16(2)(c) and continued through this morning.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:31 PM
To: Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

I'm working on a list of emails … there were many, and sent to multiple recipients. Will get that to everyone in the next 15 minutes I hope.

16(2)(c).21(1)(a).21(1)(b)

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:09 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

On 16(2)(c) ..give or take 5 minutes.

rob

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:07 PM
To: Sargent, Rob: SSC-SPC

Cc: NSG Security - Securité GSR
Subject: Phishing investigation

Rob, please search the 16(2)(c) for a subject line " 16(2)(c) " from the 16(2)(c)

Cheers,

rob

Robert Edwards
Manager Network Security Services | Gestionnaire du Réseau des services de sécurité
Shared Services Canada - Services partagés Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@spc-ssc.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 13:40
To: Farah, Elias: SSC-SPC; Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Hi Elias, yes 16(2)(c)

Denis

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 1:40 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Hi Rob,

One more thing. Did you 16(2)(c)

Rob E asked that 16(2)(c) if not done yet.

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:37 PM
To: Farah, Elias: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

16(2)(c) can't indicate originating IP.

I'm looking through the 16(2)(c) on the server, which logs successful logons, and I don't see anything yet in terms of accessing this mailbox

---

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 1:32 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation
Importance: High

Hi Rob S,

Is there any indication in the mail server logs where those connections are coming from? Do we see connections from internal IP addresses? Do you have that information?

That would be very helpful as to whether we have any compromised machines or not.

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:02 PM

To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line '16(2)(c)', here is the list of emails.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:51 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line 16(2)(c) only 2 such emails were sent out since 16(2)(c)

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:45 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Here's a list of emails with the following characteristics:

- Taken from tracking logs on both 16(2)(c) and 16(2)(c) .. i.e. results are combined.
- subject line: 16(2)(c)

This is similar to what I see being generated on 16(2)(c)
16(2)(c)
Emails started on 16(2)(c) and continued through this morning.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:31 PM
To: Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

I'm working on a list of emails … there were many, and sent to multiple recipients. Will get that to everyone in the next 15 minutes I hope.

16(2)(c),21(1)(a),21(1)(b)

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:09 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

On 16(2)(c) ..give or take 5 minutes.

rob

From: Edwards, Robert: SSC-SPC

Sent: Wednesday, January 23, 2013 12:07 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: Phishing investigation

Rob, please search the 16(2)(c) for a subject line " 16(2)(c) " from the 16(2)(c)

Cheers,

rob

Robert Edwards
Manager Network Security Services | Gestionnaire du Réseau des services de sécurité
Shared Services Canada - Services partagés Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@spc-ssc.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Sargent, Rob: SSC-SPC
Sent: Thursday, January 24, 2013 10:47
To: Phillips, James: SSC-SPC; Farah, Elias: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

One of the two, 19(1) has a BlackBerry with an account on our BES.

From: Phillips, James: SSC-SPC
Sent: Thursday, January 24, 2013 10:37 AM
To: Farah, Elias: SSC-SPC; Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Hi Rob,

Can you confirm whether the two users that have access to the account have a blackberry?

If so, please indicate who.

We are seeing blackberry accesses from the US via the web browser on the phone.

James Phillips
Technical Specialist, Network Security | Spécialiste technique, sécurité du réseau
Shared Services Canada - Industry Canada | Services partagés Canada - Industrie Canada
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
James.Phillips@ic.gc.ca
Telephone | Téléphone 613-941-7874
Facsimile | Télécopieur 613-941-4615
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 4:25 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Hi Denis and Rob S,

Does the user have a blackberry? Do we have any BES logs?

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:37 PM
To: Farah, Elias: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

16(2)(c) can't indicate originating IP.

I'm looking through the 16(2)(c) on the server, which logs successful logons, and I don't see anything yet in terms of accessing this mailbox

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 1:32 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation
Importance: High

Hi Rob S,

Is there any indication in the mail server logs where those connections are coming from? Do we see connections from internal IP addresses? Do you have that information?

That would be very helpful as to whether we have any compromised machines or not.

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:02 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line '16(2)(c)', here is the list of emails.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:51 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line 16(2)(c) only 2 such emails were sent out since 16(2)(c)

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:45 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Here's a list of emails with the following characteristics:

- Taken from tracking logs on both 16(2)(c) and 16(2)(c) .. i.e. results are combined.
- subject line: 16(2)(c)

This is similar to what I see being generated on 16(2)(c)
16(2)(c)
Emails started on 16(2)(c) and continued through this morning.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:31 PM
To: Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR

Subject: RE: Phishing investigation

I'm working on a list of emails … there were many, and sent to multiple recipients. Will get that to everyone in the next 15 minutes I hope.

16(2)(c),21(1)(a),21(1)(b)

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:09 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

On 16(2)(c) ..give or take 5 minutes.

rob

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:07 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: Phishing investigation

Rob, please search the 16(2)(c) for a subject line '16(2)(c)' from the 16(2)(c)

Cheers,

rob

Robert Edwards
Manager Network Security Services | Gestionnaire du Réseau des services de sécurité
Shared Services Canada - Services partagés Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@spc-ssc.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 13:58
To: Begin, Denis: SSC-SPC (NCR-RCN); Fournier, Denis: CIO-BI; MDP Team
Subject: RE: 16(2)(c)

FYI I also just put a 16(2)(c) on the mailbox to 16(2)(c) ..

I set the 16(2)(c)

From: Begin, Denis: SSC-SPC (NCR-RCN)
Sent: Wednesday, January 23, 2013 11:06 AM
To: Fournier, Denis: CIO-BI; MDP Team
Subject: RE: 16(2)(c)

16(2)(c)

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 11:01 AM
To: MDP Team
Cc: IT Security
Subject: 16(2)(c)

Hi,

Until we are able to clear up what happen in this event please 16(2)(c) 16(2)(c) from sending emails.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, October 17, 2012 16:43
To: Fournier, Denis: CIO-BI
Cc: CTEC
Subject: [CE2012-1247]: IT Security 30-12 IMP Cyber Incident Report

Classification: UNCLASSIFIED

Hi Denis,

That's quite interesting; these guys are obviously using the same infrastructure for this new 15(1) phishing campaign as the previous one. Good catch!

Thank you,

15(1)

<---------->
15(1)
GC-CTEC Cyber Analyst
Cyber Threat Evaluation Centre
Tel# 15(1)

From: Denis.Fournier@ic.gc.ca [mailto:Denis.Fournier@ic.gc.ca]
Sent: October 17, 2012 2:58 PM
To: CTEC
Subject: IT Security 30-12 IMP Cyber Incident Report

Hi guys, tough you would like this one right away

Thanks

<<IC_IT_Sec30-12_IMP Cyber Incident Report.doc>> <<Header IMP30-12.doc>> <<email imp30-12.doc>>

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Industry Canada Industrie Canada

Canada

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 11:28
To: IT Service Desk - Centre de services TI
Cc: IT Security
Subject: "URGENT" Suspicious activity Potential Malware

Service Desk,

Please create a ticket under IT Security and assign a technician for immediate action

The following action needs to be taken **ASAP** without any **delays**.

16(2)(c)

19(1)

Take a look if the " 16(2)(c) " mailbox is open on there computer

IT Security will update ticket once we have information from TSO.

Thank you

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: McCloskey, Paul: CIO-BI (NCR-RCN)
Sent: Friday, January 11, 2013 16:14
To: Gosselin, Andrée: CIO-BI
Cc: CIO IT CAB Members; Corman, Chris: CIO-BI; CIO IT Problem Manager; Thibaudeau, Stéphane: CB-BC; IT Security
Subject: Emergency Virtual CAB to address confidential request from CTEC (GC's Cyber Threat Evaluation Centre) RFC # 105769

Importance: High

RFC: **105769**

IR: **105770**

DESCRIPTION OF CHANGE - This is a confidential request from CTEC (GC's Cyber Threat Evaluation Centre), reference CE2-013-1602 which requires 16(2)(c) 16(2)(c) We request this work be performed this weekend which has been determined to be an acceptable timeframe to the client.

Details are with NSG Security (Rob Edwards).

The above changes are user impacting and are being requested to be implemented this weekend

If anyone has any issues with these changes being implemented, please advise immediately.

Paul McCloskey
Manager, IT Service Management | Gestionnaire, Gestion des services
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Paul.McCloskey@ic.gc.ca
Telephone | Téléphone 613-954-5511
Facsimile | Télécopieur 613-946-3320
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Frendo, Mona: SPS
Sent: Thursday, January 24, 2013 10:47
To: Fournier, Denis: CIO-BI; 19(1)
Subject: RE: Account comprimised

Thanks everyone.

From: Fournier, Denis: CIO-BI
Sent: Thursday, January 24, 2013 10:19 AM
To: Frendo, Mona: SPS; 19(1)
Subject: RE: Account comprimised

Hi Mona, I just talk to 19(1) and she is very helpful. She is doing a bit of research for me and I am suppose to call her back at around 11.

Thanks

From: Frendo, Mona: SPS
Sent: Thursday, January 24, 2013 10:17 AM
To: Fournier, Denis: CIO-BI; 19(1)
Subject: RE: Account comprimised

Wow! What happened and how?

From: Fournier, Denis: CIO-BI
Sent: Thursday, January 24, 2013 10:06 AM
To: 19(1)
Cc: Frendo, Mona: SPS
Subject: Account comprimised

Hi 19(1)

Can you please call me. We have evidence that your account is compromised and more then 25000 spam emails were sent from the 16(2)(c)

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:46
To: Fournier, Denis: CIO-BI
Subject: RE: Infected computer sending Spam

perfect

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 12:46 PM
To: Edwards, Robert: SSC-SPC
Subject: Re: Infected computer sending Spam

Ok it should be over at around 13:50
I will ping you

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:44 PM Eastern Standard Time
To: Fournier, Denis: CIO-BI
Subject: RE: Infected computer sending Spam

after that meeting should be good...we may want to have CTEC on a call later today...but we should chat first.

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 12:43 PM
To: Edwards, Robert: SSC-SPC
Subject: Re: Infected computer sending Spam

When do you want to meet. I have the CCIRC meeting at 13;30

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 11:51 AM Eastern Standard Time
To: Fournier, Denis: CIO-BI
Subject: RE: Infected computer sending Spam

Elias and I need to meet with you...

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 11:51 AM
To: Edwards, Robert: SSC-SPC
Subject: Re: Infected computer sending Spam

I will look in the sent items and send it to you

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 11:48 AM Eastern Standard Time
To: Fournier, Denis: CIO-BI
Cc: NSG Security - Securité GSR; MDP Team
Subject: RE: Infected computer sending Spam

Denis, I believe you said you have access to the mailbox. Please forward the two emails from the 16(2)(c) mailbox time stamped 16(2)(c)

Since they appear to have orginated from the mailbox, we need to look at the header and message body of the messages in their original form.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 10:29 AM
To: Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Infected computer sending Spam

Hi Rob, don't now what happened there. But here is another one:

<< Message: 16(2)(c) >>

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:55 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Denis, the header information is missing within the messages.

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:33 AM
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Rob, here are the 4 examples of emails that were sent with the account.

<< Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >>

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:29 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Can you provide an original message which went outbound? As well, within the mail logs, if enable, the ability to see originating IP address. You need to look deep.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:27 AM
To: NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: Infected computer sending Spam

Hi Guy's,

We have an internal computer that sent Spam on 16(2)(c)
We have the logs that show this was sent and we have the account sent items that show all the emails.

We need to find out what computer was used to send these emails and the user if possible. Is there a way that you would have this information in your logs 16(2)(c)

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 11:52
To: Fournier, Denis: CIO-BI
Subject: RE: Infected computer sending Spam

Elias and I need to meet with you...

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 11:51 AM
To: Edwards, Robert: SSC-SPC
Subject: Re: Infected computer sending Spam

I will look in the sent items and send it to you

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 11:48 AM Eastern Standard Time
To: Fournier, Denis: CIO-BI
Cc: NSG Security - Securité GSR; MDP Team
Subject: RE: Infected computer sending Spam

Denis, I believe you said you have access to the mailbox. Please forward the two emails from the 16(2)(c) mailbox time stamped 16(2)(c)

Since they appear to have orginated from the mailbox, we need to look at the header and message body of the messages in their original form.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 10:29 AM
To: Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Infected computer sending Spam

Hi Rob, don't now what happened there. But here is another one:

<< Message: 16(2)(c) >>

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:55 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team

Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Denis, the header information is missing within the messages.

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:33 AM
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Rob, here are the 4 examples of emails that were sent with the account.

<< Message: 16(2)(c) >> << Message: 16(2)(c)
>> << Message: 16(2)(c) >> << Message: 16(2)(c) >>

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:29 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Can you provide an original message which went outbound? As well, within the mail logs, if enable, the ability to see originating IP address. You need to look deep.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:27 AM
To: NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: Infected computer sending Spam

Hi Guy's,

We have an internal computer that sent Spam on 16(2)(c)
We have the logs that show this was sent and we have the account sent items that show all the emails.

We need to find out what computer was used to send these emails and the user if possible. Is there a way that you would have this information in your logs 16(2)(c)

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 11:28
To: Fournier, Denis: CIO-BI; Messaging Engineering
Cc: IT Security
Subject: RE: Infected computer sending Spam

16(2)(c)

Recipients lists to follow...

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 11:03 AM
To: Fournier, Denis: CIO-BI; Messaging Engineering
Cc: IT Security
Subject: RE: Infected computer sending Spam

Hi again, I forgot to mention, that we also need the internal recipient list for these accounts.

Thanks

Denis

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 10:28 AM
To: Messaging Engineering
Cc: IT Security
Subject: Infected computer sending Spam

Hi guys,

You gave us the recipient list for the "16(2)(c)" subject line

16(2)(c) that are related with this case and give us the recipient lists for each.

Thanks

16(2)(c)

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 10:29
To: Fournier, Denis: CIO-BI; Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security
Subject: RE: Infected computer sending Spam

Hi Denis,

Can you please provide us with all the information you have regarding this incident? Including the ctec alert and timeline of events.

Thanks,

Elias

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:33 AM
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Rob, here are the 4 examples of emails that were sent with the account.

<< Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >>

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:29 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Can you provide an original message which went outbound? As well, within the mail logs, if enable, the ability to see originating IP address. You need to look deep.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:27 AM
To: NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: Infected computer sending Spam

Hi Guy's,

We have an internal computer that sent Spam on 16(2)(c) We have the logs that show this was sent and we have the account sent items that show all the emails.

We need to find out what computer was used to send these emails and the user if possible. Is there a way that you would

have this information in your logs 16(2)(c)

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, January 23, 2013 10:08
To: Fournier, Denis: CIO-BI
Subject: RE: Infected computer sending Spam

HI Denis,
Can you ask for the recipient lists for all of the spam emails sent from that account. Please be sure that they include the internal user recipient list as well.
Thanks,
Jen

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:33 AM
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Rob, here are the 4 examples of emails that were sent with the account.

<< Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >>

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:29 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Can you provide an original message which went outbound? As well, within the mail logs, if enable, the ability to see originating IP address. You need to look deep.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:27 AM
To: NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: Infected computer sending Spam

Hi Guy's,

We have an internal computer that sent Spam on 16(2)(c) We have the logs that show this was sent and we have the account sent items that show all the emails.

We need to find out what computer was used to send these emails and the user if possible. Is there a way that you would have this information in your logs 16(2)(c)

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Tennian, Frank: SSC-SPC
Sent: Wednesday, January 23, 2013 8:58
To: Fournier, Denis: CIO-BI; Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Done.

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:56 AM
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: Re: Infected computer sending Spam

Frank can you remove the rights for 19(1) for this account. She does not work for this group anymore

Thanks

Denis

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 08:33 AM Eastern Standard Time
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Rob, here are the 4 examples of emails that were sent with the account.

16(2)(c)

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:29 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Can you provide an original message which went outbound? As well, within the mail logs, if enable, the ability to see originating IP address. You need to look deep.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:27 AM
To: NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: Infected computer sending Spam

Hi Guy's,

We have an internal computer that sent Spam on 16(2)(c)
We have the logs that show this was sent and we have the account sent items that show all the emails.

We need to find out what computer was used to send these emails and the user if possible. Is there a way that you would have this information in your logs 16(2)(c)

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 8:45
To: Fournier, Denis: CIO-BI; Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

I'm checking the logs to see if I can determine an originating IP....

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:33 AM
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Rob, here are the 4 examples of emails that were sent with the account.

<< Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >>

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:29 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Can you provide an original message which went outbound? As well, within the mail logs, if enable, the ability to see originating IP address. You need to look deep.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:27 AM
To: NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: Infected computer sending Spam

Hi Guy's,

We have an internal computer that sent Spam on 16(2)(c) We have the logs that show this was sent and we have the account sent items that show all the emails.

We need to find out what computer was used to send these emails and the user if possible. Is there a way that you would have this information in your logs 16(2)(c)

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI

Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 15:50
To: Fournier, Denis: CIO-BI
Subject: RE: Infected computer sending Spam

Hi Denis,

The mailbox you gave me is for which user?

Thanks,

Elias

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 2:48 PM
To: Farah, Elias: SSC-SPC; ITSec
Cc: Edwards, Robert: SSC-SPC
Subject: RE: Infected computer sending Spam

Yes, yesterday TSOs were sent to the 2 persons that had access to that account and found nothing

I'm going up

Denis

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 2:46 PM
To: Fournier, Denis: CIO-BI; ITSec
Cc: Edwards, Robert: SSC-SPC
Subject: RE: Infected computer sending Spam

Hi Denis,

Did anyone check the users' machines to ensure they are clean?

Thanks,

Elias

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 10:42 AM
To: Farah, Elias: SSC-SPC
Cc: Edwards, Robert: SSC-SPC
Subject: RE: Infected computer sending Spam

Elias,

The only 2 persons that have access to send emails from this account is:

19(1)	16(2)(c)

19(1)

Denis

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 10:38 AM
To: Fournier, Denis: CIO-BI
Subject: FW: Infected computer sending Spam

Hi Denis,

The message below was meant for you.

Elias

From: Begin, Denis: SSC-SPC (NCR-RCN)
Sent: Wednesday, January 23, 2013 10:36 AM
To: Farah, Elias: SSC-SPC; Fournier, Denis: CIO-BI
Subject: Re: Infected computer sending Spam

Sorry, which Denis.... Me or Fournier?

For me, I provided Denis Fournier with 16(2)(c)
16(2)(c)

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 10:28 AM
To: Fournier, Denis: CIO-BI; Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security
Subject: RE: Infected computer sending Spam

Hi Denis,

Can you please provide us with all the information you have regarding this incident? Including the ctec alert and timeline of events.

Thanks,

Elias

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:33 AM
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Rob, here are the 4 examples of emails that were sent with the account.

<< Message: 16(2)(c) >> << Message: 16(2)(c)
>> << Message: 16(2)(c) >> << Message: 16(2)(c) >>

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 8:29 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: RE: Infected computer sending Spam

Can you provide an original message which went outbound? As well, within the mail logs, if enable, the ability to see originating IP address. You need to look deep.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:27 AM
To: NSG Security - Securité GSR; MDP Team
Cc: IT Security; NSG Operations - Exploitation GSR
Subject: Infected computer sending Spam

Hi Guy's,

We have an internal computer that sent Spam on 16(2)(c)
We have the logs that show this was sent and we have the account sent items that show all the emails.

We need to find out what computer was used to send these emails and the user if possible. Is there a way that you would have this information in your logs 16(2)(c)

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Edwards, Robert: SSC-SPC
Sent: Thursday, January 24, 2013 9:53
To: Cullen, Jennifer: CIO-BI
Cc: Fournier, Denis: CIO-BI; Farah, Elias: SSC-SPC
Subject: RE: Meeting Summary

Hi Jen, we are still reviewing the 16(2)(c) and other logs in concert....we will provide an update around noon.

Cheers,

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, January 23, 2013 3:59 PM
To: Edwards, Robert: SSC-SPC
Cc: Fournier, Denis: CIO-BI; Farah, Elias: SSC-SPC
Subject: Meeting Summary

Hi Rob,

To recap our short meeting of this afternoon, you had stated that you have exhausted all avenues for the purpose of determining the source (system) of the SPAM emails. If I remember correctly, I think James is also analysing some logs. Can you please provide a summary of these activities?

Also, Denis had provided to you 16(2)(c) logs that were provided to us by Messaging Engineering. The logs cover, at a minimum, from 16(2)(c) Within the logs, we had noticed what appears to a be a related icent account labelled 16(2)(c) for the mailbox 16(2)(c). As requested, could you please have a look at the logs in order to determine what this 16(2)(c) account is?

In the meantime, we will follow-up with the client to understand the purpose of this mailbox and understand her recent login activity.

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Thursday, January 24, 2013 10:52
To: Phillips, James: SSC-SPC; Farah, Elias: SSC-SPC; Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Hi James,

I have a bit more information on this.

The old client that use to be the admin for this account 19(1) did have a BB 11/2 ago when she was working SPS. But does not have one anymore

The other person that is now the admin for the account 19(1) has a BB phone number 19(1)

She explained to me that she has not accessed the account in over 1 year and they do not use it anymore.

They were using this account when they were sending emails out emails for the group concerning project.

Both user have changed there username and password for all their accounts.

Denis

From: Phillips, James: SSC-SPC
Sent: Thursday, January 24, 2013 10:37 AM
To: Farah, Elias: SSC-SPC; Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Hi Rob,

Can you confirm whether the two users that have access to the account have a blackberry?

If so, please indicate who.

We are seeing blackberry accesses from the US via the web browser on the phone.

James Phillips
Technical Specialist, Network Security | Spécialiste technique, sécurité du réseau
Shared Services Canada - Industry Canada | Services partagés Canada - Industrie Canada
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
James.Phillips@ic.gc.ca
Telephone | Téléphone 613-941-7874
Facsimile | Télécopieur 613-941-4615
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 4:25 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Hi Denis and Rob S,

Does the user have a blackberry? Do we have any BES logs?

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:37 PM
To: Farah, Elias: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

16(2)(c) can't indicate originating IP.

I'm looking through the 16(2)(c) on the server, which logs successful logons, and I don't see anything yet in terms of accessing this mailbox

---

From: Farah, Elias: SSC-SPC
Sent: Wednesday, January 23, 2013 1:32 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation
Importance: High

Hi Rob S,

Is there any indication in the mail server logs where those connections are coming from? Do we see connections from internal IP addresses? Do you have that information?

That would be very helpful as to whether we have any compromised machines or not.

Thanks,

Elias

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 1:02 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line "16(2)(c)", here is the list of emails.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:51 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC; IT Security
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

FYI For the subject line 16(2)(c) only 2 such emails were sent out since 16(2)(c)

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:45 PM
To: Sargent, Rob: SSC-SPC; Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR; Messaging Engineering
Subject: RE: Phishing investigation

Here's a list of emails with the following characteristics:

- Taken from tracking logs on both 16(2)(c) and 16(2)(c) .. i.e. results are combined.
- subject line: 16(2)(c)

This is similar to what I see being generated on 16(2)(c) the home server of the 16(2)(c) mailbox.
Emails started on 16(2)(c) and continued through this morning.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Wednesday, January 23, 2013 12:31 PM
To: Edwards, Robert: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

I'm working on a list of emails … there were many, and sent to multiple recipients. Will get that to everyone in the next 15 minutes I hope.

16(2)(c),21(1)(a),21(1)(b)

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:09 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: RE: Phishing investigation

On 16(2)(c) ..give or take 5 minutes.

rob

From: Edwards, Robert: SSC-SPC
Sent: Wednesday, January 23, 2013 12:07 PM
To: Sargent, Rob: SSC-SPC
Cc: NSG Security - Securité GSR
Subject: Phishing investigation

Rob, please search the 16(2)(c) for a subject line " 16(2)(c) " from the 16(2)(c)

Cheers,

rob

Robert Edwards
Manager Network Security Services | Gestionnaire du Réseau des services de sécurité
Shared Services Canada - Services partagés Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@spc-ssc.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Tennian, Frank: SSC-SPC
Sent: Wednesday, January 23, 2013 8:07
To: ITSec; Sargent, Rob: SSC-SPC; Fournier, Denis: CIO-BI
Cc: Nadon, Rick: SSC-SPC; IT Security
Subject: Re: Request of logs from 16(2)(c)

Hi.

I believe Denis was going to stop by with a thumb drive.

After 8:30 would be good. Let me know.

Thanks
Frank

From: ITSec
Sent: Tuesday, January 22, 2013 06:29 PM Eastern Standard Time
To: Sargent, Rob: SSC-SPC; Fournier, Denis: CIO-BI; Tennian, Frank: SSC-SPC
Cc: Nadon, Rick: SSC-SPC; IT Security
Subject: RE: Request of logs from 16(2)(c)

Hi Rob,

The logs files attached in the original email 16(2)(c) Can you get the logs to us in another manner?

Thanks!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 2:59 PM
To: Fournier, Denis: CIO-BI; Tennian, Frank: SSC-SPC

Cc: Nadon, Rick: SSC-SPC; Hagarty, Richard: CIO-BI; IT Security
Subject: RE: Request of logs from 16(2)(c)

Hi Denis,

The IIS logs from the two 16(2)(c) servers 16(2)(c) are attached. 16(2)(c) is the main 16(2)(c) logon server.

There are 2 logs from 16(2)(c) .. That's the server we run part of our 16(2)(c) so I think it logs directly to one (or both) of those files.

<< File: 16(2)(c) >> << File 16(2)(c) >> << File: 16(2)(c) >>

Rob

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 2:29 PM
To: MDP Team
Cc: Nadon, Rick: SSC-SPC; Hagarty, Richard: CIO-BI; IT Security
Subject: Request of logs from 16(2)(c)

Hi all

We would need the 16(2)(c) logs from the time period of 16(2)(c) at 14h30 to 16(2)(c) at 18h00. This is for a case that we are working on.

Can you please advise when this could be done.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Hagarty, Richard: CIO-BI
Sent: Tuesday, January 22, 2013 19:49
To: Fournier, Denis: CIO-BI
Subject: Re: Request of logs from 16(2)(c)

Ok

Richard Hagarty
(613) 948-7283

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 07:20 PM Eastern Standard Time
To: Hagarty, Richard: CIO-BI; Sargent, Rob: SSC-SPC
Cc: IT Security
Subject: RE: Request of logs from 16(2)(c)

Richard, I have already fixed a time with Rob to go and get them tomorrow.

Thanks

Denis

From: ITSec
Sent: Tuesday, January 22, 2013 6:29 PM
To: Sargent, Rob: SSC-SPC; Fournier, Denis: CIO-BI; Tennian, Frank: SSC-SPC
Cc: Nadon, Rick: SSC-SPC; IT Security
Subject: RE: Request of logs from 16(2)(c)

Hi Rob,

The logs files attached in the original email 16(2)(c) Can you get the logs to us in another manner?

Thanks!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389

Government of Canada | Gouvernement du Canada

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 2:59 PM
To: Fournier, Denis: CIO-BI; Tennian, Frank: SSC-SPC
Cc: Nadon, Rick: SSC-SPC; Hagarty, Richard: CIO-BI; IT Security
Subject: RE: Request of logs from 16(2)(c)

Hi Denis,

The IIS logs from the two 16(2)(c) servers 16(2)(c) are attached. 16(2)(c) is the main 16(2)(c) logon server.

There are 2 logs from 16(2)(c). That's the server we run part of our 16(2)(c) so I think it logs directly to one (or both) of those files.

<< File: 16(2)(c) >> << File: 16(2)(c) >> << File: 16(2)(c) >>

Rob

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 2:29 PM
To: MDP Team
Cc: Nadon, Rick: SSC-SPC; Hagarty, Richard: CIO-BI; IT Security
Subject: Request of logs from 16(2)(c)

Hi all

We would need the 16(2)(c) logs from the time period of 16[2][c] at 14h30 to 16(2)(c) at 18h00. This is for a case that we are working on.

Can you please advise when this could be done.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389

Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 15:37
To: Fournier, Denis: CIO-BI
Subject: RE: Request of logs from 16(2)(c)

I'll let him know where the files are.

Best to call Frank before you come to make sure he's there .. the team has a breakfast meeting on Wednesday mornings.

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 3:34 PM
To: Sargent, Rob: SSC-SPC
Subject: Re: Request of logs from 16(2)(c)

Perfect, I willgo see him

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 03:20 PM Eastern Standard Time
To: Fournier, Denis: CIO-BI
Subject: RE: Request of logs from 16(2)(c)

19(1)

Frank Tennian should be in ... I can let him know where the files are.

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 3:19 PM
To: Sargent, Rob: SSC-SPC
Subject: Re: Request of logs from 16(2)(c)

I can maybe come by tomorrow morning with a memory stick

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 03:18 PM Eastern Standard Time
To: Fournier, Denis: CIO-BI
Subject: RE: Request of logs from 16(2)(c)

Do we have a share we can put them on? ..maybe somewhere on the 16[2][c] ?

The largest is 16(2)(c) The other two are 16(2)(c) and 16(2)(c) .. so I could email those if necessary

---

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 3:16 PM

To: Sargent, Rob: SSC-SPC
Subject: RE: Request of logs from 16(2)(c)

Hi Rob,

No they did not go through

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 3:15 PM
To: Fournier, Denis: CIO-BI
Subject: RE: Request of logs from 16(2)(c)

Gee ... 16(2)(c)

Please let me know if these get through. :-)

<< File: 16(2)(c) >> << File: 16(2)(c) >> << File: 16(2)(c) >>

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 3:11 PM
To: Sargent, Rob: SSC-SPC
Subject: RE: Request of logs from 16(2)(c)

Rob, because there are 16(2)(c) .. lol

16(2)(c)

Denis

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 2:59 PM
To: Fournier, Denis: CIO-BI; Tennian, Frank: SSC-SPC
Cc: Nadon, Rick: SSC-SPC; Hagarty, Richard: CIO-BI; IT Security
Subject: RE: Request of logs from 16(2)(c)

Hi Denis,

The IIS logs from the two 16(2)(c) servers 16(2)(c) are attached. 16(2)(c) is the main 16(2)(c) server.

There are 2 logs from 16(2)(c) .. That's the server we run part of our 16(2)(c) so I think it logs directly to one (or both) of those files.

<< File: 16(2)(c) >> << File: 16(2)(c) >> << File: 16(2)(c) >>

Rob

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 2:29 PM
To: MDP Team
Cc: Nadon, Rick: SSC-SPC; Hagarty, Richard: CIO-BI; IT Security
Subject: Request of logs from 16(2)(c)

Hi all

We would need the 16(2)(c) logs from the time period of 16(2)(c) at 14h30 to 16(2)(c) at 18h00. This is for a case that we are working on.

Can you please advise when this could be done.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Tennian, Frank: SSC-SPC
Sent: Wednesday, January 23, 2013 8:35
To: Fournier, Denis: CIO-BI
Subject: RE: Request of logs from 16(2)(c)

ok

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 8:35 AM
To: Tennian, Frank: SSC-SPC
Subject: RE: Request of logs from 16(2)(c)

Thanks Frank, I will be leaving in about 5 min.

Thanks

From: Tennian, Frank: SSC-SPC
Sent: Wednesday, January 23, 2013 8:07 AM
To: ITSec; Sargent, Rob: SSC-SPC; Fournier, Denis: CIO-BI
Cc: Nadon, Rick: SSC-SPC; IT Security
Subject: Re: Request of logs from 16(2)(c)

Hi.

I believe Denis was going to stop by with a thumb drive.

After 8:30 would be good. Let me know.

Thanks
Frank

From: ITSec
Sent: Tuesday, January 22, 2013 06:29 PM Eastern Standard Time
To: Sargent, Rob: SSC-SPC; Fournier, Denis: CIO-BI; Tennian, Frank: SSC-SPC
Cc: Nadon, Rick: SSC-SPC; IT Security
Subject: RE: Request of logs from 16(2)(c)

Hi Rob,

The logs files attached in the original email 16(2)(c) Can you get the logs to us in another manner?

Thanks!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Chief Informatics Office | Bureau de l'informatique

Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 2:59 PM
To: Fournier, Denis: CIO-BI; Tennian, Frank: SSC-SPC
Cc: Nadon, Rick: SSC-SPC; Hagarty, Richard: CIO-BI; IT Security
Subject: RE: Request of logs from 16(2)(c)

Hi Denis,

The IIS logs from the two 16(2)(c) servers 16(2)(c) are attached. 16(2)(c) is the main 16(2)(c) server.

There are 2 logs from 16(2)(c).. That's the server we run part of our 16(2)(c) so I think it logs directly to one (or both) of those files.

<< File: 16(2)(c) >> << File: 16(2)(c) >> << File: 16[2][c] >>

Rob

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 2:29 PM
To: MDP Team
Cc: Nadon, Rick: SSC-SPC; Hagarty, Richard: CIO-BI; IT Security
Subject: Request of logs from 16(2)(c)

Hi all

We would need the 16(2)(c) logs from the time period of 16(2)(c) at 14h30 to 16(2)(c) at 18h00. This is for a case that we are working on.

Can you please advise when this could be done.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique

Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 14:22
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR
Cc: IT Security
Subject: RE: Search on the 16(2)(c) and logs

Thanks Robert,

I will send an email to the messaging group

Denis

From: Edwards, Robert: SSC-SPC
Sent: Tuesday, January 22, 2013 2:15 PM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR
Cc: IT Security
Subject: RE: Search on the 16(2)(c) and logs

Denis, sorry but we don't process 16(2)(c) logs ... you will need to go directly to the messaging group.

Cheers,

Rob

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 2:08 PM
To: Edwards, Robert: SSC-SPC; NSG Security - Securité GSR
Cc: IT Security
Subject: RE: Search on the 16(2)(c) and logs

Hi Rob,

Just to check that you have received the request for the 16(2)(c) logs.

Thanks

Denis

From: Edwards, Robert: SSC-SPC
Sent: Tuesday, January 22, 2013 10:59 AM
To: Fournier, Denis: CIO-BI; NSG Security - Securité GSR
Cc: IT Security
Subject: RE: Search on the 16(2)(c) and logs

Thanks for the heads up...

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 10:47 AM
To: NSG Security - Securité GSR
Cc: IT Security
Subject: Search on the 16(2)(c) and logs

Hi,

I will be doing searches on the 16(2)(c) for a case we have received 16(2)(c)

Also is it possible to get the 16(2)(c) logs from the time period of 16(2)(c) at 14h30 to 16(2)(c) at 18h00. This is also for this case.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Begin, Denis: SSC-SPC (NCR-RCN)
Sent: Wednesday, January 23, 2013 11:01
To: Fournier, Denis: CIO-BI; MDP Team
Cc: IT Security
Subject: RE: 16(2)(c)

I'll handle this, I will disable it ASAP

From: Fournier, Denis: CIO-BI
Sent: Wednesday, January 23, 2013 11:01 AM
To: MDP Team
Cc: IT Security
Subject: 16(2)(c)

Hi,

Until we are able to clear up what happen in this event please 16(2)(c) 16(2)(c) from sending emails.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Gosselin, Andrée: CIO-BI
Sent: Thursday, November 8, 2012 14:26
To: Rivard, Karen: CIO-BI; Bullock, Sarah: CIO-BI; Corman, Christopher: CIO-BI; Cullen, Jennifer: CIO-BI
Cc: Hagarty, Richard: CIO-BI; Milito, Lora: CIO-BI
Subject: FW: BF TUES NOON- Bi-weekly Update to the DM / Mise à jour bi-hebdomadaire au SM

Attachments: FW: Bi-weekly Update to the DM / Mise à jour bi-hebdomadaire au SM; DM bi-weekly report template.doc

Can you please provide to me by 11am on Tuesday please.
Once Lora is back, it will be through Lora :)
Thanks,

Andrée

613-954-0101

From: Lamoureux, Marie-Eve: CIO-BI
Sent: Thursday, November 8, 2012 1:45 PM
To: Trudel, Susan: CIO-BI; Gosselin, Andrée: CIO-BI; Smith, Melissa: CIO-BI
Subject: BF TUES NOON- Bi-weekly Update to the DM / Mise à jour bi-hebdomadaire au SM

Good Afternoon,

FYA pls by Tuesday NOON (remember Monday is a holiday).

Below is what we provided last time:

FW: Bi-weekly Update to the DM...

Both "problems" will be removed so no need for anyone to update that. I will also remove the Cyberthreat item and will include that the DM binder was delivered to DMO Nov 5th.

Thanks.

From: Dunn, Danielle: SBTMS-SMTPE
Sent: Thursday, November 8, 2012 11:40 AM
To: Aitken, Jenifer: SBTMS-SMTPE; Dagenais, Eric: SBB-DGPE; Girouard, Marcie: CORP (NCR-RCN); James, Bill: OSB-BSF; Johnston, Alan: MC; Rehberg, Ilona: TB-DGT; Rinholm, Rick: CIO-BI; Wong, Harvey: SBTMS-SMTPE
Cc: Bastien, Therese: SBTMS-SMTPE; Bergeron, Denyse: SBB-DGPE; Cannalonga, Gisele: CORP; Deganutti, Lisa: CIO-BI; Eadie, Kimberly: SBTMS-SMTPE; Gaudreau, Gail: SBTMS-SMTPE; Joiner, Tanya: MC; Lajeunesse, Richard: IRSP-DGEIPS; Lepage, Diane: IMB-GI; OSB Corporate Secretariat - BSF Secrétariat ministériel: OSB-BSF; Pernot, Danielle: TB-DGT; Rudeen, Line: SBTMS-SMTPE
Subject: Bi-weekly Update to the DM / Mise à jour bi-hebdomadaire au SM

Good morning -- since Monday is a holiday, I'm sending the call-out 1 day earlier than usual so that you have the same # of days to complete.

Thank-you,
Danielle
****

Le français suit.

Hello/Bonjour,

DM bi-weekly report template.d...

I am writing to request your input for the ADM's Update to the Deputy Minister's report (from November 5 to 16, 2012, inclusive). The content should focus on policy and operational issues of interest to the DM. These may cover, for example: recent events, current status, next steps, concerns, and should be written in concise bullet-form language.

To further streamline this process, please submit your input using the attached *MS Word* template (please track changes = click under tools menu) or via email (please track changes = for additions use yellow highlight, for deletions use ~~strikethrough~~).

Please provide your input to me by **noon on Wednesday, November 14,** in order to allow enough time for the ADM to review the document and/or provide her comments.

Thank-you,

Je vous écris afin de solliciter la contribution de votre direction générale à la mise à jour du rapport au sous-ministre (du 5 au 16 novembre 2012, inclusivement). Le contenu devrait se concentrer sur les enjeux opérationnels et politiques d'intérêt pour le SM. Par exemple, peuvent contenir : les événements récents, le statut actuel, les prochaines étapes, les préoccupations, et devraient être rédigés dans un langage concis télescopique.

Afin d'améliorer le processus, nous vous demandons de nous soumettre votre contribution dans le document *MS Word* ci-joint (svp en activant la fonction de suivi des changements dans le menu Outils) ou encore simplement dans un courriel (en identifiant également les changements, par exemple les ajouts surlignés en jaune et les éléments enlevés ~~barrés~~).

Veuillez svp me faire parvenir votre contribution d'ici **midi mercredi le 14 novembre**, afin que la SMA puisse avoir suffisamment de temps pour revoir le document et/ou donner ses commentaires.

Merci,

Danielle Dunn
613-947-7710
danielle.dunn@ic.gc.ca

Rusenstrom, Sashsha: SBTMS-SMTPE

From: Deganutti, Lisa: CIO-BI
Sent: Thursday, November 8, 2012 13:32
To: Deganutti, Lisa: CIO-BI
Subject: FW: Bi-weekly Update to the DM / Mise à jour bi-hebdomadaire au SM

From: Deganutti, Lisa: CIO-BI
Sent: Tuesday, October 30, 2012 1:57 PM
To: Dunn, Danielle: SBTMS-SMTPE
Subject: Bi-weekly Update to the DM / Mise à jour bi-hebdomadaire au SM

Hi Danielle.
Input from CIO below, thanks.

Problems in the past week (both provided in the DM bi-weekly report:

1- As a follow up to our last week report to the DM, Bell (operators of Secure Channel) has informed us that on October 20th, Microsoft / Hotmail has adjusted the thresholds set previously to alleviate the issues related to the delivery of IC messages to Hotmail. In addition, Bell is monitoring the delivery of IC messages to Hotmail as a high priority. Based on the last report from Bell and according to their system logs, there has been no failure in delivery since the adjustment to the threshold. SSC will keep the status of this issue "open" for the weeks to come as a way to ensure that the adjustment made will meet IC's requirements adequately.

2- SSC continues to monitor the data centre generator. A faulty component in the fuel tank was identified and replaced. The faulty component allowed air to seep into the fuel line causing the generator to stall. A pressure test of the entire fuel system is being planned over the next week. To mitigate any risk of failure recurring until the pressure test is completed, the generator is started twice every week.

Planned IT Services interruptions for the next six months:

Email and BlackBerry email Shared Services maintenance - Saturday, November 3, 2012 from 08:00 to 16:00. There will be intermittent delays for email delivery of up to 15 minutes. BlackBerry PIN to PIN will be available at all times.

Remote Access Service Monthly Security Patches - originally scheduled for Tuesday, October 30, 2012 is postponed at the request of SITT. Emergency Telecom is a critical function for SITT in their response to hurricane Sandy and IC Remote access is an essential tool for SITT staff in Ontario and Québec. The work is tentatively being rescheduled to next Tuesday, November 6th.

Other:

Q2 IT Report (July - September) will be provided by November 2nd.

Cyber Threat Evaluation Centre (CTEC) Alert - Distributed Denial of Service (DDOS):
Departments have been made aware that a Distributed Denial of Service (DDoS) operation against the GC is scheduled to run from November 3rd to November 15th, 2012. GoC monitoring suggests that a number of departments (approx. 40) might already be impacted. We have confirmed that there is currently no notable activities observed for Industry Canada. CTEC and Shared Services Canada (SSC) are reviewing and monitoring the situation and have been keeping departments informed in a timely manner. Furthermore, IC and SSC have heightened their monitoring since last Friday

and have established the necessary protocols. 21(1)(a),21(1)(b)

21(1)(a),21(1)(b)

Lisa Deganutti
Executive Assistant to the CIO | Adjointe exécutive pour le Chef d'informatique
Chief Informatics Office | Bureau de l'informatique
Industry Canada | Industrie Canada
235 rue Queen Street, Ottawa ON K1A 0H5
Lisa.Deganutti@ic.gc.ca
Telephone | Téléphone 613-954-3570
Government of Canada | Gouvernement du Canada

From: Dunn, Danielle: SBTMS-SMTPE
Sent: Friday, October 26, 2012 8:00 AM
To: Aitken, Jenifer: SBTMS-SMTPE; Dagenais, Eric: SBB-DGPE; Girouard, Marcie: CORP (NCR-RCN); James, Bill: OSB-BSF; Johnston, Alan: MC; Rehberg, Ilona: TB-DGT; Rinholm, Rick: CIO-BI; Wong, Harvey: SBTMS-SMTPE
Cc: Bastien, Therese: SBTMS-SMTPE; Bergeron, Denyse: SBB-DGPE; Cannalonga, Gisele: CORP; Deganutti, Lisa: CIO-BI; Eadie, Kimberly: SBTMS-SMTPE; Gaudreau, Gail: SBTMS-SMTPE; Joiner, Tanya: MC; Lajeunesse, Richard: IRSP-DGEIPS; Lepage, Diane: IMB-GI; OSB Corporate Secretariat - BSF Secrétariat ministériel: OSB-BSF; Pernot, Danielle: TB-DGT; Rudeen, Line: SBTMS-SMTPE
Subject: Bi-weekly Update to the DM / Mise à jour bi-hebdomadaire au SM

Le français suit.
<< File: DM bi-weekly report template.doc >>
Hello/Bonjour,

I am writing to request your input for the ADM's Update to the Deputy Minister's report (from October 9 to 19, 2012). The content should focus on policy and operational issues of interest to the DM. These may cover, for example: recent events, current status, next steps, concerns, and should be written in concise bullet-form language.

To further streamline this process, please submit your input using the attached *MS Word* template (please track changes = click under tools menu) or via email (please track changes = for additions use yellow highlight, for deletions use ~~strikethrough~~).

Please provide your input to me by **noon on Wednesday, October 31,** in order to allow enough time for the ADM to review the document and/or provide her comments.

Thank you for your cooperation.

Je vous écris afin de solliciter la contribution de votre direction générale à la mise à jour du rapport au sous-ministre (du 9 au 19 octobre 2012). Le contenu devrait se concentrer sur les enjeux opérationnels et politiques d'intérêt pour le SM. Par exemple, peuvent contenir : les événements récents, le statut actuel, les prochaines étapes, les préoccupations, et devraient être rédigés dans un langage concis télescopique.

Afin d'améliorer le processus, nous vous demandons de nous soumettre votre contribution dans le document *MS Word* ci-joint (svp en activant la fonction de suivi des changements dans le menu Outils) ou encore simplement dans un courriel (en identifiant également les changements, par exemple les ajouts surlignés en jaune et les éléments enlevés ~~barrés~~).

Veuillez svp me faire parvenir votre contribution d'ici **midi mercredi le 31 octobre**, afin que la SMA puisse avoir suffisamment de temps pour revoir le document et/ou donner ses commentaires.

Merci de votre collaboration.

Danielle Dunn
613-947-7710
danielle.dunn@ic.gc.ca

BI-WEEKLY UPDATE TO THE DEPUTY MINISTER
Small Business, Tourism and Marketplace Services
(Weeks of November 5 to 16, 2012)

SMALL BUSINESS

Issue (Sub-title)

Content should focus on key policy and operational issues that may be of interest to the DM. These may cover for instance: recent events, current status, next steps, concerns, and should be written in concise bullet-form language.

Example:
Small Business Action Plan:
Meeting with Industry representatives took place on March XX, 2011. Issues from the exchange include X, Y, Z. Another meeting is planned for June 2011. A report on this meeting will be forwarded to your office by March 20, 2011.

TOURISM

Issue (Sub-title)

Content should focus on key policy and operational issues that may be of interest to the DM. These may cover for instance: recent events, current status, next steps, concerns, and should be written in concise bullet-form language.

MARKETPLACE SERVICES

Issue (Sub-title) – This section includes OSB, MC, CC and IR.

The content should focus on key policy and operational issues that may be of interest to the DM while respecting constraints associated with the OSB and CC. These may cover for instance: recent events, current status, next steps, concerns, and should be written in concise bullet-form language.

Investment Review

Please see weekly reports to the Minister for details on specific cases. We would be pleased to brief you on individual cases, if required.

INFORMATION MANAGEMENT / INFORMATION TECHNOLOGY

Issue (Sub-title) – This section includes CIO and IMB

Content should focus on key policy and operational issues that may be of interest to the DM. These may cover for instance: recent events, current status, next steps, concerns, and should be written in concise bullet-form language.

OTHERS (FINANCIAL AND HUMAN RESOURCES)

CIO Branch update to ADMO (SBTMS) for October 26 to Nov 9, 2012

2 Week Look-ahead

Upcoming Key meetings within CIO:

SAM Steering committee meeting- November 8th
POC (Project Oversight Committee)- November 13th (No agenda items to date)
CIOC (CIO Council)- November 14th

Anything else that is coming up from within the branch that ADM needs to have on her radar

GCWCC update:
SBTMS has surpassed their target! (Total to date: $122,267.72 out of $117,203.00 =104%). 21(1)(a),21(1)(b)
21(1)(a),21(1)(b)

Cyber Threat Evaluation Centre (CTEC) Alert - Distributed Denial of Service (DDOS):
Departments have been made aware that a Distributed Denial of Service (DDoS) operation against the GC is scheduled to run from November 3rd to November 15th, 2012. GoC monitoring suggests that a number of departments (approx. 40) might already be impacted. We have confirmed that there is currently no notable activities observed for Industry Canada. CTEC and Shared Services Canada (SSC) are reviewing and monitoring the situation and have been keeping departments informed in a timely manner.

21(1)(a),21(1)(b)

The Deputy Minister is planning a video conference with Executives from across the country on November 14th. The boardrooms for this meeting have been reserved and testing of the video conferencing functionality completed. Also, a meeting chaired by CMB was held on November 1st to discuss logistics and agenda.

Based on the DM's request at the October 31 Management Committee, we are planning to send a short deck to him by the end of next week that will facilitate a discussion on the management of IT at Industry Canada and the department's forward strategy.

Problems in the past week (both provided in the DM bi-weekly report:

Nothing to report

Planned IT Services interruptions for the next six months (Provided in DM bi-weekly report):

Email and BlackBerry email Shared Services maintenance - Saturday, November 3, 2012 from 08:00 to 16:00. There will be intermittent delays for email delivery of up to 15 minutes. BlackBerry PIN to PIN will be available at all times.

CIO Branch update to ADMO (SBTMS) for October 26 to Nov 9, 2012

Remote Access Service Monthly Security Patches – Tuesday, November 6, 2012 from 20:00 to midnight. Remote access will not be available. This was postponed from Tuesday, October 30, 2012 at the request of SITT. Emergency Telecom is a critical function for SITT in their response to hurricane Sandy and IC Remote access was deemed an essential tool for SITT staff in Ontario and Québec.

Lacroix, Lise: SBTMS-SMTPE

From: Gosselin, Andrée: CIO-BI
Sent: Thursday, November 8, 2012 9:53
To: Cullen, Jennifer: CIO-BI
Cc: Hagarty, Richard: CIO-BI
Subject: Re: BF Thursday noon - 2WLA

Thanks Jennifer!

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, November 08, 2012 09:50 AM
To: Gosselin, Andrée: CIO-BI
Cc: Hagarty, Richard: CIO-BI
Subject: FW: BF Thursday noon - 2WLA

Hi Andrée,

Understanding that it was probably Richard who provided the information on the Cyber Threat Evaluation Centre (CTEC) Alert - Distributed Denial of Service (DDOS), here is an update:

****
Cyber Threat Evaluation Centre (CTEC) Alert - Distributed Denial of Service (DDOS):

Government of Canada and Industry Canada continue to be prepared for and respond to the Distributed Denial of Service (DDoS) operation against the GC that is scheduled to run from November 3rd to November 15th, 2012. GoC monitoring has detected activity consistent with DDOS attempts, however there has been no major impact on the GC by any of the observed activity to date. Further, we have confirmed that there is currently no notable activities observed for Industry Canada. CTEC and Shared Services Canada (SSC) continue to review and monitor the situation and have been keeping departments informed in a timely manner. Furthermore, IC and SSC continue to heighten their monitoring and have established the necessary protocols. Latest reports indicate that the focus will be provincial level targets.

****

Thank you,
Jennifer

From: Gosselin, Andrée: CIO-BI
Sent: Monday, November 5, 2012 11:41 AM
To: Rivard, Karen: CIO-BI; Bullock, Sarah: CIO-BI; Cullen, Jennifer: CIO-BI; Corman, Christopher: CIO-BI
Subject: Fw: BF Thursday noon - 2WLA

FYI-FYA
Please provide to me at the latest by 10 am Thursday so I can review...
Andrée

From: Lamoureux, Marie-Eve: CIO-BI
Sent: Monday, November 05, 2012 11:38 AM
To: Trudel, Susan: CIO-BI; Gosselin, Andrée: CIO-BI; Smith, Melissa: CIO-BI
Cc: Milito, Lora: CIO-BI
Subject: BF Thursday noon - 2WLA

Good Morning,

Please review and advise of any changes (**highlighted pls**) for the period Nov 12 to 23 **before Thursday noon**. Below is what Lisa is proposing to send this week:

<<2WLA Nov 9.doc>>

This is what was submitted last time:

<<2WLA Nov 2.doc>>

Please note: for any RGBB updates, please include the same sentence I have added.

Please note: ADM has emphasized the importance of including meetings in this report. **If there are any meetings that you attend that you feel are significant enough that ADM should be made aware of, please include them.**

Merci,

Marie-Eve Lamoureux
Executive Assistant

Planning and Customer Relations Division

Chief Informatics Office

Small Business, Tourism and Marketplace Services Industry Canada

235 Queen Street, Ottawa ON K1A 0H5

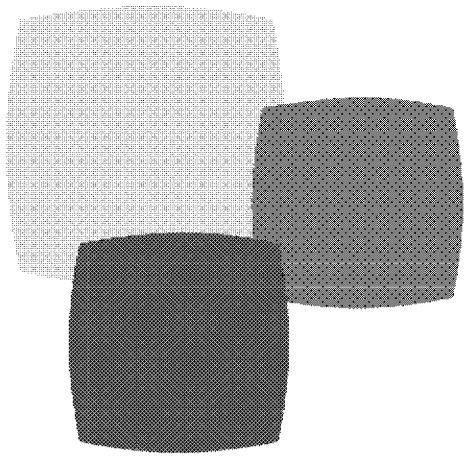
Telephone | Téléphone 613-952-7414
Facsimile | Télécopieur 613-941-4615
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

IT Security Incident Management

IT Security Incident Response Plan

"Anonymous" Threat

October 2012 (V1)



Canada

IT Security Incident Response Plan

- **“Anonymous” Threat**
- **GC Preparation and Response**
- **IC Preparation and Response**
- **Reporting**
- **Communications**

IT Security Incident Response Plan

- **Anonymous Threat Situation**
  - GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous is planning against the GC.
  - The goal appears to be disruption of GC sites and services.
  - The operation is scheduled to run 3 to 15 November 2012.
- **Observations to date**
  - Traffic that is related to this DDoS attack has been observed as early as 22 October 2012, 16(2)(c)
  - There is no indication that IC is being affected/is among those departments affected.
  - However, the scope and level of activity may increase as the targeted date range approaches.
- 16(2)(c),21(1)(a),21(1)(b)

Canada

IT Security Incident Response Plan

- **GC Preparation and Response**
  - GC-CTEC is **coordinating** the incident response and the threat evaluation for this event.
  - GC-CTEC is informing its constituency.
  - Shared Services Canada Operations Centre will be **leading the mitigation effort** with the service provider 16(2)(c)
  - Departments are to report any outages or suspicious network activities that require mitigation by contacting both:
    - SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
    - GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca.
  - Mitigation typically involves 16(2)(c),21(1)(b)

16(2)(c),21(1)(b)

IT Security Incident Response Plan

- **IC Preparation**
  - **IT Security to identify key response personnel.**
  - **IT Security is working to identify IC's critical external facing applications and their related IP addresses.**
  - **Provide this information to IC and SSC (IC) responders.**
  - **Inform Service Management & Service Desk of potential threat to services.**
  - **Service Management/Service Desk to inform clients.**
  - **IT Security to provide regular updates to CIO management.**

IT Security Incident Response Plan

- **IC Response**
  - **IT Security is coordinating the IC incident response.**
  - **SSC (IC)'s Network Services Group/Network Security is leading the mitigation effort and have coordinated their monitoring with the SSC (IC) middleware group, and have heightened monitoring and counter measure.**
  - **the event of an attack, SSC (IC) will implement appropriate measures, then advise IT Security.**
  - **CIO/ASD to monitor critical services (Francine and Frankie – identify critical apps, and related IP addresses, report to ITS/SM**
  - **Service Management (Service Desk) to inform clients.**

IT Security Incident Response Plan

- **Reporting**
  - Departments are to report any outages or suspicious network activities that require mitigation by contacting both:
    - SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
    - GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca.
  - SSC (IC) reports to ITS and SSC Operations Centre & GC-CTEC
  - Francine & Frankie report to ITS
  - ITS reports to Service Management & Service Desk
  - ITS reports to IC management.

Reporting/Communications

- Departments ((i.e. SSC(IC)) are to report any outages or suspicious network activities that require mitigation by contacting both:
  - SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
  - GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca.
- SSC (IC) reports to ITS and SSC Operations Centre & GC-CTEC
- ITS informs to Service Management & Service Desk
- ITS informs/consults to IC/CIO management and DSO.

IT Security Incident Response Plan

- **Communications**

Contact Information

IC/CIO/IT Security
IC/CIO/ASD
IC/CIO/Service Management
IC/CIO/Service Desk
SSC (IC) NSG/Sec
SSC (IC) Midrange
GC-CTEC
GC-SSC-Operations Centre

Q&A

- Questions?

Thank you!

Canada

IT Security Incident Response Plan

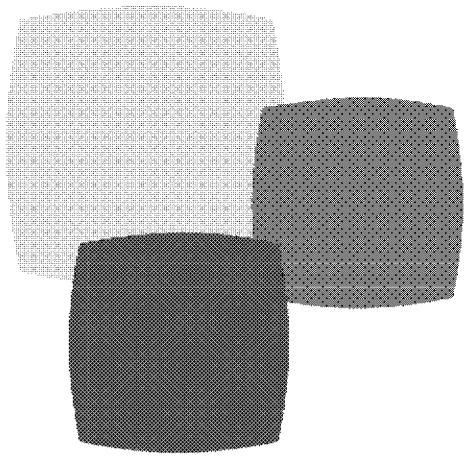
- **Anonymous Threat**
- **GC Mitigation**
- **IC Mitigation**
- **Reporting**
- **Communications**

IT Security Incident Management

IT Security Incident Response Plan

"Anonymous" Cyber Threat

October 2012 (V1)



Canada

Introduction

- **“Anonymous” Threat**
- **GC Preparation and Response**
- **IC Preparation and Response**
- **Reporting/Communications**
- **Contact Information**

"Anonymous" Threat

- **Background**
  - GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous is planning against the GC.
  - The goal appears to be disruption of GC sites and services.
  - The operation is scheduled to run 3 to 15 November 2012.
- **Observations to date**
  - Traffic that is related to this DDoS attack has been observed as early as 22 October 2012, 16(2)(c)
  - There is no indication that IC is being affected/is among those departments affected.
  - However, the scope and level of activity may increase as the targeted date range approaches.
- 21(1)(a),21(1)(b)

GC Preparation and Response

- GC-CTEC is **coordinating** the incident response and the threat evaluation for this event.
- GC-CTEC is informing its constituency.
- Shared Services Canada (SSC) Operations Centre will be **leading the mitigation effort** with the service provider 16(2)(c) .
- Departments are to report any outages or suspicious network activities that require mitigation by contacting both GC-CTEC and SSC Operations Centre.
- Mitigation typically involves 16(2)(c),21(1)(b)

16(2)(c),21(1)(b)

IC Preparation and Response

- **Key response personnel:**
  - IC/CIO/IT Security
  - IC/CIO/Service Management
  - IC/CIO/Service Desk
  - SSC (IC) NSG/Sec with support from SSC (IC) Middleware

- **IC's critical external facing applications:**
  - To be Identified

IC Preparation and Response

- **IC Response Roles**
  - IT Security is coordinating the IC incident response.
  - Service Desk prepare for client issue reporting.
  - Service Management provides communications.
  - IT Security to provide regular updates to IC/CIO management and DSO

IC Preparation and Response

- **SSC (IC) Response Roles**
  - SSC (IC)'s Network Services Group/Network Security is leading the mitigation effort and have coordinated their monitoring with the SSC (IC) middleware group, and have heightened monitoring and counter measure.
  - In the event of an attack, SSC (IC) will implement appropriate measures, then advise IT Security, and GC-CTEC and SSC Operations Centre.

Contact Information

IC/CIO/IT Security - Jennifer Cullen

16(2)(c) **(W) 613-948-4029, BB** 15(1)

BB PIN 18(a)

IT Security Conference Bridge,

IC/CIO/Service Management

IC/CIO/Service Desk

SSC (IC) NSG/Sec

SSC (IC) Midrange

GC-CTEC

GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca or (613)991-2300.

GC-SSC-Operations Centre

SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca.

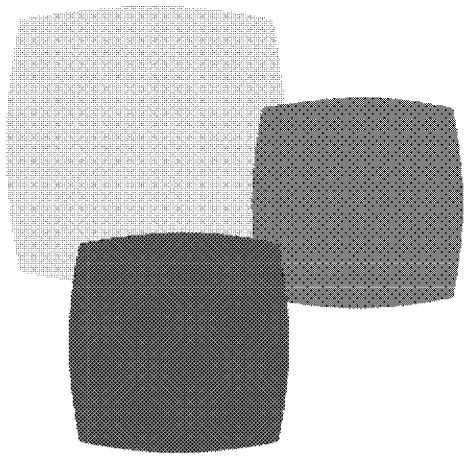
Canada

IT Security Incident Management

IT Security Incident Response Plan

"Anonymous" Cyber Threat

October 2012 (V3)



Canada

Introduction

- **“Anonymous” Threat**
- **GC Preparation and Response**
- **IC Preparation and Response**
- **Reporting/Communications**
- **Contact Information**

"Anonymous" Threat

- **Background**
  - GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous is planning against the GC.
  - The goal appears to be disruption of GC sites and services.
  - The operation is scheduled to run 3 to 15 November 2012.
- **Observations to date**
  - Traffic that is related to this DDoS attack has been observed as early as 22 October 2012, 16(2)(c)
  - There is no indication that IC is being affected/is among those departments affected.
  - However, the scope and level of activity may increase as the targeted date range approaches.
- 21(1)(a),21(1)(b)

GC Preparation and Response

- GC-CTEC is **coordinating** the incident response and the threat evaluation for this event.
- GC-CTEC is informing its constituency.
- Shared Services Canada (SSC) Operations Centre will be **leading the mitigation effort** with the service provider 16(2)(c) .
- Departments are to report any outages or suspicious network activities that require mitigation by contacting both GC-CTEC and SSC Operations Centre.
- Mitigation typically involves 16(2)(c),21(1)(b)

16(2)(c),21(1)(b)

Canada

IC Preparation and Response

- **Key response personnel:**
  - IC/CIO/IT Security
  - IC/CIO/Service Management
  - 16(2)(c)
  - IC/CIO/Web Service Centre
  - IC/CIO/Service Desk
  - SSC (IC) NSG/Sec with support from SSC (IC) Middleware

- **IC's critical external facing applications:**
  - To be Identified

IC Preparation and Response

- **IC Response Roles**
  - IT Security is coordinating the IC incident response.
  - Web Service Centre and Service Desk track and manage client issue reporting.
  - 16(2)(c)
  - Service Management provides communications.
  - IT Security to provide regular updates to IC/CIO management and DSO

IC Preparation and Response

- **SSC (IC) Response Roles**
  - SSC (IC)'s Network Services Group/Network Security is leading the mitigation effort and have coordinated their monitoring with the SSC (IC) middleware group, and have heightened monitoring and counter measure.
  - In the event of an attack, SSC (IC) will implement appropriate measures then advise 16(2)(c) IT Security, and GC-CTEC and SSC Operations Centre.

Contact Information

IC/CIO/IT Security - Jennifer Cullen

16(2)(c) **(W) 613-948-4029, BB** 15(1) ,

BB PIN 18(a)

IT Security Conference Bridge,

IC/CIO/Service Management

16(2)(c)

IC/CIO/Web Service Centre

IC/CIO/Service Desk

SSC (IC) NSG/Sec

SSC (IC) Midrange

GC-CTEC

GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca or (613)991-2300.

GC-SSC-Operations Centre

SSC Operations Duty Analyst 819-956-4806 or

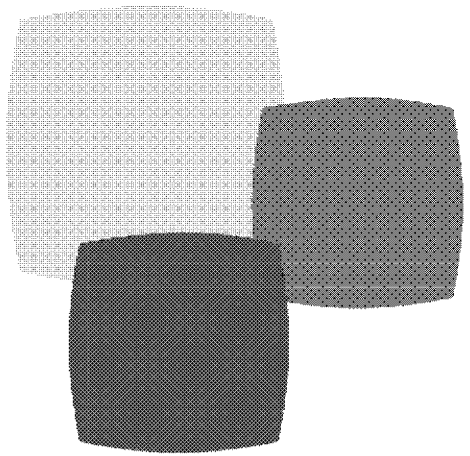
Canada

IT Security Incident Management

IT Security Incident Response Plan

"Anonymous" Cyber Threat

October 2012 (V4)



Canada

Introduction

- **“Anonymous” Threat**
- **GC Preparation and Response**
- **IC Preparation and Response**
- **Reporting/Communications**
- **Contact Information**

"Anonymous" Threat

- **Background**
  - GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous is planning against the GC.
  - The goal appears to be disruption of GC sites and services.
  - The operation is scheduled to run 3 to 15 November 2012, possibly until 30 November 2012.
- **Observations to date**
  - Traffic that is related to this DDoS attack has been observed as early as 22 October 2012, 16(2)(c)
  - There is no indication that IC is being affected/is among those departments affected.
  - However, the scope and level of activity may increase as the targeted date range approaches.
- 21(1)(a),21(1)(b)

Canada

GC Preparation and Response

- GC-CTEC is **coordinating** the incident response and the threat evaluation for this event.
- GC-CTEC is informing its constituency.
- Shared Services Canada (SSC) Operations Centre will be **leading the mitigation effort** with the service provider 16(2)(c).
- Departments are to report any outages or suspicious network activities that require mitigation by contacting both GC-CTEC and SSC Operations Centre.
- Mitigation typically involves 16(2)(c),21(1)(b)

16(2)(c),21(1)(b)

Canada

IC Preparation and Response

- **Key response personnel:**
  - IC/CIO/IT Security
  - IC/CIO/Service Management
  - 16(2)(c)
  - IC/CMB/Web Service Centre
  - IC/CIO/Service Desk
  - IC/CMB/Corporate Communications
  - SSC (IC) NSG/Sec in coordination with SSC (IC) Midrange

- **IC's critical external facing applications:**
  - To be Identified

IC Preparation and Response

- **IC Response Roles**
  - IT Security is coordinating the IC incident response.
  - Web Service Centre and Service Desk track and manage client issue reporting.
  - 16(2)(c) to track and manage related incidents, work with SSC/NSG/Sec and SSC/Midrange. Inform application/service custodian/owner, Web Service Centre, and IT Security.
  - Service Management provides communications.
  - CMB/Corporate Communications provides communications.
  - IT Security to provide regular updates to IC/CIO Senior Management and DSO
    - Rick Rinholm, Kelly Acton, Patti Pomeroy, Diane Basque Spickett, Andrée Gosselin, and Kim Thompson.

IC Preparation and Response

- **SSC (IC) Response Roles**
  - SSC (IC)'s Network Services Group/Network Security is leading the mitigation effort and have coordinated their monitoring with the SSC (IC) Midrange group, and have heightened monitoring and counter measure.
  - In the event of an attack, SSC (IC) will implement appropriate measures then advise 16(2)(c), IT Security, and GC-CTEC and SSC Operations Centre.

Contact Information

IC/CIO/IT Security

Jennifer Cullen

(w) 613-948-4029, (BB) 15(1) **(PIN)** 18(a) 16(2)(c)

IT Security Conference Bridge, 18(a) **or** 18(a) 18(a) **, Conference** 18(a),21(1)(b)

IC/CIO/Service Management

Karen Rivard (w) 613-946-0515,

Suzanne Lord (w) 613-952-1664,

CIO IT Problem Manager 16(2)(c) **,**

see PCRD Contact Card for further details.

Canada

Contact Information cont.

16(2)(c)

IC/CIO/Content Management Systems

Frankie Morin, (w) 613-952-0146, frankie.morin@ic.gc.ca.

IC/CMB/Web Service Centre

613-954-5031 or 1-800-328-6189,

16(2)(c)

Alt. Susan Shapiro, (w) 613-952-5480, susan.shapiro@ic.gc.ca.

Canada

Contact Information cont.

IC/CIO/Service Desk

Denis Parisien, (w) 613-952-7802 (BB) 613-899-2401 (PIN)

18(a)

Johnny Francis, (w) 613-946-6953, (BB) 613-222-6826 (PIN)

18(a)

CMB/Corporate Communications

Denis Dummer, (w) 613-992-3552, denis.dummer@ic.gc.ca.

Canada

Contact Information cont.

SSC (IC) NSG/Sec

Robert Edwards: (w) 613-948-6126, (BB) 613-325-3249
NSG Sec Pager: 613-368-0342,
NSG Voice Mail: 954-6422.

NSG Ops Pager: 613-239-7968,
NSG Ops Cel: 613-298-6310,
NSG Ops VM: 613-957-4170,
NSG Eng Pager: 613-954-6422.

SSC (IC) Midrange

Via SSC (IC) NSG/Sec.

Contact Information cont.

GC-CTEC

GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca or (613)991-2300.

GC-SSC-Operations Centre

SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Hagarty, Richard: CIO-BI
Sent: Tuesday, January 22, 2013 10:19
To: Rinholm, Rick: CIO-BI
Cc: Hagarty, Richard: CIO-BI; Acton, Kelly: CIO-BI; Gosselin, Andrée: CIO-BI; ITSec
Subject: RE: 16(2)(c)

Hi Rick,

Please note that 16(2)(c) since 5pm last night. We are currently awaiting confirmation that they have been implemented.

We have conducted a high-level analysis of the detail data coming from the suspicious email header. Our analysis suggests that 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

The situation should be contained at this point 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b) 21(1)(a),21(1)(b)

21(1)(b),21(1)(a)

I will follow-up with a situational report during the day if there is more to this incident than what we typically see.

Thank you and have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

From: Hagarty, Richard: CIO-BI
Sent: Tuesday, January 22, 2013 8:17 AM
To: Rinholm, Rick: CIO-BI; Nadon, Rick: SSC-SPC; Bernard, Mario: CIO-BI
Subject: RE: 16(2)(c)

We will take care of the it. Have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

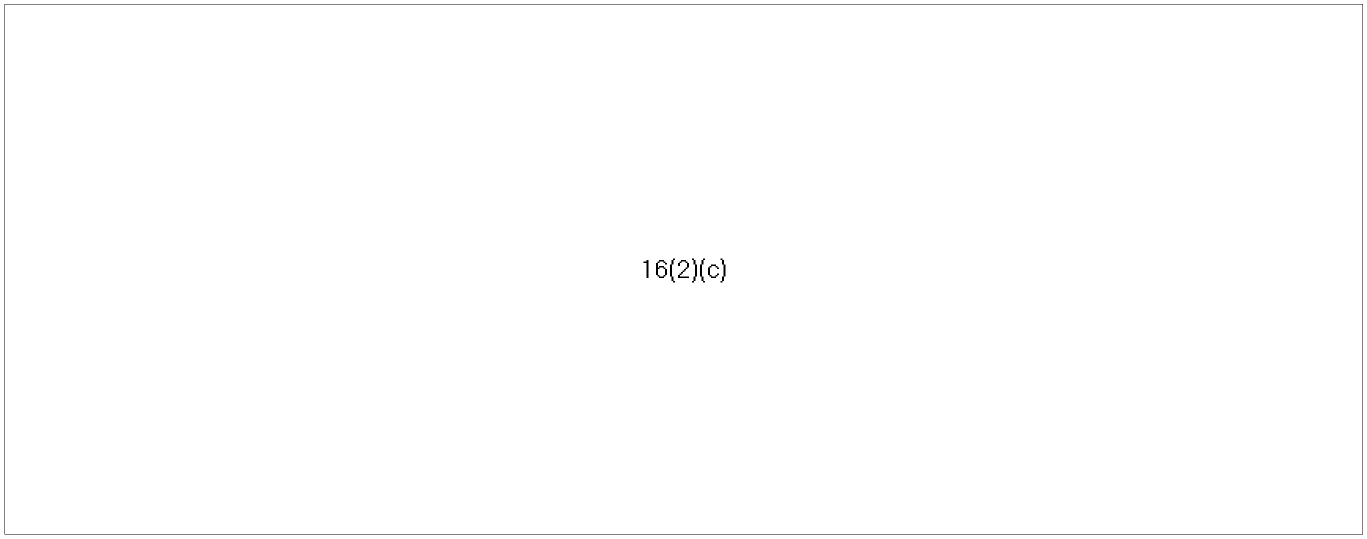
From: Rinholm, Rick: CIO-BI
Sent: Monday, January 21, 2013 8:37 PM
To: Hagarty, Richard: CIO-BI; Nadon, Rick: SSC-SPC; Bernard, Mario: CIO-BI
Subject: Fw: 16(2)(c) !!

FYA as required.

Rick

From: Stewart, Iain: SPS
Sent: Monday, January 21, 2013 07:00 PM
To: Rinholm, Rick: CIO-BI; Novak, Rione: SPS; Altherr, Nathalie: SPS
Subject: FW: 16(2)(c)

rick - this email is pretty tricky - looks alot like the real one you guys send



Lacroix, Lise: SBTMS-SMTPE

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 10:44
To: Fournier, Denis: CIO-BI; ITSec; Messaging Engineering
Cc: IT Security
Subject: RE: Possible Phishing Attempt - 16(2)(c)

Maybe you're right. I do see those messages on the outgoing gateway too.

In addition to 19(1) the only other user I see with direct mailbox rights is 19(1):

From: Fournier, Denis: CIO-BI
Sent: Tuesday, January 22, 2013 10:23 AM
To: Sargent, Rob: SSC-SPC; ITSec; Messaging Engineering
Cc: IT Security
Subject: RE: Possible Phishing Attempt - 16(2)(c)

21(1)(a),21(1)(b)

Also you say that there are a lot of NDR's. Sorry not sure what it means.. (maybe not delivered?)

Can you also give us the users that would have the rights to send from this account. In the properties of this account we have 19(1) as manager of account.

Thanks

Denis

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 8:16 AM
To: Sargent, Rob: SSC-SPC; ITSec; Messaging Engineering; NSG Security - Securité GSR
Subject: RE: Possible Phishing Attempt - 16(2)(c)

Recipients list is attached.

Interesting attack ... looks like they used the address '16(2)(c)' as a spoofed sender address, which is why so many NDRs came back to us from internet email servers.

<< File: 16(2)(c) >>

From: Sargent, Rob: SSC-SPC
Sent: Tuesday, January 22, 2013 8:00 AM
To: ITSec; Messaging Engineering; NSG Security - Securité GSR
Subject: RE: Possible Phishing Attempt - 16(2)(c)

16(2)(c)

Recipients list to follow.

From: ITSec
Sent: Monday, January 21, 2013 4:57 PM
To: Messaging Engineering; NSG Security - Securité GSR
Subject: Possible Phishing Attempt - 16(2)(c)

Messaging Engineering

Possible Phishing email.

Please 16(2)(c) advise who has received this email:

" 16(2)(c) !"

Please also confirm the sender address.

NSG

16(2)(c) >>

Thanks,
Jen

Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Tuesday, January 22, 2013 11:14
To: Brabant, Mathieu: CIO-BI
Subject: ITSINC-2013-016 - Possible Internal Phishing email

Hi Mathieu,

In response to a possible Phishing email that may have originated internally, could we please get a report on the SEP activity for all of the STRATEGIC POLICY SECTOR (SPS) and the INDUSTRY SECTOR (IC).

Thanks,
Jen

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: 19(1)
Sent: Thursday, January 24, 2013 10:37
To: Fournier, Denis: CIO-BI
Subject: RE:

Wow! Did you get the stuff I sent?

From: Fournier, Denis: CIO-BI
Sent: Thursday, January 24, 2013 10:32 AM
To: 19(1)
Subject:

Hi 19(1) these are the emails that were sent from the account. You can look at them but do not click on the links

<< Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >> << Message: 16(2)(c) >>

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

CTEC GC IT IMP Report Number: CE2013-1674 **Industry Canada IT Security Incident Number: ITSINC-2013-016**			
1.0 Reporting Entity			
Name of organization:	Industry Canada		
2.0 Contact Information			
First name:	Jennifer	Initials:	
Last name:	Cullen	Position:	Team Lead, IT Security, IC
Phone:	(613) 948-4029	Cell:	18(a)
Pager:	( )	Fax:	(613) 946-3367
Email:	Jennifer.cullen@ic.gc.ca		
Office address:	235 Queen St., Ottawa.		
3.0 Incident Description and Impact			
Date and time of incident:	(date, time, and time zone) 2013-01-20 19:25		
Location of site affected by incident:			
(if more than one site is affected, please list) Industry Canada, 235 Queen St., Ottawa.			
Estimated impact:	Unknown at this time.		
Incident duration:	(if incident is over; otherwise, report 'ongoing') The situation is contained, yet ongoing.		
Estimated number of systems affected:	unknown		

CTEC GC IT IMP Report Number: CE2013-1674 **Industry Canada IT Security Incident Number: ITSINC-2013-016**	
Percentage of departmental systems affected:	Unknown at this time.

Brief description of the incident:

2013-01-21 16:40 - IT Security received 5 incident tickets regarding SPAM/Phishing emails with Subject line: 16(2)(c)

2013-01-22 10:23 - IT Security determines, based on the header information of one of the sample emails, the SPAM/Phishing emails originated from the 16(2)(c) email system, using an internal email resource as the sender.

2013-01-22 10:44 – Two IC employees have access to this email resource. A technician was dispatched to the desktops of these 2 users. On one desktop, 16(2)(c) was discovered. IT Security has requested 16(2)(c)

2013-01-22 10:47 – In another line of investigation, IT Security 16(2)(c) 16(2)(c)

2013-01-23 – Analysis of the 16(2)(c) 16(2)(c)

2013-01-25 16:30 – In light of the evidence found so far in our analysis, management has decided to 16(2)(c) 16(2)(c) This will provide the necessary time for IC and SSC/Economic Portfolio to conduct a more detailed analysis in order to provide Industry Canada with proper mitigation plan.

Actions taken:

(include date and time if possible)

16(2)(c)

Supporting documents attached:

(describe if any)

4.0 Status of Mitigation Actions

Mitigation details to date:	(list any actions that have been taken to mitigate

CTEC GC IT IMP Report Number: CE2013-1674 Industry Canada IT Security Incident Number: ITSINC-2013-016	
	incident and by whom) 16(2)(c)
Results of mitigation:	
Additional assistance required?	NO
5.0 Incident Type	
Malicious code	SPAM/Phishing
Known vulnerability exploit	*n/a*
System compromise	16(2)(c)
Data compromise	*n/a*
Denial of service	*n/a*
Access violation	successful unauthorized access
Accident or error	*n/a*
Other or unknown	*n/a*
6.0 Systems Affected	
Network zone affected	16(2)(c)
Type of system affected	16(2)(c)
Operating system (specify version)	n/a

CTEC GC IT IMP Report Number: CE2013-1674 **Industry Canada IT Security Incident Number: ITSINC-2013-016**	
Protocols or services	n/a
Application	16(2)(c)

7.0 Apparent Origin of Incident or Attack

Source IP and port:	n/a	Protocol:	n/a
URL:	n/a	Malware:	n/a

Note: Electronic data exchange details are available from the CTEC.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 10:41
To: Gosselin, Andrée: CIO-BI
Subject: "Anonymous" DDoS Threat Update #2

Hi Andrée.

Could I please get some advice and direction from you? I think it appropriate to provide updates to Mr Rinholm and CIO Senior Management even if there is no change to IC's environment as a result of the DDoS threat, however, I am unsure at what frequency I should provide updates when there is no change. I would appreciate your feedback?

This morning's message would be along the lines of:

****
The situation is similar to the first update provided Saturday morning (03 Nov). There has been minimal threat activity against IC detected, prompting only minimal mitigation response activities 16(2)(c).

SSC continues to monitor IC's perimeter and will implement appropriate measures if necessary and then advise IT Security. Responsible groups within IC and SSC remain ready to respond to the planned Distributed Denial of Service (DDoS) attacks against the GC.

Of note:
- one GC site reported a DDoS attempt Saturday morning, but there is no evidence of disruption to gc.ca departments;
- SSC (IC) deployed security devices at the IC perimeter Saturday night with the result of augmenting detection and blocking;
- CTEC released two Cyber Flashes providing mitigation recommendations which have been implemented or are being reviewed;
- CTEC has informed us that these DDoS activities against GC may extend beyond the original end date of 15 November to 30 November;
- TBS is to provide official updates to partners.

I trust this is enough information to provide assurances that IC's Services have not been affected at this time and that appropriate monitoring and response plans are in place. I will keep you updated if the situation changes.

Thank you,
Jennifer
****

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 9:51
To: Amott, Chris: SSC-SPC
Subject: FW: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Chris,

Can you let me know the communication plan moving forward in regards to this "Anonymous" DDoS Cyber Threat both during and after regular office hours?

In order for IC to keep CIO Senior Management informed, Rob was providing regular updates to IT Security, specifically, updates every 4 to 5 hours or at the time the situation changed for IC (e.g. at the time one or more IC external facing services/applications was affected by DDoS).

Thank you,
Jennifer

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 9:07 AM
To: Cullen, Jennifer: CIO-BI
Subject: Out of Office AutoReply: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

*****Away from the Office Alert*******

Bonjour, Je suis présentement absent du bureau et serai de retour le 5 Nov 2012. Les affaires qui demandent normalement mon assistance devraient être portées à l'attention de Chirs Amott. Je m'occuperai d'autres questions à mon retour. Merci.

Hi, I am presently away from the office and will return 19(1) 2012. If you require immediate asistance, please contact Amott. All other questions I will address when I return. Thank you.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Saturday, October 27, 2012 15:08
To: Hagarty, Richard: CIO-BI
Subject: Fw: Information Note IN12-002: Anonymous DDoS activity against GC - Update 3

Fyi

----- Original Message -----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Saturday, October 27, 2012 03:06 PM
To: CTEC <CTEC@CSE-CST.GC.CA>
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 3

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 27 October 2012
==========

==========
Update 3: 27 October 2012
- Updated assessment information
- Added SCNet: Shared Services Canada will be leading the mitigation effort with the service SCNet provider.
- Corrected SSC title: SSC Operations Duty Analyst
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

As of 27 October, activity related to this Information Note appears to be continuing at similar levels as observed yesterday and remains under control. This activity is still believed to be related to the Anonymous operation #OpPartyCrasher and related operations, which are scheduled to occur from 3 to 15 November 2012. At this stage 21(1)(b)

21(1)(b)

The departments receiving traffic related to this activity may be affected to varying degrees, from no observable effect to a successful DDoS. The way the network responds to this DDoS traffic depends on many factors, 16(2)(c)

16(2)(c)

GC-CTEC advises that the scope and level of activity may increase as the targeted date range approaches.

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:

- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Sunday, October 28, 2012 19:39
To: Hagarty, Richard: CIO-BI
Subject: Fw: Information Note IN12-002: Anonymous DDoS activity against GC - Update 4

Importance: High

Fyi

----- Original Message -----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Sunday, October 28, 2012 06:56 PM
To: CTEC <CTEC@CSE-CST.GC.CA>
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 4

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 28 October 2012
==========

==========
Update 4: 28 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

As of 28 October, activity related to this Information Note appears to be increasing compared to previous days with new techniques being used. This activity is still believed to be related to the Anonymous operation #OpPartyCrasher and related operations, which is scheduled to occur from 3 to 15 November 2012. At this stage 21(1)(b)

21(1)(b)

Some of the activity attributed to this recent campaign is not indicative to known uses of High Orbit Ion Cannon (HOIC) or other Anonymous techniques. 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Shared Services Canada is working with 16(2)(c) providers to help mitigate this activity as

it is identified. 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

The departments receiving traffic related to this activity may be affected to varying degrees, from no observable effect to a complete denail of service. The way the network responds to this DDoS traffic depends on many factors, 16(2)(c)

16(2)(c)

GC-CTEC advises that the scope and level of activity may increase as the targeted date range approaches, and that it may not follow typical Anonymous techniques.

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:

- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here:
http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the

Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Friday, October 26, 2012 8:35
To: Hagarty, Richard: CIO-BI
Subject: FW: Information Note IN12-002: Anonymous DDoS activity against GC

FYI.

From: Edwards, Robert: SSC-SPC
Sent: Friday, October 26, 2012 8:34 AM
To: Cullen, Jennifer: CIO-BI
Subject: RE: Information Note IN12-002: Anonymous DDoS activity against GC

Hey Jen, this is informational notice and we expect more details shortly,. Our standard tools are in place and we have coordinated our monitoring with our middleware group. If there has been any changes to IC's Incident Handling process or contact list please forward the information.

Cheers,

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, October 25, 2012 2:43 PM
To: Edwards, Robert: SSC-SPC
Subject: FW: Information Note IN12-002: Anonymous DDoS activity against GC
Importance: High

Hi Rob,

In light of the Information Note (IN12-002) received from CTEC, can you let me know what is in place or what shall be put in place or augmented in order to prepare for, detect, and respond to the event described below? Can you also let me know what escalations will occur in the event of DDoS activity being detected or disrupting services, especially those services that IC provides to Canadians?

Thank you,
Jennifer

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 1:24 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========

GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========
On 20 October 2012, GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous was planning against the GC. The Anonymous activity is being distributed under the name of #OpPartyCrasher, but several other operations are also linked to this activity. The manifesto, schedule and the configuration files for the attack, are being posted to public file sharing sites. The tool being used for this campaign is the High Orbit Ion Cannon(HOIC). The goal appears to be disruption of GC sites and services.

According to the publicly posted schedule, the operation is scheduled to run 3 to 15 November 2012. Traffic that is related to this DDOS attack has been observed as early as 22 October 2012. The level of activity appears to be increasing on each subsequent day. As of 25 October 16(2)(c) GC-CTEC advises that the scope and level of activity may increase as we move into the targeted date range. At this stage 21(1)(b)

21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider.

To report any outages or suspicious network activities that require mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@tpsgc-pwgsc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

NOTICE:
This message and accompanying attachments contain information that is intended only

Note to readers

==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, November 7, 2012 14:19
To: 'CTEC'
Subject: FW: Update 13: Information Note IN12-002: Anonymous DDoS activity against GC

Hi,
Would you be able to provide an answer to the question below?
Thank you,
Jennifer

-----Original Message-----
From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, November 7, 2012 9:43 AM
To: 'CTEC'
Subject: RE: Update 13: Information Note IN12-002: Anonymous DDoS activity against GC

Hi,

Given the schedule within this Update 13:IN12-002, does this mean the previously provided schedule is not longer valid? Specifically from Update 12:IN12-002:

"Anonymous has posted a schedule of attacks on pastebay[.]net (paste 1151488) and has announced that they will provide a revised list of targets and boosters one hour before the designated attack times. The listed times are as follows:

Saturday	November 3	12:00-18:00
Sunday	November 4	12:00-18:00
Monday	November 5	Guy Fawkes Day - nothing scheduled
Tuesday	November 6	18:00-22:00
Wednesday	November 7	18:00-22:00
Thursday	November 8	18:00-22:00
Friday	November 9	18:00-22:00"

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone 613-948-4029
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, November 6, 2012 4:25 PM
To: CTEC
Subject: Update 13: Information Note IN12-002: Anonymous DDoS activity against GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 6 November 2012
==========

==========
Update 13: 6 November 2012
- Restructured assessment section
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Current trends show that booster scripts for HOIC are posted 1 hour before a scheduled attack.

Nov. 3
Planned target: Conservative Party of Canada.
Booster target: victoews.com
Target impact: Anonymous claims the website was down for 4 hours. Reports of error pages being presented for a short period of time.
GC impact: No impact reported by GC departments.

Nov. 4
Planned target: Prime Minister Of Canada website.
Booster target: jimflaheretymp.ca
Target impact: Anonymous claims the website was down for 3 hours.
GC impact: No impact reported by GC departments.

Nov. 5

Planned target: Guy Fawkes Day, nothing planned
Booster target: Surrey.ca
Target impact: Anonymous claims the website was down for 2 hours.
GC impact: No impact reported by GC departments.

Nov. 6
Planned target: Quebec Conservatives
Booster target: petermackay.ca
Target impact: None reported at time of update.
GC impact: None reported at time of update.

Nov. 7
Planned target: Ontario Conservatives

Nov. 8
Planned target: PEI Conservatives

Nov. 9
Planned target: Nova Scotia Conservatives

Nov. 10
Planned target: New Brunswick Conservatives

Nov. 11
Planned target: Remembrance Day, nothing planned

Nov. 12
Planned target: Newfoundland and Labrador Conservatives

Nov. 13
Planned target: Manitoba Conservatives

Nov. 14
Planned target: Alberta Conservatives

Nov. 15
Planned target: BC Conservatives

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider, 16(2)(c)

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, November 14, 2012 9:43
To: Edwards, Robert: SSC-SPC
Subject: FW: Update 17: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Hi Rob,

In light of what we are receiving from CTEC, can you confirm if there has been (no) any activity against IC this past week Nov 5 to present. Could you also describe your current and foreseeable future operational monitoring and readiness levels

Thank you,
Jennifer

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, November 13, 2012 3:39 PM
To: CTEC
Subject: Update 17: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 13 November 2012
==========

NOTICE:
This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

==========
Update 17: 13 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Current trends show that booster scripts for HOIC are posted 1 hour before a scheduled attack.

The below schedule is based on one originally posted by Anonymous. Some deviation from the scheduled has been observed through the course of the campaign, and more is anticipate as Anonymous has stated they will be directing their attention away from GC systems.

Nov. 3
 Planned target: Conservative Party of Canada.
 Booster target: victoews.com
 Target impact: Anonymous claims the website was down for 4 hours. Reports of error pages being presented for a short period of time.
 GC impact: No impact reported by GC departments.

Nov. 4
 Planned target: Prime Minister Of Canada website.
 Booster target: jimflahertymp.ca
 Target impact: Anonymous claims the website was down for 3 hours.
 GC impact: No impact reported by GC departments.

Nov. 5
 Planned target: Guy Fawkes Day, nothing planned
 Booster target: surrey.ca
 Target impact: Anonymous claims the website was down for 2 hours.
 GC impact: No impact reported by GC departments.

Nov. 6
 Planned target: Quebec Conservatives
 Booster target: petermackay.ca
 Target impact: Anonymous claims the website was down for 7 hours.
 GC impact: No impact reported by GC departments.

Nov. 7
 Planned target: Ontario Conservatives
 Booster target: blakerichards.ca
 Target impact: Anonymous claims the website was down for 5 hours.
 GC impact: Some DDoS activity was observed at 18 GC departments, resulting in a minor outage at one department. Analysis is on-going to determine if this is linked to the current Anonymous campaign.

Nov. 8
 Planned target: PEI Conservatives
 Booster target: www.pm.gc.ca
 Target impact: Anonymous claims the english version of the website www.pm.gc.ca was down for 2 hours and the french version of the same website for 3 hours.
 GC impact: Some DDoS activity was detected, but no outage was observed or reported.

Nov. 9
 Planned target: Nova Scotia Conservatives
 Booster target: www.conservative.ca
 Target impact: Tweets containing crafted links that take advantage of a

minor flaw in the www.conservative.ca website have been posted, purportedly by Anonymous. Although no compromise has taken place on the website, those visiting using these crafted links will see what appears to be a modified version of the website.
 GC impact: No impact reported by GC departments.

Nov. 10
 Planned target: New Brunswick Conservatives
 Booster target: None
 Target impact: None
 GC impact: No impact reported by GC departments.

Nov. 11
 Planned target: Remembrance Day, nothing planned
 Booster target: None
 Target impact: None
 GC impact: No impact reported by GC departments.

Nov. 12
 Planned target: Newfoundland and Labrador Conservatives
 Booster target: None
 Target impact: None
 GC impact: No impact reported by GC departments.

Nov. 13
 Planned target: Manitoba Conservatives
 Booster target: None
 Target impact: None
 GC impact: No impact reported by GC departments.

Nov. 14
 Planned target: Alberta Conservatives

Nov. 15
 Planned target: BC Conservatives

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider, 16(2)(c)

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
 - SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
 - GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contain information which may have been collected from external sources for which GC-CTEC cannot verify the accuracy and integrity. GC-CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Friday, October 26, 2012 15:51
To: Hagarty, Richard: CIO-BI
Subject: FW: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

FYI.

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, October 26, 2012 3:50 PM
To: Cullen, Jennifer: CIO-BI
Cc: CTEC
Subject: RE: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

Hello Jennifer,

Thank you for your email. There is an update regarding this information note to be released shortly to all departments.

Thank you for your patience.

Regards,

15(1)
GC-CTEC - Cyber Analyst
15(1)

From: Jennifer.Cullen@ic.gc.ca [mailto:Jennifer.Cullen@ic.gc.ca]
Sent: October 26, 2012 8:12 AM
To: CTEC
Subject: RE: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Hello,

Can you inform as to whether Industry Canada is one of the 44 departments, and if so can you provide any details that may be specific to Industry Canada?

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada

235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 3:08 PM
To: CTEC
Subject: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: UNCLASSIFIED

La version française suit.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 1:

We have corrected the e-mail address for SSC to RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca

As of 25 October CTEC has observed related traffic to 44 departments. Not all of the departments that have been targeted are affected to the same degree.

French version is now attached and reflects this update.
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========
On 20 October 2012, GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous was planning against the GC. The Anonymous activity is being distributed under the name of #OpPartyCrasher, but several other operations are also linked to this activity. The manifesto, schedule and the configuration files for the attack, are being posted to public file sharing sites. The tool being used for this campaign is the High Orbit Ion Cannon(HOIC). The goal appears to be disruption of GC sites and services.

According to the publicly posted schedule, the operation is scheduled to run 3 to 15 November 2012. Traffic that is related to this DDOS attack has been observed as early as 22 October 2012. The level of activity appears to be increasing on each subsequent day. As of 25 October 16(2)(c) GC-CTEC advises that the scope and level of activity may increase as we move into the targeted date range. At this stage it

21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider.

To report any outages or suspicious network activities that require mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

==========

CECM-GC – Note d'information IN12-002
Date : 25 octobre 2012
==========

==========
Update 1:

Voici la bonne adresse de courriel de SPC : RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca.

Depuis le 25 octobre, le CECM-GC a observé du trafic connexe dans 44 ministères, mais ceux-ci n'ont pas tous été touchés aussi sévèrement.

Vous trouverez ci-joint la version française qui reflète ce changement.
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======
Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

ÉVALUATION
==========
Le 20 octobre 2012, le CECM-GC a appris qu'Anonymous planifiait une attaque par déni de service distribué contre le gouvernement du Canada (GC). Cette attaque est distribuée sous le nom de #OpPartyCrasher, mais plusieurs autres activités y sont liées. Les auteurs ont affiché sur des sites d'échange de fichiers publics leur manifeste, l'horaire et les fichiers de configuration pour l'attaque. Ils semblent avoir pour objectif l'interruption des sites et des services du GC, et ils ont choisi l'outil High Orbit Ion Cannon (HOIC) pour y arriver.

D'après l'horaire affiché publiquement, l'opération sera menée du 3 au 15 novembre 2012. Le CECM-GC a toutefois observé du trafic lié à cette attaque dès le 22 octobre 2012, et le niveau d'activité n'a cessé d'augmenter depuis. Le 25 octobre, 16(2)(c) Le CECM-GC estime que la portée et le niveau d'activité risquent d'augmenter à mesure que nous approchons des dates prévues de l'opération. Pour l'instant, 21(1)(b)

21(1)(b)

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada (SPC) sera responsable de l'atténuation avec le fournisseur de services.

Pour signaler toute interruption de service ou activité réseau suspecte aux fins d'atténuation, veuillez communiquer avec les deux entités suivantes :

- l'agent de service du Centre de protection de l'information (CPI) de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;

- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse cst.gc.ca.

==========

Note aux lecteurs
==========
Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Gosselin, Andrée: CIO-BI
Sent: Monday, November 5, 2012 10:58
To: Cullen, Jennifer: CIO-BI
Subject: RE: "Anonymous" DDoS Threat Update #2

Thanks Jennifer!!!

Andrée

613-954-0101

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 10:57 AM
To: Rinholm, Rick: CIO-BI
Cc: Gosselin, Andrée: CIO-BI; Acton, Kelly: CIO-BI; Basque Spickett, Diane: CIO-BI; Pomeroy, Patti: CIO-BI; Thompson, Kim: CAS-SCA
Subject: "Anonymous" DDoS Threat Update #2

Mr. Rinholm,

The situation is similar to the first update provided Saturday morning (03 Nov). There has been minimal threat activity against IC detected, prompting only minimal mitigation response activities 16(2)(c)

SSC continues to monitor IC's perimeter and will implement appropriate measures if necessary and then advise IT Security. Responsible groups within IC and SSC remain ready to respond to the planned Distributed Denial of Service (DDoS) attacks against the GC.

Of note:

- one GC site reported a DDoS attempt Saturday morning, but there is no evidence of disruption to gc.ca departments;
- 16(2)(c),21(1)(b)
- CTEC released two Cyber Flashes providing additional mitigation recommendations which have been implemented or are being reviewed;
- CTEC has informed us that these DDoS activities against GC may extend beyond the original end date of 15 November to 30 November;
- TBS is to provide official updates to partners.

I trust this is enough information to provide assurances that IC's Services have not been affected at this time and that appropriate monitoring and response plans are in place. I will provide weekly updates unless there is a change in the situation that warrants your attention.

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 10:58
To: Gosselin, Andrée: CIO-BI
Subject: RE: "Anonymous" DDoS Threat Update #2

Yes, it will be me providing the updates.

From: Gosselin, Andrée: CIO-BI
Sent: Monday, November 5, 2012 10:58 AM
To: Cullen, Jennifer: CIO-BI
Subject: RE: "Anonymous" DDoS Threat Update #2

You will provide the updates :)

Andrée

613-954-0101

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 10:51 AM
To: Gosselin, Andrée: CIO-BI
Subject: RE: "Anonymous" DDoS Threat Update #2

Andrée,

Perfect. Thank you for your feedback and recommendation. I will send this one to Rick and senior management today and emphasize that you will provide weekly updates from now on (i.e. your changes below).

Jennifer

From: Gosselin, Andrée: CIO-BI
Sent: Monday, November 5, 2012 10:46 AM
To: Cullen, Jennifer: CIO-BI
Subject: RE: "Anonymous" DDoS Threat Update #2

Hi Jennifer,

I propose you send this one to Rick and senior management today and emphasize that you will provide weekly updates from now on, unless there is a change in the situation or something similar to what I added below. Are you ok with that?

Andrée

613-954-0101

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 10:41 AM
To: Gosselin, Andrée: CIO-BI
Subject: "Anonymous" DDoS Threat Update #2

Hi Andrée.

Could I please get some advice and direction from you? I think it appropriate to provide updates to Mr Rinholm and CIO Senior Management even if there is no change to IC's environment as a result of the DDoS threat, however, I am unsure at what frequency I should provide updates when there is no change. I would appreciate your feedback?

This morning's message would be along the lines of:

****

The situation is similar to the first update provided Saturday morning (03 Nov). There has been minimal threat activity against IC detected, prompting only minimal mitigation response activities 16(2)(c).

SSC continues to monitor IC's perimeter and will implement appropriate measures if necessary and then advise IT Security. Responsible groups within IC and SSC remain ready to respond to the planned Distributed Denial of Service (DDoS) attacks against the GC.

Of note:

- one GC site reported a DDoS attempt Saturday morning, but there is no evidence of disruption to gc.ca departments;
- 16(2)(c),21(1)(b)
- CTEC released two Cyber Flashes providing mitigation recommendations which have been implemented or are being reviewed;
- CTEC has informed us that these DDoS activities against GC may extend beyond the original end date of 15 November to 30 November;
- TBS is to provide official updates to partners.

I trust this is enough information to provide assurances that IC's Services have not been affected at this time and that appropriate monitoring and response plans are in place. I will **provide weekly updates unless there is a change in the situation that warrants your attention**.

Thank you,
Jennifer
****

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, November 8, 2012 9:02
To: Edwards, Robert: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Thank you.

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Thursday, November 8, 2012 9:01 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, nothing new to report.

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 06, 2012 01:14 PM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, nothing new. Today target has been identified and it's not IC's turn. We don't expect a busy day.

Cheers,

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 06, 2012 11:47 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Nothing to report

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 06, 2012 04:24 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

No Impacts have been reported.

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 05, 2012 12:27 PM
To: Cullen, Jennifer: CIO-BI; IT Security

Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

No impacts have been report with respect OpPartyCrasher at IC. Non at other GOC departments as well.

Cheers,

Rob

----- Original Message -----
From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 05, 2012 10:38 AM
To: Edwards, Robert: SSC-SPC
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

OK thank you.

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 10:18 AM
To: Amott, Chris: SSC-SPC; Cullen, Jennifer: CIO-BI
Cc: Phillips, James: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, I will still be providing updates. As well the CTEC advisories is meant to keeping department informed.

Cheers,

Rob

----- Original Message -----
From: Amott, Chris: SSC-SPC
Sent: Monday, November 05, 2012 10:08 AM
To: Cullen, Jennifer: CIO-BI
Cc: Edwards, Robert: SSC-SPC; Phillips, James: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Jennifer,

Jim is the primary from our group on this issue. I'll discuss with him and get back to you.

Chris

-----Original Message-----
From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 9:51 AM
To: Amott, Chris: SSC-SPC
Subject: FW: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Chris,

Can you let me know the communication plan moving forward in regards to this "Anonymous" DDoS Cyber Threat both during and after regular office hours?

In order for IC to keep CIO Senior Management informed, Rob was providing regular updates to IT Security, specifically, updates every 4 to 5 hours or at the time the situation changed for IC (e.g. at the time one or more IC external facing

services/applications was affected by DDoS).

Thank you,
Jennifer

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 9:07 AM
To: Cullen, Jennifer: CIO-BI
Subject: Out of Office AutoReply: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

*****Away from the Office Alert*******

Bonjour, Je suis présentement absent du bureau et serai de retour le 5 Nov 2012. Les affaires qui demandent normalement mon assistance devraient être portées à l'attention de Chirs Amott. Je m'occuperai d'autres questions à mon retour. Merci.

Hi, I am presently away from the office and will return on 19(1) If you require immediate asistance, please contact Amott. All other questions I will address when I return. Thank you.

Lacroix, Lise: SBTMS-SMTPE

From: Edwards, Robert: SSC-SPC
Sent: Friday, November 9, 2012 7:39
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Quiet night

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Thursday, November 08, 2012 03:49 PM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Uneventful day with regards to DDoS.

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Thursday, November 08, 2012 09:00 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, nothing new to report.

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 06, 2012 01:14 PM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, nothing new. Today target has been identified and it's not IC's turn. We don't expect a busy day.

Cheers,

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 06, 2012 11:47 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Nothing to report

Rob

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

From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 06, 2012 04:24 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

No Impacts have been reported.

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 05, 2012 12:27 PM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

No impacts have been report with respect OpPartyCrasher at IC. Non at other GOC departments as well.

Cheers,

Rob

----- Original Message -----
From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 05, 2012 10:38 AM
To: Edwards, Robert: SSC-SPC
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

OK thank you.

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 10:18 AM
To: Amott, Chris: SSC-SPC; Cullen, Jennifer: CIO-BI
Cc: Phillips, James: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, I will still be providing updates. As well the CTEC advisories is meant to keeping department informed.

Cheers,

Rob

----- Original Message -----
From: Amott, Chris: SSC-SPC
Sent: Monday, November 05, 2012 10:08 AM
To: Cullen, Jennifer: CIO-BI
Cc: Edwards, Robert: SSC-SPC; Phillips, James: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Jennifer,

Jim is the primary from our group on this issue. I'll discuss with him and get back to you.

Chris

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

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 9:51 AM
To: Amott, Chris: SSC-SPC
Subject: FW: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Chris,

Can you let me know the communication plan moving forward in regards to this "Anonymous" DDoS Cyber Threat both during and after regular office hours?

In order for IC to keep CIO Senior Management informed, Rob was providing regular updates to IT Security, specifically, updates every 4 to 5 hours or at the time the situation changed for IC (e.g. at the time one or more IC external facing services/applications was affected by DDoS).

Thank you,
Jennifer

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 9:07 AM
To: Cullen, Jennifer: CIO-BI
Subject: Out of Office AutoReply: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

*****Away from the Office Alert*******

Bonjour, Je suis présentement absent du bureau et serai de retour le 5 Nov 2012. Les affaires qui demandent normalement mon assistance devraient être portées à l'attention de Chirs Amott. Je m'occuperai d'autres questions à mon retour. Merci.

Hi, I am presently away from the office and will return on 19(1). If you require immediate asistance, please contact Amott. All other questions I will address when I return. Thank you.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Tuesday, November 6, 2012 9:05
To: Edwards, Robert: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Thank you Rob.

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 6, 2012 4:25 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

No Impacts have been reported.

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 05, 2012 12:27 PM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

No impacts have been report with respect OpPartyCrasher at IC. Non at other GOC departments as well.

Cheers,

Rob

----- Original Message -----
From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 05, 2012 10:38 AM
To: Edwards, Robert: SSC-SPC
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

OK thank you.

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 10:18 AM
To: Amott, Chris: SSC-SPC; Cullen, Jennifer: CIO-BI
Cc: Phillips, James: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, I will still be providing updates. As well the CTEC advisories is meant to keeping department informed.

Cheers,

Rob

----- Original Message -----
From: Amott, Chris: SSC-SPC

Sent: Monday, November 05, 2012 10:08 AM
To: Cullen, Jennifer: CIO-BI
Cc: Edwards, Robert: SSC-SPC; Phillips, James: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Jennifer,

Jim is the primary from our group on this issue. I'll discuss with him and get back to you.

Chris

-----Original Message-----
From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 9:51 AM
To: Amott, Chris: SSC-SPC
Subject: FW: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Chris,

Can you let me know the communication plan moving forward in regards to this "Anonymous" DDoS Cyber Threat both during and after regular office hours?

In order for IC to keep CIO Senior Management informed, Rob was providing regular updates to IT Security, specifically, updates every 4 to 5 hours or at the time the situation changed for IC (e.g. at the time one or more IC external facing services/applications was affected by DDoS).

Thank you,
Jennifer

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 9:07 AM
To: Cullen, Jennifer: CIO-BI
Subject: Out of Office AutoReply: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

*****Away from the Office Alert*******

Bonjour, Je suis présentement absent du bureau et serai de retour le 5 Nov 2012. Les affaires qui demandent normalement mon assistance devraient être portées à l'attention de Chirs Amott. Je m'occuperai d'autres questions à mon retour. Merci.

Hi, I am presently away from the office and will return on 19(1) If you require immediate asistance, please contact Amott. All other questions I will address when I return. Thank you.

Lacroix, Lise: SBTMS-SMTPE

From: Bordage, Francine: CIO-BI
Sent: Monday, November 5, 2012 11:24
To: Cullen, Jennifer: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Perfect. I will advise the teams.

Thank you Jennifer.
Francine

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 11:23 AM
To: Bordage, Francine: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Thank you very much Francine. Yes, in addition to your normal procedures, please inform IT Security of any event related to this cyber threat. Please use the IT Security distribution list.
Thank you,
Jennifer

From: Bordage, Francine: CIO-BI
Sent: Monday, November 5, 2012 11:06 AM
To: Cullen, Jennifer: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

The following link provides you with a view of any problems, threats, or downtime of the applications listed on the report. It will show red or yellow if any of the sites listed experience problems. This will show you all outages not specifically ones related to "Anonymous" DDoS Cyber Attack threat. We would first have to determine the source of the problem. Marc initially thought it was static, but it is apparently dynamic so you can look at it anytime and it will show the last 24 hours. How would you like us to proceed in the event of a situation? We normally contact the affected client immediately and provide updates until the problem is resolved. Did you want us to inform you of any events related to this cyber threat?

16(2)(c)

Francine

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 9:59 AM
To: Bordage, Francine: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Good Morning Francine,

Understanding that if there was an outage the custodian and/or service owner would have already been informed through standard procedures, please submit the report to me.

Thank you,
Jennifer

From: Bordage, Francine: CIO-BI
Sent: Monday, November 5, 2012 9:57 AM
To: Cullen, Jennifer: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Jennifer,

How would you like us to proceed with regards to the daily reports? We submit it to you and you disseminate to whomever else you think should get it?

Francine

From: Cullen, Jennifer: CIO-BI
Sent: Friday, November 2, 2012 1:54 PM
To: Bordage, Francine: CIO-BI
Cc: Lapointe, Pierre: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Excellent. Thank you Francine.

From: Bordage, Francine: CIO-BI
Sent: Friday, November 2, 2012 1:45 PM
To: Cullen, Jennifer: CIO-BI
Cc: Lapointe, Pierre: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

16(2)(c),21(1)(b)

Let me know if you need any additional information.

Francine

From: Cullen, Jennifer: CIO-BI
Sent: Friday, November 2, 2012 10:57 AM
To: Bordage, Francine: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Francine,

16(2)(c)

Thank you,
Jennifer

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, November 1, 2012 12:22 PM
To: Bordage, Francine: CIO-BI; Patry, Xavier: CMB-DGCM
Cc: Hagarty, Richard: CIO-BI; Gosselin, Andrée: CIO-BI
Subject: FW: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Francine and Xavier,

After discussion with Service Management, I have come to realize that your teams will be implicated from a support perspective in regards to the "Anonymous" DDoS Cyber Attack threat. As a result, I am reaching out to you to ensure that key responders are aware of and prepared for the possibility of this attack.

As I understand, you have had to deal with DDoS attacks in the past and I expect normal standard operating procedures will be used to track and manage any related incidents. However, as this planned attack is resulting in the requirement for a higher level of awareness, IT Security would like to understand if and when any critical external facing applications are degraded or disrupted.

That said, Francine, I would like to request regular daily reports from November 3-15, 2012 as to which external facing services or applications are affected and to what degree as a result of this DDoS attack.

Finally, please review the attached information deck and provide to me the Point of Contact and contact information for your group should it be necessary to increase response and mitigation activities beyond normal operating procedures.

If you have any questions, please give me a call.
Thank you,
Jennifer

<< File: IT Sec Plan_Anonymous_DDoS 2012-10-30_V3_JC.ppt >>

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, October 31, 2012 3:59 PM
To: Bernard, Mario: CIO-BI; Rivard, Karen: CIO-BI; Edwards, Robert: SSC-SPC
Cc: El Chaar, Chahine: CIO-BI; Lord, Suzanne: CIO-BI; Hagarty, Richard: CIO-BI; Gosselin, Andrée: CIO-BI
Subject: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi all,

You may already be aware, "Anonymous" is planning a Distributed Denial of Service (DDoS) attack against the GC from 3 to 15 November, 2012. As such, Industry Canada may be a target which could result in a degradation or disruption of critical external facing applications.

IT Security would like to ensure that key responders are aware of and prepared for the possibility of this attack.

Please review the attached information deck and provide to me the Point of Contact and contact information for your group should it be necessary to respond to and mitigate against the DDoS activities.

I will appreciate if you can remain behind (or join us) after OSM tomorrow to discuss (around 9:30, Room 3 West Lobby).

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 10:53
To: Cullen, Jennifer: CIO-BI
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

I am not in office, however still handling certain activities. Btw, nothing new on DDoS front.

Rob

----- Original Message -----
From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 05, 2012 10:38 AM
To: Edwards, Robert: SSC-SPC
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

OK thank you.

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 10:18 AM
To: Amott, Chris: SSC-SPC; Cullen, Jennifer: CIO-BI
Cc: Phillips, James: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, I will still be providing updates. As well the CTEC advisories is meant to keeping department informed.

Cheers,

Rob

----- Original Message -----
From: Amott, Chris: SSC-SPC
Sent: Monday, November 05, 2012 10:08 AM
To: Cullen, Jennifer: CIO-BI
Cc: Edwards, Robert: SSC-SPC; Phillips, James: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Jennifer,

Jim is the primary from our group on this issue. I'll discuss with him and get back to you.

Chris

-----Original Message-----
From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 9:51 AM
To: Amott, Chris: SSC-SPC
Subject: FW: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Chris,

Can you let me know the communication plan moving forward in regards to this "Anonymous" DDoS Cyber Threat both during and after regular office hours?

In order for IC to keep CIO Senior Management informed, Rob was providing regular updates to IT Security, specifically, updates every 4 to 5 hours or at the time the situation changed for IC (e.g. at the time one or more IC external facing services/applications was affected by DDoS).

Thank you,
Jennifer

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 9:07 AM
To: Cullen, Jennifer: CIO-BI
Subject: Out of Office AutoReply: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

*****Away from the Office Alert*******

Bonjour, Je suis présentement absent du bureau et serai de retour le 5 Nov 2012. Les affaires qui demandent normalement mon assistance devraient être portées à l'attention de Chirs Amott. Je m'occuperai d'autres questions à mon retour. Merci.

Hi, I am presently away from the office and will return on 19(1). If you require immediate asistance, please contact Amott. All other questions I will address when I return. Thank you.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 9:07
To: Edwards, Robert: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Thank you

From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 7:12 AM
To: Cullen, Jennifer: CIO-BI
Cc: IT Security
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Nothing to report

From: Cullen, Jennifer: CIO-BI
Sent: Sunday, November 04, 2012 03:35 PM
To: Edwards, Robert: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Rob,
Understood.
Jen

From: Edwards, Robert: SSC-SPC
Sent: Sunday, November 04, 2012 02:07 PM
To: Cullen, Jennifer: CIO-BI
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, you do know that this DDoS extremely difficult to stop since it acts and looks like a web browser?

16(2)(c),21(1)(a),21(1)(b)

Cheers,

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Sunday, November 04, 2012 02:04 PM
To: Edwards, Robert: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Thank you.

From: Edwards, Robert: SSC-SPC
Sent: Sunday, November 04, 2012 12:48 PM
To: Cullen, Jennifer: CIO-BI
Cc: IT Security
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, no change....

Robert Edwards

Network Security and Integration
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@ic.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Cullen, Jennifer: CIO-BI
Sent: Sun 2012-11-04 8:44 AM
To: Edwards, Robert: SSC-SPC
Cc: IT Security
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Rob,
Thank you very much for the updates.
Jen

From: Edwards, Robert: SSC-SPC
Sent: Sunday, November 04, 2012 05:21 AM
To: Edwards, Robert: SSC-SPC; Cullen, Jennifer: CIO-BI
Cc: IT Security
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

no update on IC front

Rob

Robert Edwards
Network Security and Integration
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@ic.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Edwards, Robert: SSC-SPC
Sent: Sun 2012-11-04 12:26 AM
To: Cullen, Jennifer: CIO-BI
Cc: IT Security
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, no news on HOIC OpPartyCrasher side.

16(2)(c),21(1)(a),21(1)(b)

16(2)(c) no issues were found. 16(2)(c) operating normal.

Cheers,

Rob

Robert Edwards
Network Security and Integration
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Robert.Edwards@ic.gc.ca
Telephone | Téléphone 613-948-6126
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Cullen, Jennifer: CIO-BI
Sent: Sat 2012-11-03 3:54 PM
To: Edwards, Robert: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Thank you.

From: Edwards, Robert: SSC-SPC
Sent: Saturday, November 03, 2012 01:48 PM
To: Cullen, Jennifer: CIO-BI
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Nothing new....

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Saturday, November 03, 2012 10:22 AM
To: Edwards, Robert: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Please keep me informed if there are any changes. I will check my BB every couple of hours.
Thanks,
Jen

From: Edwards, Robert: SSC-SPC
Sent: Saturday, November 03, 2012 10:14 AM
To: Cullen, Jennifer: CIO-BI
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Nothing to update. Only that tonight we are 16(2)(c),21(1)(b) 16(2)(c),21(1)(b)

One GOC site was hit this morning.

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Saturday, November 03, 2012 09:41 AM
To: Edwards, Robert: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Good morning Rob,

I am preparing an update for IC CIO Senior Management. Before I send it, can you provide an update?

Thank you,

Jen

From: Edwards, Robert: SSC-SPC
Sent: Friday, November 02, 2012 04:06 PM
To: IT Security
Subject: Fw: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Fyi

From: Edwards, Robert: SSC-SPC
Sent: Friday, November 02, 2012 04:05 PM
To: Cullen, Jennifer: CIO-BI
Cc: Hagarty, Richard: CIO-BI
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

We will do our best to send updates. TBS, is suppose provide official updates to partners, so we can focus on fire fighting.

We had no impact to service today.. 16(2)(c),21(1)(b) 16(2)(c),21(1)(b) We are receiving regular updates from SSC IPC and CTEC.

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Friday, November 02, 2012 03:43 PM
To: Edwards, Robert: SSC-SPC
Cc: Hagarty, Richard: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Thank you Rob for the prompt detailed reply.
The reason I ask for regular updates is that I will be updating IC CIO senior management and would like to ensure I am providing accurate meaningful information.

Thank you for the 16(2)(c) info. Would you (or who would) be able to tell if the above average requests are service affecting?

Thanks,
Jen

From: Edwards, Robert: SSC-SPC
Sent: Friday, November 2, 2012 3:03 PM
To: Cullen, Jennifer: CIO-BI
Cc: Hagarty, Richard: CIO-BI; IT Security
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

It Sec, 16(2)(c)

Chers,

Rob

From: Edwards, Robert: SSC-SPC
Sent: Friday, November 02, 2012 02:09 PM
To: Cullen, Jennifer: CIO-BI
Cc: Hagarty, Richard: CIO-BI
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, I have asked for the communications protocol again.

Without knowing how much we can share. I will say that we have been working hard all week 16(2)(c)

16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

From blackberry...sorry for spelling

Cheers,

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Friday, November 02, 2012 01:38 PM
To: Edwards, Robert: SSC-SPC
Cc: Hagarty, Richard: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Rob,

For final preparation for this weekend, could you (or your team) provide regular updates (not matter the DDoS activity level) to IT Security distribution list?

Thanks,
Jen

From: Edwards, Robert: SSC-SPC
Sent: Thursday, November 1, 2012 11:17 AM
To: Cullen, Jennifer: CIO-BI
Cc: Hagarty, Richard: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, yes my team is point for IC infrastructure and 16(2)(c)

16(2)(c)

16(2)(c)

16(2)(c) Again, we will be working to defend against attacks, so it will be post any counter measure. As well, as per the deck I forwarded, TBS is working on the greater communication plan.

Cheers,

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, November 1, 2012 10:50 AM
To: Edwards, Robert: SSC-SPC
Cc: Hagarty, Richard: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Thank you Rob.

From an operational perspective, can you confirm my understanding of your team's role in this event. I understand that SSC (IC)'s Network Services Group/Network Security:

- is leading the mitigation effort,
- will coordinate monitoring with the SSC (IC) middleware group,

- have heightened monitoring and ensured counter measures are in place,
- in the event of an attack, SSC (IC) will implement appropriate measures, 16(2)(c)

16(2)(c)

16(2)(c)

Please let me know if I have missed or misunderstood anything.

Thank you,
Jennifer

From: Edwards, Robert: SSC-SPC
Sent: Thursday, November 1, 2012 8:46 AM
To: Cullen, Jennifer: CIO-BI; Hagarty, Richard: CIO-BI
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jennifer, the following presentation by SSC Operational Security Branch to all SSC Sr. Management and portfolio leads. This may have already been shared with IC Sr. Mgt, however at our SSC daily security meeting were advised that we could share this deck with our ITSC counterparts within partner organizations.

<< File: Brief to Ops committee updated.pptx >>
Cheers,

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, October 31, 2012 3:59 PM
To: Bernard, Mario: CIO-BI; Rivard, Karen: CIO-BI; Edwards, Robert: SSC-SPC
Cc: El Chaar, Chahine: CIO-BI; Lord, Suzanne: CIO-BI; Hagarty, Richard: CIO-BI; Gosselin, Andrée: CIO-BI
Subject: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi all,

You may already be aware, "Anonymous" is planning a Distributed Denial of Service (DDoS) attack against the GC from 3 to 15 November, 2012. As such, Industry Canada may be a target which could result in a degradation or disruption of critical external facing applications.

IT Security would like to ensure that key responders are aware of and prepared for the possibility of this attack.

Please review the attached information deck and provide to me the Point of Contact and contact information for your group should it be necessary to respond to and mitigate against the DDoS activities.

I will appreciate if you can remain behind (or join us) after OSM tomorrow to discuss (around 9:30, Room 3 West Lobby).

Thank you,
Jennifer
<< File: IT Sec Plan_Anonymous_DDoS 2012-10-30_V2_JC.ppt >>

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca

Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Friday, November 9, 2012 8:50
To: Edwards, Robert: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Perfect. Thank you.

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Friday, November 9, 2012 8:34 AM
To: Cullen, Jennifer: CIO-BI
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

We are on call all weekend. If anything happens we will send out an alert.

Rob

----- Original Message -----
From: Cullen, Jennifer: CIO-BI
Sent: Friday, November 09, 2012 08:16 AM
To: Edwards, Robert: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Thank you Rob for the regular updates.
Jen

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Thursday, November 8, 2012 3:50 PM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Uneventful day with regards to DDoS.

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Thursday, November 08, 2012 09:00 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, nothing new to report.

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 06, 2012 01:14 PM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, nothing new. Today target has been identified and it's not IC's turn. We don't expect a busy day.

Cheers,

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 06, 2012 11:47 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Nothing to report

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Tuesday, November 06, 2012 04:24 AM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

No Impacts have been reported.

Rob

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 05, 2012 12:27 PM
To: Cullen, Jennifer: CIO-BI; IT Security
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

No impacts have been report with respect OpPartyCrasher at IC. Non at other GOC departments as well.

Cheers,

Rob

----- Original Message -----
From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 05, 2012 10:38 AM
To: Edwards, Robert: SSC-SPC
Cc: Phillips, James: SSC-SPC; Amott, Chris: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

OK thank you.

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 10:18 AM
To: Amott, Chris: SSC-SPC; Cullen, Jennifer: CIO-BI
Cc: Phillips, James: SSC-SPC
Subject: Re: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Jen, I will still be providing updates. As well the CTEC advisories is meant to keeping department informed.

Cheers,

Rob

----- Original Message -----
From: Amott, Chris: SSC-SPC
Sent: Monday, November 05, 2012 10:08 AM
To: Cullen, Jennifer: CIO-BI
Cc: Edwards, Robert: SSC-SPC; Phillips, James: SSC-SPC
Subject: RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Jennifer,

Jim is the primary from our group on this issue. I'll discuss with him and get back to you.

Chris

-----Original Message-----
From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 9:51 AM
To: Amott, Chris: SSC-SPC
Subject: FW: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

Hi Chris,

Can you let me know the communication plan moving forward in regards to this "Anonymous" DDoS Cyber Threat both during and after regular office hours?

In order for IC to keep CIO Senior Management informed, Rob was providing regular updates to IT Security, specifically, updates every 4 to 5 hours or at the time the situation changed for IC (e.g. at the time one or more IC external facing services/applications was affected by DDoS).

Thank you,
Jennifer

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Monday, November 5, 2012 9:07 AM
To: Cullen, Jennifer: CIO-BI
Subject: Out of Office AutoReply: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat

*****Away from the Office Alert*******

Bonjour, Je suis présentement absent du bureau et serai de retour le 5 Nov 2012. Les affaires qui demandent normalement mon assistance devraient être portées à l'attention de Chirs Amott. Je m'occuperai d'autres questions à mon retour. Merci.

Hi, I am presently away from the office and will return on 19(1). If you require immediate asistance, please contact Amott. All other questions I will address when I return. Thank you.

Lacroix, Lise: SBTMS-SMTPE

From: Hagarty, Richard: CIO-BI
Sent: Monday, October 29, 2012 7:35
To: Cullen, Jennifer: CIO-BI
Subject: Re: Information Note IN12-002: Anonymous DDoS activity against GC - Update 4

Hi Jen,

We will need to provide a proposed action plan to mitigate against this threat. The Action Plan (i.e. a deck) will need to define the situation, the risk to our programs and services, the escalation procedures and the reporting mechanisms.

Note that I'm unsure what the final product look like. I will provide visibility on this situation as part of the reporting to Senior Management. That said, I will expect that they will want to know what we are doing about it.

Thanks!

Richard Hagarty
(613) 948-7283

----- Original Message -----
From: Cullen, Jennifer: CIO-BI
Sent: Sunday, October 28, 2012 07:39 PM
To: Hagarty, Richard: CIO-BI
Subject: Fw: Information Note IN12-002: Anonymous DDoS activity against GC - Update 4

Fyi

----- Original Message -----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Sunday, October 28, 2012 06:56 PM
To: CTEC <CTEC@CSE-CST.GC.CA>
Subject: Information Note IN12-002: Anonymous DDoS activity against GC - Update 4

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 28 October 2012
==========

==========
Update 4: 28 October 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========

As of 28 October, activity related to this Information Note appears to be increasing compared to previous days with new techniques being used. This activity is still believed to be related to the Anonymous operation #OpPartyCrasher and related operations, which is scheduled to occur from 3 to 15 November 2012. 21(1)(b)

21(1)(b)

Some of the activity attributed to this recent campaign is not indicative to known uses of High Orbit Ion Cannon (HOIC) or other Anonymous techniques. 16(2)(c)

16(2)(c),21(1)(a),21(1)(b)

The departments receiving traffic related to this activity may be affected to varying degrees, from no observable effect to a complete denail of service. The way the network responds to this DDoS traffic depends on many factors, 16(2)(c)

16(2)(c)

GC-CTEC advises that the scope and level of activity may increase as the targeted date range approaches, and that it may not follow typical Anonymous techniques.

SUGGESTED ACTION
================

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service 16(2)(c) provider.

If a department is observing any traffic related to this DDOS, or is experiencing any outages please contact both:

- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

If a department is not experiencing any outages or observing traffic, but requires further information on this information note please contact CTEC@cse-cst.gc.ca

To report incidents please complete the Incident Report found here:
http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf>
and submit it to ctec@cse-cst.gc.ca

==========

This message and accompanying attachments contain information which may have been collected from external sources for which GC CTEC cannot verify the accuracy and integrity. GC CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Edwards, Robert: SSC-SPC
Sent: Friday, October 26, 2012 16:07
To: Cullen, Jennifer: CIO-BI
Cc: Hagarty, Richard: CIO-BI; Gosselin, Andrée: CIO-BI
Subject: Re: Information Note IN12-002: Anonymous DDoS activity against GC

Jen, thank you for the information. In the event of issues with regards to this CTEC. I think it will be an inform since the nature of this DDoS is to target network and web infrastructure. In the event of an attack, we will implement appropriate measures, then advice since time is something we would not have at our disposal. We have been working throughout the day with the SSC middle ware team to ensure we have heightened monitoring and counter measures in place.

We will keep you informed if we experience any issues.

Cheers,

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Friday, October 26, 2012 03:40 PM
To: Edwards, Robert: SSC-SPC
Cc: Hagarty, Richard: CIO-BI; Gosselin, Andrée: CIO-BI
Subject: RE: Information Note IN12-002: Anonymous DDoS activity against GC

Hi Rob,

For ongoing communication to keep us informed, please use the 16(2)(c) 16(2)(c) . I will be monitoring for incoming emails sent to this list.

In the cases where you require an immediate decision by IC, please contact me on my BB at 15(1) 15(1)

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Edwards, Robert: SSC-SPC
Sent: Friday, October 26, 2012 3:25 PM

To: Cullen, Jennifer: CIO-BI
Subject: RE: Information Note IN12-002: Anonymous DDoS activity against GC

Jen, please forward the contact names and IC's incident handling process so that we can ensure we follow IC's process. SSC has put all it's security teams on elevated monitoring as a proactive measure in response to the CTEC alert.

Cheers,

Rob

From: Edwards, Robert: SSC-SPC
Sent: Friday, October 26, 2012 8:34 AM
To: Cullen, Jennifer: CIO-BI
Subject: RE: Information Note IN12-002: Anonymous DDoS activity against GC

Hey Jen, this is informational notice and we expect more details shortly,. Our standard tools are in place and we have coordinated our monitoring with our middleware group. If there has been any changes to IC's Incident Handling process or contact list please forward the information.

Cheers,

Rob

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, October 25, 2012 2:43 PM
To: Edwards, Robert: SSC-SPC
Subject: FW: Information Note IN12-002: Anonymous DDoS activity against GC
Importance: High

Hi Rob,

In light of the Information Note (IN12-002) received from CTEC, can you let me know what is in place or what shall be put in place or augmented in order to prepare for, detect, and respond to the event described below? Can you also let me know what escalations will occur in the event of DDoS activity being detected or disrupting services, especially those services that IC provides to Canadians?

Thank you,
Jennifer

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 1:24 PM
To: CTEC
Subject: Information Note IN12-002: Anonymous DDoS activity against GC
Importance: High

Classification: UNCLASSIFIED

La version française suivra.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========
On 20 October 2012, GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous was planning against the GC. The Anonymous activity is being distributed under the name of #OpPartyCrasher, but several other operations are also linked to this activity. The manifesto, schedule and the configuration files for the attack, are being posted to public file sharing sites. The tool being used for this campaign is the High Orbit Ion Cannon(HOIC). The goal appears to be disruption of GC sites and services.

According to the publicly posted schedule, the operation is scheduled to run 3 to 15 November 2012. Traffic that is related to this DDOS attack has been observed as early as 22 October 2012. The level of activity appears to be increasing on each subsequent day. As of 25 October 16(2)(c) GC-CTEC advises that the scope and level of activity may increase as we move into the targeted date range. At this stage 21(1)(b)

21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider.

To report any outages or suspicious network activities that require mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@tpsgc-pwgsc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

NOTICE:

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, November 7, 2012 14:51
To: 'CTEC'
Subject: RE: Update 13: Information Note IN12-002: Anonymous DDoS activity against GC

Thank you 15(1) . I was just trying to understand from the provided information what to forward to our responders. I will go by the latest schedules posted.
Thank you,
Jennifer

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Wednesday, November 7, 2012 2:49 PM
To: Cullen, Jennifer: CIO-BI
Cc: CTEC
Subject: RE: Update 13: Information Note IN12-002: Anonymous DDoS activity against GC

Classification: UNCLASSIFIED

Hello Jennifer,

The data that we are reporting on is based on the latest schedules posted by different factions of Anonymous.

As such, it is as valid as can be expected from an loosely organized group intent on disrupting Government websites. The possibility also exists that some of their postings are intentionally misleading and the "official" schedule is being distributed via some other channel.

Regards,

15(1)
<---------->
15(1)
GC-CTEC Cyber Duty Officer
Cyber Threat Evaluation Centre
CTEC@CSE-CST.GC.CA
15(1)

-----Original Message-----
From: Jennifer.Cullen@ic.gc.ca [mailto:Jennifer.Cullen@ic.gc.ca]
Sent: November 7, 2012 9:43 AM
To: CTEC
Subject: RE: Update 13: Information Note IN12-002: Anonymous DDoS activity against GC

Hi,

Given the schedule within this Update 13:IN12-002, does this mean the previously provided schedule is not longer valid? Specifically from Update 12:IN12-002:

"Anonymous has posted a schedule of attacks on pastebay[.]net (paste 1151488) and has announced that they will provide a revised list of targets and boosters one hour before the designated attack times. The listed times are as follows:

Saturday	November 3	12:00-18:00
Sunday	November 4	12:00-18:00
Monday	November 5	Guy Fawkes Day - nothing scheduled

Tuesday November 6 18:00-22:00
Wednesday November 7 18:00-22:00
Thursday November 8 18:00-22:00
Friday November 9 18:00-22:00"

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI Chief Informatics Office | Bureau de l'informatique Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca Telephone | Téléphone 613-948-4029 Facsimile | Télécopieur 613-946-3367 Teletypewriter | Téléimprimeur 1-866-694-8389 Government of Canada | Gouvernement du Canada

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, November 6, 2012 4:25 PM
To: CTEC
Subject: Update 13: Information Note IN12-002: Anonymous DDoS activity against GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 6 November 2012
==========

==========
Update 13: 6 November 2012
- Restructured assessment section
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current

Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Current trends show that booster scripts for HOIC are posted 1 hour before a scheduled attack.

Nov. 3
 Planned target: Conservative Party of Canada.
 Booster target: victoews.com
 Target impact: Anonymous claims the website was down for 4 hours.
Reports of error pages being presented for a short period of time.
 GC impact: No impact reported by GC departments.

Nov. 4
 Planned target: Prime Minister Of Canada website.
 Booster target: jimflaheretymp.ca
 Target impact: Anonymous claims the website was down for 3 hours.
 GC impact: No impact reported by GC departments.

Nov. 5
 Planned target: Guy Fawkes Day, nothing planned
 Booster target: Surrey.ca
 Target impact: Anonymous claims the website was down for 2 hours.
 GC impact: No impact reported by GC departments.

Nov. 6
 Planned target: Quebec Conservatives
 Booster target: petermackay.ca
 Target impact: None reported at time of update.
 GC impact: None reported at time of update.

Nov. 7
 Planned target: Ontario Conservatives

Nov. 8
 Planned target: PEI Conservatives

Nov. 9
 Planned target: Nova Scotia Conservatives

Nov. 10
 Planned target: New Brunswick Conservatives

Nov. 11
 Planned target: Remembrance Day, nothing planned

Nov. 12
 Planned target: Newfoundland and Labrador Conservatives

Nov. 13
 Planned target: Manitoba Conservatives

Nov. 14
 Planned target: Alberta Conservatives

Nov. 15
 Planned target: BC Conservatives

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider, 16(2)(c)

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
- SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, November 14, 2012 9:47
To: Edwards, Robert: SSC-SPC
Subject: RE: Update 17: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Thank you for the info and the prompt reply.
Jen

-----Original Message-----
From: Edwards, Robert: SSC-SPC
Sent: Wednesday, November 14, 2012 9:45 AM
To: Cullen, Jennifer: CIO-BI
Cc: IT Security
Subject: RE: Update 17: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Jen, no new activity on the HOIC front. We have been asked to stay on call until Nov 15th. After this date, we will still be monitoring the situation during operating hours.

Cheers,

Rob

-----Original Message-----
From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, November 14, 2012 9:43 AM
To: Edwards, Robert: SSC-SPC
Subject: FW: Update 17: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Hi Rob,

In light of what we are receiving from CTEC, can you confirm if there has been (no) any activity against IC this past week Nov 5 to present. Could you also describe your current and foreseeable future operational monitoring and readiness levels

Thank you,
Jennifer

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, November 13, 2012 3:39 PM
To: CTEC
Subject: Update 17: GC CTEC - Information Note IN12-002: Anonymous DDoS activity against GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC CTEC - Information Note IN12-002
Date: 13 November 2012
==========

==========
Update 17: 13 November 2012
- Updated assessment information
==========

==========
Anonymous DDoS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

PURPOSE
=======

The purpose of this Information Note is to provide situational awareness on the current Anonymous DDOS operation, #OpPartyCrasher, against the GC.

ASSESSMENT
==========

Current trends show that booster scripts for HOIC are posted 1 hour before a scheduled attack.

The below schedule is based on one originally posted by Anonymous. Some deviation from the scheduled has been observed through the course of the campaign, and more is anticipate as Anonymous has stated they will be directing their attention away from GC systems.

Nov. 3
Planned target: Conservative Party of Canada.
Booster target: victoews.com
Target impact: Anonymous claims the website was down for 4 hours.
Reports of error pages being presented for a short period of time.
GC impact: No impact reported by GC departments.

Nov. 4
Planned target: Prime Minister Of Canada website.
Booster target: jimflahertymp.ca
Target impact: Anonymous claims the website was down for 3 hours.
GC impact: No impact reported by GC departments.

Nov. 5
Planned target: Guy Fawkes Day, nothing planned
Booster target: surrey.ca
Target impact: Anonymous claims the website was down for 2 hours.
GC impact: No impact reported by GC departments.

Nov. 6

Planned target: Quebec Conservatives
Booster target: petermackay.ca
Target impact: Anonymous claims the website was down for 7 hours.
GC impact: No impact reported by GC departments.

Nov. 7
Planned target: Ontario Conservatives
Booster target: blakerichards.ca
Target impact: Anonymous claims the website was down for 5 hours.
GC impact: Some DDoS activity was observed at 18 GC departments, resulting in a minor outage at one department. Analysis is on-going to determine if this is linked to the current Anonymous campaign.

Nov. 8
Planned target: PEI Conservatives
Booster target: www.pm.gc.ca
Target impact: Anonymous claims the english version of the website www.pm.gc.ca was down for 2 hours and the french version of the same website for 3 hours.
GC impact: Some DDoS activity was detected, but no outage was observed or reported.

Nov. 9
Planned target: Nova Scotia Conservatives
Booster target: www.conservative.ca
Target impact: Tweets containing crafted links that take advantage of a minor flaw in the www.conservative.ca website have been posted, purportedly by Anonymous. Although no compromise has taken place on the website, those visiting using these crafted links will see what appears to be a modified version of the website.
GC impact: No impact reported by GC departments.

Nov. 10
Planned target: New Brunswick Conservatives
Booster target: None
Target impact: None
GC impact: No impact reported by GC departments.

Nov. 11
Planned target: Remembrance Day, nothing planned
Booster target: None
Target impact: None
GC impact: No impact reported by GC departments.

Nov. 12
Planned target: Newfoundland and Labrador Conservatives
Booster target: None
Target impact: None
GC impact: No impact reported by GC departments.

Nov. 13
Planned target: Manitoba Conservatives
Booster target: None
Target impact: None
GC impact: No impact reported by GC departments.

Nov. 14
Planned target: Alberta Conservatives

Nov. 15
Planned target: BC Conservatives

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider, 16(2)(c)

Departments should continue to implement the mitigation advice provided in Cyber Flashes.

If a department is experiencing any outages please contact both:
 - SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca, and
 - GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC-CTEC

at ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Saturday, October 27, 2012 8:29
To: 'CTEC@CSE-CST.GC.CA'
Cc: Hagarty, Richard: CIO-BI
Subject: Re: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Hello 15(1)

Thank you for the update. And yes, monitoring is being performed.

Thank you,

Jennifer

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, October 26, 2012 04:03 PM
To: Cullen, Jennifer: CIO-BI
Cc: CTEC <CTEC@CSE-CST.GC.CA>
Subject: RE: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Classification: UNCLASSIFIED

Hello Jennifer,

This message is in response to your request for more information regarding IN12-002. As of today, we have not observed any traffic directed against IC. However, it would be prudent to continue monitoring for any increase in traffic that may suggest a similar circumstance.

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

Thank you for your attention.

Regards,

15(1)
GC-CTEC - Cyber Analyst
15(1)

From: Jennifer.Cullen@ic.gc.ca [mailto:Jennifer.Cullen@ic.gc.ca]
Sent: October 26, 2012 8:12 AM
To: CTEC
Subject: RE: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC

Hello,

Can you inform as to whether Industry Canada is one of the 44 departments, and if so can you provide any details that may be specific to Industry Canada?

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, October 25, 2012 3:08 PM
To: CTEC
Subject: Update 1: Information Note / Note d'information IN12-002: Anonymous DDoS activity against GC / Anonymous - Attaque par déni de service distribué visant le GC
Importance: High

Classification: UNCLASSIFIED

La version française suit.

==========
GC CTEC - Information Note IN12-002
Date: 25 October 2012
==========

==========
Update 1:

We have corrected the e-mail address for SSC to RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca

As of 25 October CTEC has observed related traffic to 44 departments. Not all of the departments that have been targeted are affected to the same degree.

French version is now attached and reflects this update.
==========

==========
Anonymous DDOS activity against GC
==========

AUDIENCE
========

This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========
On 20 October 2012, GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous was planning against the GC. The Anonymous activity is being distributed under the name of #OpPartyCrasher, but several other operations are also linked to this activity. The manifesto, schedule and the configuration files for the attack, are being posted to public file sharing sites. The tool being used for this campaign is the High Orbit Ion Cannon(HOIC). The goal appears to be disruption of GC sites and services.

According to the publicly posted schedule, the operation is scheduled to run 3 to 15 November 2012. Traffic that is related to this DDOS attack has been observed as early as 22 October 2012. The level of activity appears to be increasing on each subsequent day. As of 25 October 16(2)(c) GC-CTEC advises that the scope and level of activity may increase as we move into the targeted date range. At this stage it

21(1)(b)

SUGGESTED ACTION
==========

GC-CTEC is coordinating the incident response and the threat evaluation for this event. Shared Services Canada will be leading the mitigation effort with the service provider.

To report any outages or suspicious network activities that require mitigation , please contact both

- SSC GOP Duty Analyst duty analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca
- GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca

To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and submit it to ctec@cse-cst.gc.ca

==========

Note to readers
==========
The Government of Canada Cyber Threat Evaluation Centre (GC CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information

systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact GC CTEC at ctec@cse-cst.gc.ca

==========
CECM-GC – Note d'information IN12-002
Date : 25 octobre 2012
==========

==========
Update 1:

Voici la bonne adresse de courriel de SPC : RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca.

Depuis le 25 octobre, le CECM-GC a observé du trafic connexe dans 44 ministères, mais ceux-ci n'ont pas tous été touchés aussi sévèrement.

Vous trouverez ci-joint la version française qui reflète ce changement.
==========

==========
Anonymous – Attaque par déni de service distribué visant le GC
==========

PUBLIC
======
Cette note d'information est destinée aux professionnels des TI et aux gestionnaires du gouvernement fédéral.

ÉVALUATION
==========
Le 20 octobre 2012, le CECM-GC a appris qu'Anonymous planifiait une attaque par déni de service distribué contre le gouvernement du Canada (GC). Cette attaque est distribuée sous le nom de #OpPartyCrasher, mais plusieurs autres activités y sont liées. Les auteurs ont affiché sur des sites d'échange de fichiers publics leur manifeste, l'horaire et les fichiers de configuration pour l'attaque. Ils semblent avoir pour objectif l'interruption des sites et des services du GC, et ils ont choisi l'outil High Orbit Ion Cannon (HOIC) pour y arriver.

D'après l'horaire affiché publiquement, l'opération sera menée du 3 au 15 novembre 2012. Le CECM-GC a toutefois observé du trafic lié à cette attaque dès le 22 octobre 2012, et le niveau d'activité n'a cessé d'augmenter depuis. Le 25 octobre, 16(2)(c) Le CECM-GC estime que la portée et le niveau d'activité risquent d'augmenter à mesure que nous approchons des dates prévues de l'opération. Pour l'instant, 21(1)(b)

21(1)(b)

MESURES RECOMMANDÉES
==========

Le CECM-GC coordonne l'intervention et l'évaluation de la menace dans ce dossier. Services partagés Canada

(SPC) sera responsable de l'atténuation avec le fournisseur de services.

Pour signaler toute interruption de service ou activité réseau suspecte aux fins d'atténuation, veuillez communiquer avec les deux entités suivantes :

- l'agent de service du Centre de protection de l'information (CPI) de SPC, au 819-956-1006 ou à RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca;

- l'agent de cybersécurité de service du CECM-GC à ctec@cse-cst.gc.ca.

Pour signaler un incident, veuillez remplir le rapport d'incident (disponible à l'adresse http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-fra.rtf) et l'envoyer à ctec@cse cst.gc.ca.

==========

Note aux lecteurs
==========
Le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC) est le centre de coordination de l'analyse, des alertes et de l'intervention liées aux cybervulnérabilités et aux cybermenaces. Le CECM-GC aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale relativement aux incidents de cybersécurité d'intérêt national. L'équipe du CECM-GC, qui évolue au sein du Centre de la sécurité des télécommunications Canada (CSTC), cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler un incident touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à ctec@cse-cst.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Friday, November 2, 2012 20:43
To: Fournier, Denis: CIO-BI
Subject: Fw: Cyber Flash / Cybercapsule GCCF12-009: Possible use of HOIC for DDoS campaign against the GC

Just an FYI

----- Original Message -----
From: Edwards, Robert: SSC-SPC
Sent: Friday, November 02, 2012 07:35 PM
To: Cullen, Jennifer: CIO-BI
Subject: Re: Cyber Flash / Cybercapsule GCCF12-009: Possible use of HOIC for DDoS campaign against the GC

We have implemented or were not vulnerable to some attacks..

Rob

----- Original Message -----
From: Cullen, Jennifer: CIO-BI
Sent: Friday, November 02, 2012 05:07 PM
To: Edwards, Robert: SSC-SPC
Subject: Fw: Cyber Flash / Cybercapsule GCCF12-009: Possible use of HOIC for DDoS campaign against the GC

Hi Rob,

Could you or one of your team members inform as to whether or not the mitigation recommendations from GCCF12-09 and GCCF12-10 have been implemented? (great timing for sending/receiving these CFs :))

Thank you,
Jennifer

----- Original Message -----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, November 02, 2012 04:14 PM
To: CTEC <CTEC@CSE-CST.GC.CA>
Subject: Cyber Flash / Cybercapsule GCCF12-009: Possible use of HOIC for DDoS campaign against the GC

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC-CTEC - Cyber Flash GCCF12-009
Date: 02 November 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal government.

TITLE

=====
Possible use of HOIC for DDoS campaign against the GC

DETAILS
=======
This Cyber Flash is related to 'Information Note IN12-002: Anonymous DDoS activity against GC' and all updates.

The High Orbit Ion Cannon (HOIC) is a Windows-based DDoS tool characteristically attributed to Anonymous. HOIC is a multi-threaded DDoS tool that transmits HTTP requests. In order for it to work effectively, HOIC relies on a configurable "booster" script that is commonly posted publicly. Users may leverage the booster script to specify a list of rotating URLs for HTTP requests, using either the GET or POST (user-specified data) request methods. Users may also randomize the user-agent (based on a user-defined list) and create custom headers (composed of user-defined strings, appended in the order of their choice). The request rate can also be set (default is 2 threads).

MITIGATION
==========

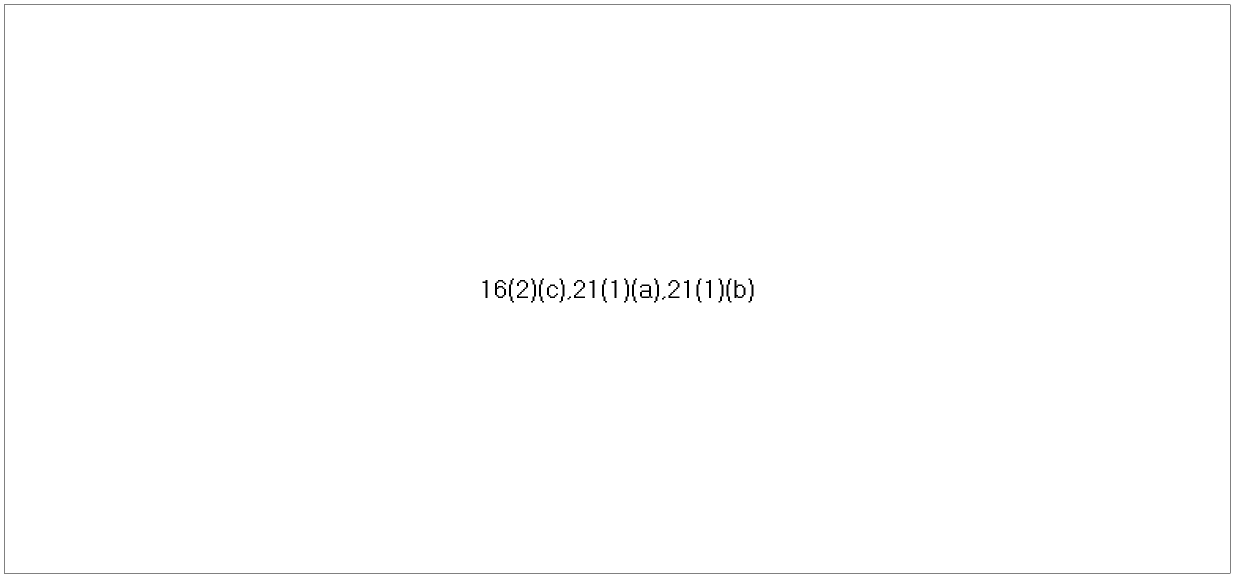
Network-based mitigation

16(2)(c),21(1)(a),21(1)(b)

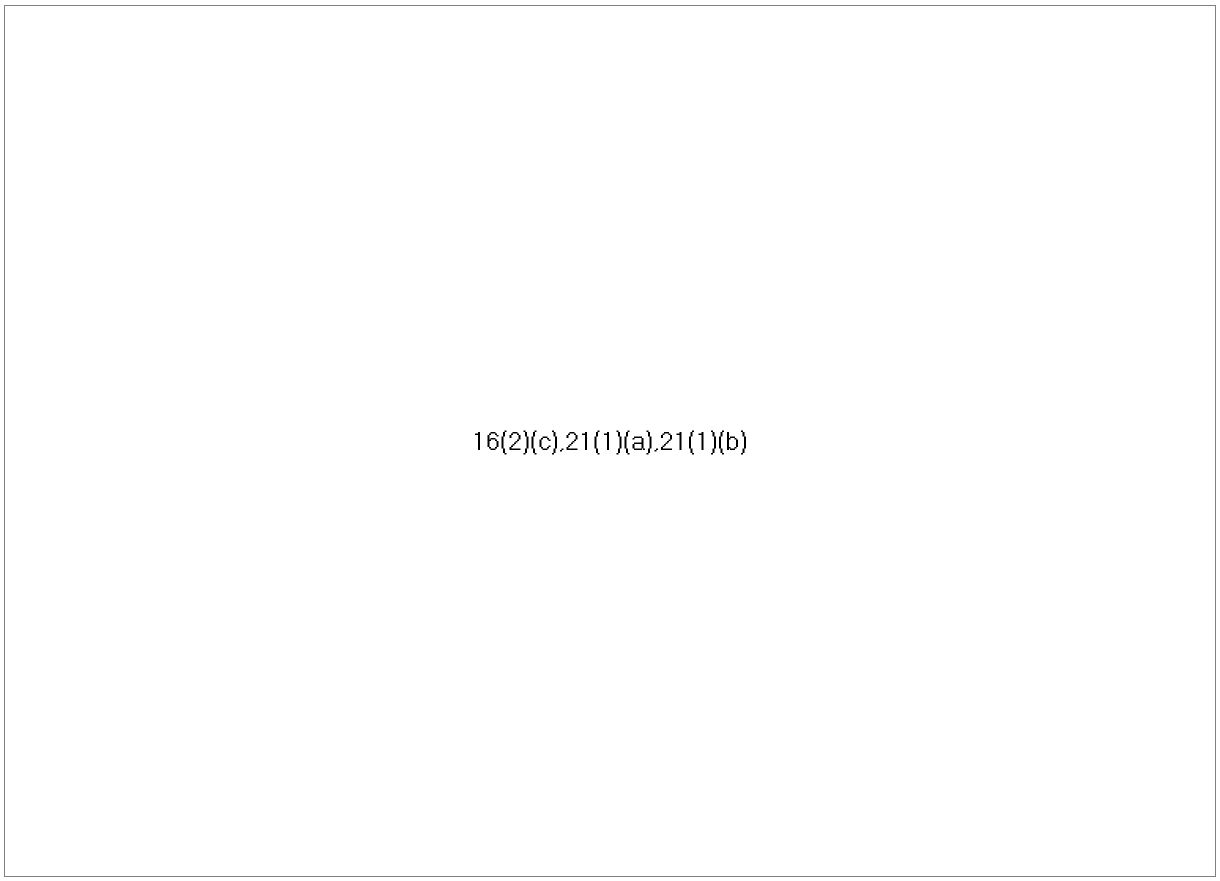
In the case where a booster script is being used, detection involves identification of non-typical search patterns attributed to popular search engines.

16(2)(c),21(1)(a),21(1)(b)

In order to help minimize the effect of this attack tool on websites, GC website administrators are advised to take the following mitigative actions where practical:



While the request header names and payloads, in and of themselves, are valid, the order in which they are defined in the request do not match what normal web browsers would send. The easiest characteristic to notice is that, in HOIC, the Host header is always listed last in the header order while this is not the case in any legitimate browsers.



Tactical mitigation

In addition to the traffic patterns that may be observed above,

16(2)(c).21(1)(a).21(1)(b)

Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.
The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

REPORTING
=========
Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC. To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

NOTE TO READERS
===============
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.
To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca or (613)991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Friday, November 2, 2012 19:19
To: IT Security
Subject: FW: Cyber flash GCCF12-009: Possible use of HOIC for DDoS campaign against the GC

Forgot to put IT Security cc

From: Fournier, Denis: CIO-BI
Sent: Friday, November 2, 2012 7:18 PM
To: NSG Security - Securité GSR; MDP Team; AMIS Hotline / GASI Assistance
Cc: NSGSEC-E
Subject: FW: Cyber flash GCCF12-009: Possible use of HOIC for DDoS campaign against the GC

Please review mitigation as per subj flash and makes necessary changes where appropriate.

If IT Security can be of any help please don't hesitate to get in contact with us

Thanks

From: Fournier, Denis: CIO-BI
Sent: Friday, November 2, 2012 7:08 PM
To: IT Security Advisory / Avis Sécurité TI
Subject: Cyber flash GCCF12-009: Possible use of HOIC for DDoS campaign against the GC

Please disseminate to the appropriate staff

Disséminez svp au personnel approprié

==========
GC-CTEC - Cyber Flash GCCF12-009
Date: 02 November 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal government.

TITLE
=====
Possible use of HOIC for DDoS campaign against the GC

DETAILS
=======
This Cyber Flash is related to 'Information Note IN12-002: Anonymous DDoS activity against GC' and all updates.

The High Orbit Ion Cannon (HOIC) is a Windows-based DDoS tool characteristically attributed to Anonymous. HOIC is a multi-threaded DDoS tool that transmits HTTP requests. In order for it to work effectively, HOIC relies on a configurable "booster" script that is commonly posted publicly. Users may leverage the booster script to specify a list of rotating URLs for HTTP requests, using either the GET or POST (user-specified data) request methods. Users may also randomize the user-agent (based on a user-defined list) and create custom headers (composed of user-defined strings, appended in the order of their

choice). The request rate can also be set (default is 2 threads).

MITIGATION
==========

Network-based mitigation

16(2)(c),21(1)(a),21(1)(b)

Please be aware if the security devices on your network will fail in an open or closed manner in the event of a DDoS attack. The implications of each are briefly covered below:

16(2)(c),21(1)(a),21(1)(b)

In order to help minimize the effect of this attack tool on websites, GC website administrators are advised to take the following mitigative actions where practical:

16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

While the request header names and payloads, in and of themselves, are valid, the order in which they are defined in the request do not match what normal web browsers would send. The easiest characteristic to notice is that, in HOIC, the Host header is always listed last in the header order while this is not the case in any legitimate browsers.

16(2)(c),21(1)(a),21(1)(b)

Tactical mitigation

In addition to the traffic patterns that may be observed above,

16(2)(c),21(1)(a),21(1)(b)

Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.
The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing

or crawling sites contained within this report.

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Tuesday, October 30, 2012 17:16
To: IT Security Advisory / Avis Sécurité TI
Cc: IT Security
Subject: IT Sec Flash SF010-12_DDoS campaign against the GC

Importance: High

Please disseminate to the appropriate staff

La version francaise suivra.

TITLE
=====
DDoS campaign against the GC

DETAILS
=======
This Cyber Flash is related to 'Information Note IN12-002: Anonymous DDoS activity against GC' and all updates.

On 22 October, GC-CTEC was notified that some GC departments were experiencing degraded states or periods of being offline. Further investigation resulted in the discovery of DDoS related techniques that looks to be beyond what has been characteristically attributed to Anonymous or HOIC capabilities. 21(1)(b)

21(1)(b)

This campaign has had several characteristics that set it apart from a typical DDoS event which typically use SYN or HTTP Get flooding:
- Shared Services Canada IPC has reported that it is not hitting any volume thresholds at the provider level that would normally be seen in a typical DDoS event.
- The volume of information looks to have started off slowly and ramped up over the course of several days, the volume has since returned to near normal levels

16(2)(c)

MITIGATION
==========

16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Be aware of the configuration and behaviour of security devices on your network perimeter. If they were to fail due to a DDoS attack would they fail open or closed? The implications of each are briefly covered below:

16(2)(c),21(1)(a),21(1)(b)

Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.
The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada
http://icweb.ic.gc.ca/eic/site/ciobis-sidgapi.nsf/eng/h_00713.html
http://icweb.ic.gc.ca/eic/site/ciobis-sidgapi.nsf/fra/h_00713.html
Never trouble trouble till trouble troubles you!!!

Lacroix, Lise: SBTMS-SMTPE

From: Hagarty, Richard: CIO-BI
Sent: Tuesday, October 30, 2012 15:36
To: Cullen, Jennifer: CIO-BI
Subject: Re: Cyber Flash / Cybercapsule GCCF12-007: DDoS campaign against the GC

Ok thanks!

Richard Hagarty
(613) 948-7283

From: Cullen, Jennifer: CIO-BI
Sent: Tuesday, October 30, 2012 03:34 PM
To: Hagarty, Richard: CIO-BI
Subject: FW: Cyber Flash / Cybercapsule GCCF12-007: DDoS campaign against the GC

Hi Richard,

FYI. There is nothing new here from an Anonymous activity point of view. This CF provides mitigation recommendations to departments. Tom will action it when he gets home this evening.

Thanks,
Jen

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, October 30, 2012 3:20 PM
To: CTEC
Subject: Cyber Flash / Cybercapsule GCCF12-007: DDoS campaign against the GC
Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC-CTEC - Cyber Flash GCCF12-007
Date: 30 October 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal government.

TITLE
=====
DDoS campaign against the GC

DETAILS

=======
This Cyber Flash is related to 'Information Note IN12-002: Anonymous DDoS activity against GC' and all updates.

On 22 October, GC-CTEC was notified that some GC departments were experiencing degraded states or periods of being offline. Further investigation resulted in the discovery of DDoS related techniques that looks to be beyond what has been characteristically attributed to Anonymous or HOIC capabilities. 21(1)(b)

21(1)(b)

This campaign has had several characteristics that set it apart from a typical DDoS event which typically use SYN or HTTP Get flooding:

- Shared Services Canada IPC has reported that it is not hitting any volume thresholds at the provider level that would normally be seen in a typical DDoS event.

- The volume of information looks to have started off slowly and ramped up over the course of several days, the volume has since returned to near normal levels

16(2)(c),21(1)(a),21(1)(b)

MITIGATION
==========

16(2)(c),21(1)(a),21(1)(b)

Be aware of the configuration and behaviour of security devices on your network perimeter. If they were to fail due to a DDoS attack would they fail open or closed? The implications of each are briefly covered below:

16(2)(c),21(1)(a),21(1)(b)

16(2)(c).21(1)(a).21(1)(b)

Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.

The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient.

The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

REPORTING
=========
Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC. To report incidents please complete the Incident Report found here: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf <http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf> and submit it to ctec@cse-cst.gc.ca

NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which GC CTEC cannot verify the accuracy and integrity. GC CTEC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

NOTE TO READERS
===============
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

To report incidents affecting GC infrastructures, please contact GC-CTEC at

ctec@cse-cst.gc.ca or (613)991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: Amott, Chris: SSC-SPC
Sent: Tuesday, October 30, 2012 17:47
To: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN); NSG Security - Securité GSR
Cc: IT Security
Subject: RE: IT Sec Flash SF010-12_DDoS campaign against the GC

Thanks Thomas, we will review and advise on changes.

-----Original Message-----
From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Tuesday, October 30, 2012 5:20 PM
To: NSG Security - Securité GSR
Cc: IT Security
Subject: FW: IT Sec Flash SF010-12_DDoS campaign against the GC
Importance: High

NSG

Please review mitigation as per subj flash and makes necessary changes where appropriate.

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

-----Original Message-----
From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Tuesday, October 30, 2012 5:16 PM
To: IT Security Advisory / Avis Sécurité TI
Cc: IT Security
Subject: IT Sec Flash SF010-12_DDoS campaign against the GC
Importance: High

Please disseminate to the appropriate staff

La version francaise suivra.

TITLE
=====
DDoS campaign against the GC

DETAILS

=======
This Cyber Flash is related to 'Information Note IN12-002: Anonymous DDoS activity against GC' and all updates.

On 22 October, GC-CTEC was notified that some GC departments were experiencing degraded states or periods of being offline. Further investigation resulted in the discovery of DDoS related techniques that looks to be beyond what has been characteristically attributed to Anonymous or HOIC capabilities. 21(1)(b)

21(1)(b)

This campaign has had several characteristics that set it apart from a typical DDoS event which typically use SYN or HTTP Get flooding:
- Shared Services Canada IPC has reported that it is not hitting any volume thresholds at the provider level that would normally be seen in a typical DDoS event.
- The volume of information looks to have started off slowly and ramped up over the course of several days, the volume has since returned to near normal levels

16(2)(c),21(1)(a),21(1)(b)

MITIGATION
==========

16(2)(c),21(1)(a),21(1)(b)

Be aware of the configuration and behaviour of security devices on your network perimeter. If they were to fail due to a DDoS attack would they fail open or closed? The implications of each are briefly covered below:

16(2)(c),21(1)(a),21(1)(b)

Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.
The information contained in this message is provided strictly for the

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

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Monday, November 5, 2012 14:32
To: Fournier, Denis: CIO-BI; Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Subject: "Anonymous" DDoS Threat

Attachments: IT Sec Plan_Anonymous_DDoS 2012-10-30_V4_JC.ppt; Re: Cyber Flash / Cybercapsule GCCF12-009: Possible use of HOIC for DDoS campaign against the GC; "Anonymous" DDoS Threat Update; RE: Industry Canada's Response Plan to the "Anonymous" DDoS Cyber Threat; "Anonymous" DDoS Threat Update #2; Re: Cyber Flash GCCF12-010: Mitigation for campaign against GC Website forms; RE: Cyber Flash GCCF12-010: Mitigation for campaign against GC Website forms

Hi guys,

Sorry to not have informed you sooner to the activities Richard asked me to do in light of the reported "Anonymous" DDoS Threat. There have been numerous emails going back and forth, but I think this summarizes IT Security's involvement. We can take some time tomorrow to have a look.

The attached PowerPoint presentation (version 4) is the most up to date with the plan and all the contacts. 16(2)(c)

16(2)(c)

IT Sec Anonymous_DDoS 2

A) Although numerous groups are involved, I am expecting normal operating procedures to be used when responding to this threat, but I have requested that we receive to the IT Security distribution list:

- regular updates from NSG/Sec, and
- in the event an external service is affected, 16(2)(c)

16(2)(c)

- 16(2)(c)

B) Below is some of the communications related to IC's Response Plan:

1. Response Plan email was sent to key responders (CSD/Service Desk, PCRD/Service Management, SSC/NSG/Sec, ASD/AMIS Hotline, CMB/Web Service Centre, ASD/Content Management Systems, CMB Corporate Communications). Contact information was provided.

2. SSC's Response Plan:

Re: Cyber Flash / Cybercapsule...

3. Two email updates to CIO and CIO Senior Management:


'Anonymous" DDoS Threat Update... | RE: Industry Canada's Response..

4. As you have seen coming from CTEC to the IT Security distlist, there have been 11 updates to the original Information Note IN12-002: Anonymous DDoS activity against GC, and two Cyber Flashes containing mitigation recommendations. Attached are the responses to the Cyber Flashes:



'Anonymous" DDoS Threat Update... | Re: Cyber Flash GCCF12-010: M... | RE: Cyber Flash GCCF12-010: M...

Thanks,
Jen

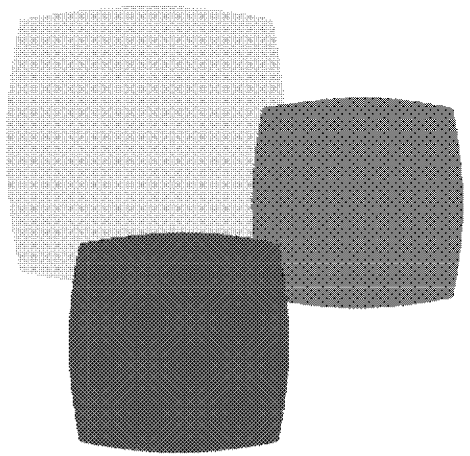
Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

IT Security Incident Management

IT Security Incident Response Plan

"Anonymous" Cyber Threat

October 2012 (V4)



Canada

Introduction

- **“Anonymous” Threat**
- **GC Preparation and Response**
- **IC Preparation and Response**
- **Reporting/Communications**
- **Contact Information**

"Anonymous" Threat

- **Background**
  - GC-CTEC was made aware of a Distributed Denial of Service (DDoS) operation Anonymous is planning against the GC.
  - The goal appears to be disruption of GC sites and services.
  - The operation is scheduled to run 3 to 15 November 2012, possibly until 30 November 2012.
- **Observations to date**
  - Traffic that is related to this DDoS attack has been observed as early as 22 October 2012, 16(2)(c)
  - There is no indication that IC is being affected/is among those departments affected.
  - However, the scope and level of activity may increase as the targeted date range approaches.
- 21(1)(a),21(1)(b)

Canada

GC Preparation and Response

- GC-CTEC is **coordinating** the incident response and the threat evaluation for this event.
- GC-CTEC is informing its constituency.
- Shared Services Canada (SSC) Operations Centre will be **leading the mitigation effort** with the service provider 16(2)(c).
- Departments are to report any outages or suspicious network activities that require mitigation by contacting both GC-CTEC and SSC Operations Centre.
- Mitigation typically involves 16(2)(c),21(1)(b)

16(2)(c),21(1)(b)

IC Preparation and Response

- **Key response personnel:**
  - IC/CIO/IT Security
  - IC/CIO/Service Management
  - 16(2)(c)
  - IC/CMB/Web Service Centre
  - IC/CIO/Service Desk
  - IC/CMB/Corporate Communications
  - SSC (IC) NSG/Sec in coordination with SSC (IC) Midrange

- **IC's critical external facing applications:**
  - To be Identified

IC Preparation and Response

- **IC Response Roles**
  - IT Security is coordinating the IC incident response.
  - Web Service Centre and Service Desk track and manage client issue reporting.
  - 16(2)(c) to track and manage related incidents, work with SSC/NSG/Sec and SSC/Midrange. Inform application/service custodian/owner, Web Service Centre, and IT Security.
  - Service Management provides communications.
  - CMB/Corporate Communications provides communications.
  - IT Security to provide regular updates to IC/CIO Senior Management and DSO
    - Rick Rinholm, Kelly Acton, Patti Pomeroy, Diane Basque Spickett, Andrée Gosselin, and Kim Thompson.

IC Preparation and Response

- **SSC (IC) Response Roles**
  - SSC (IC)'s Network Services Group/Network Security is leading the mitigation effort and have coordinated their monitoring with the SSC (IC) Midrange group, and have heightened monitoring and counter measure.
  - In the event of an attack, SSC (IC) will implement appropriate measures then advise 16(2)(c), IT Security, and GC-CTEC and SSC Operations Centre.

Contact Information

IC/CIO/IT Security - Jennifer Cullen

16(2)(c) (W) 613-948-4029, BB 15(1),

BB PIN 18(a)

IT Security Conference Bridge, 18(a) or 18(a) 18(a), Conference ID 18(a),21(1)(a)

IC/CIO/Service Management – Karen Rivard (w) 613-946-0515 /Suzanne Lord (w) 613-952-1664, CIO IT Problem Manager 16(2)(c), see PCRD Contact Card for further details.

CMB/Corporate Communications, Denis Dummer, denis.dummer@ic.gc.ca, (w) 613-992-3552

Canada

Contact Information cont.

16(2)(c)

IC/CMB/Web Service Centre
613-954-5031 or 1-800-328-6189,

16(2)(c)

Alt. Susan Shapiro, 613-952-5480

Canada

Contact Information cont.

IC/CIO/Service Desk
Denis Parisien
W: 613-952-7802
BB: 613-899-2401
PIN: 18(a)

Johnny Francis
W: 613-946-6953
BB: 613-222-6826
PIN: 18(a)

Contact Information cont.

SSC (IC) NSG/Sec
Robert Edwards: (W) 613-948-6126, (BB) 613-325-3249
NSG Sec Pager: 613-368-0342, NSG Voice Mail: 954-6422

NSG Ops Pager: 613-239-7968,
NSG Ops Cel: 613-298-6310,
NSG Ops VM: 613-957-4170
NSG Eng Pager: 613-954-6422

SSC (IC) Midrange
Via SSC (IC) NSG/Sec.

Contact Information cont.

GC-CTEC

GC-CTEC Cyber Duty Officer ctec@cse-cst.gc.ca or (613)991-2300.

GC-SSC-Operations Centre

SSC Operations Duty Analyst 819-956-1006 or RCNGPSCPI.NCRSMDIPC@ssc-spc.gc.ca.

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Monday, November 19, 2012 10:15
To: IT Service Desk - Centre de services TI
Cc: IT Security
Subject: "URGENT" infected computer 16(2)(c)

Service Desk,

Please create a ticket under the client name (Item 2) and assign a technician for immediate 16(2)(c)

The following action needs to be taken **ASAP** without any **delays**.

16(2)(c),21(1)(a)

Client Name: 19(1)

Client Host: 19(1)

Client Dept: SITT-STIT

Client Local 19(1)

I was able to reach the user and he is waiting for the TSO

3. Security logs indicate clients workstation is trying to communicate with a known Malware site multiple times that is part of the Cyber Flash: IT Sec Flash SF009-12 Update #3: Canada Post & Airline Company Email Phishing Campaign. The mitigation for this infection is 16(2)(c)

4. In the event the client is unreachable this email will also be released to the client

5. Your immediate cooperation and response is appreciated.

16(2)(c)

Question can be directed to IT Security

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada
http://icweb.ic.gc.ca/eic/site/ciobis-sidgapi.nsf/eng/h_00713.html
http://icweb.ic.gc.ca/eic/site/ciobis-sidgapi.nsf/fra/h_00713.html

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Monday, September 24, 2012 11:28
To: IT Service Desk - Centre de services TI
Cc: IT Security
Subject: "URGENT" 16(2)(c)

Attachments: 16(2)(c)

Service Desk,

Please create a ticket under the two clients name (Item 2) and assign a technician for immediate 16(2)(c) 16(2)(c)

The following action needs to be taken **ASAP** without any **delays**.

16(2)(c)

a) 19(1) 235 Queen Street, Ottawa, ON., 19(1) Heat ticket to be updated when completed. Hostname: 19(1)
B) 19(1) 155 Queen Street, Ottawa, ON., 19(1) Heat ticket to be updated when completed. Hostname: 19(1)

3. These clients were infected by the 16(2)(c) As per the CTEC Cyber Flash GCCF12-006, we are to 16(2)(c)

16(2)(c)

4. In the event the client is unreachable this email will also be release to the client.

5. Your immediate cooperation and response is appreciated.

16(2)(c)

Feel free to contact the undersigned or IT Security directly for queries/questions

Thank you

16(2)(c)

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784

Lacroix, Lise: SBTMS-SMTPE

From: 16(2)(c)@ic.gc.ca
Sent: Monday, September 24, 2012 7:20
To: ITSec HEAT
Cc: IT Service Request / Demande de Service TI
Subject: 01269926: New Assignment / Nouvelle affectation

-----Request Description / Description de la demande-----

Information- IT Security- Threat and Risk Assessment

Service request # 01269926 has been assigned to you, IT Security or your group, IT Security / Sécurité TI. /
Demande de service # 01269926 a été assigné à toi, IT Security ou à ton équipe, IT Security / Sécurité TI.

User name / Nom du client : Jennifer Cullen

Email / Courriel : mailto:Jennifer.Cullen@ic.gc.ca

City / Ville : Ottawa

Phone / Téléphone : (613) 948-4029

Room / Pièce : 271E

Target Date & Time / Date & heure ciblée : 2012-10-01 @ 06:52:25

----------Call History / Historique de l'appel

2012-09-24 @ 06:56:37 by SDBotelJ - Original Email follows:

From: Brabant, Mathieu: CIO-BI
Sent: Friday, September 21, 2012 4:39 PM
To: Hagarty, Richard: CIO-BI; Cullen, Jennifer: CIO-BI
Cc: ITSec; DPM-AVE: Anti-Virus Engineering Team; ! IT Service Desk; Peters, Bernadette: CIO-BI; Rivard, Karen: CIO-BI; McCloskey, Paul: CIO-BI (NCR-RCN); Gosselin, Andrée: CIO-BI; Bernard, Mario: CIO-BI
Subject: 16(2)(c)

Hi,

16(2)(c)

Mathieu

From: Hagarty, Richard: CIO-BI
Sent: Friday, September 21, 2012 4:16 PM

To: Rivard, Karen: CIO-BI; McCloskey, Paul: CIO-BI (NCR-RCN); Gosselin, Andrée: CIO-BI; Bernard, Mario: CIO-BI
Cc: Cullen, Jennifer: CIO-BI; ITSec; DPM-AVE: Anti-Virus Engineering Team
Subject: Communication for 16(2)(c)

Hi Karen, Paul,

We were just advised that a high number of desktop were detected with a new virus. At the same time, we are told by CTEC aka CSEC that 16(2)(c) 16(2)(c) Although the two (2) incidents are not related, the level of risk suddenly increase requiring us to further assess the situation. That said, I'm instructing

16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Thank you!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone 613-948-7283
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Cullen, Jennifer: CIO-BI
Sent: Friday, September 21, 2012 4:08 PM
To: DPM-AVE: Anti-Virus Engineering Team
Cc: IT Security; Hagarty, Richard: CIO-BI
Subject: 16(2)(c)

In light of the number of anomalous activities, the Cyber Flash issued by CTEC late this afternoon, and the CCIRC Advisory, 16(2)(c)

16(2)(c)

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone 613-948-4029
Facsimile | Télécopieur 613-946-3367

Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Automatic Notification by / Notification Automatique par HEAT Business Rule Manager

Lacroix, Lise: SBTMS-SMTPE

From: 16(2)(c)@ic.gc.ca
Sent: Monday, September 24, 2012 7:14
To: Cullen, Jennifer: CIO-BI
Cc: IT Service Request / Demande de Service TI; Hagarty, Richard: CIO-BI
Subject: 01269926: New IT Service Request / Nouvelle Demande de Service TI

Note: This is a system generated email. Please do not respond to it.
Note: Ceci est un courriel généré par le système, veuillez ne pas y répondre.

Thank you for your recent request.
According to our Service Level Standards 16(2)(c) this service request must be resolved by: 2012-10-01.
If you have any further questions or problems, please contact your IT support group.

Reference Number: 01269926

-----Request Description / Description de la demande-----

Information- IT Security- Threat and Risk Assessment

Merci d'avoir fait appel à nos services.
Selon notre entente de niveau de service 16(2)(c), votre demande de service sera résolue au plus tard le: 2012-10-01.
Pour de plus amples informations veuillez communiquer avec votre groupe de soutien en TI.

Numéro de référence : 01269926

IT Service Desk / Centre de services TI
(613) 946-5555
mailto:ITServiceDesk@ic.gc.ca / mailto:CentredeservicesTI@ic.gc.ca
Our expertise at your service / Notre expertise à votre service

16(2)(c)

From: Brabant, Mathieu: CIO-BI
Sent: Friday, September 21, 2012 4:39 PM
To: Hagarty, Richard: CIO-BI; Cullen, Jennifer: CIO-BI
Cc: ITSec; DPM-AVE: Anti-Virus Engineering Team; ! IT Service Desk; Peters, Bernadette: CIO-BI; Rivard, Karen: CIO-BI; McCloskey, Paul: CIO-BI (NCR-RCN); Gosselin, Andrée: CIO-BI; Bernard, Mario: CIO-BI
Subject: 16(2)(c)

Hi,

16(2)(c)

16(2)(c)

Mathieu

From: Hagarty, Richard: CIO-BI
Sent: Friday, September 21, 2012 4:16 PM
To: Rivard, Karen: CIO-BI; McCloskey, Paul: CIO-BI (NCR-RCN); Gosselin, Andrée: CIO-BI; Bernard, Mario: CIO-BI
Cc: Cullen, Jennifer: CIO-BI; ITSec; DPM-AVE: Anti-Virus Engineering Team
Subject: Communication for 16(2)(c)

Hi Karen, Paul,

We were just advised that a high number of desktop were detected with a new virus. At the same time, we are told by CTEC aka CSEC that 16(2)(c) 16(2)(c) Although the two (2) incidents are not related, the level of risk suddenly increase requiring us to further assess the situation. That said, I'm instructing

16(2)(c),21(1)(a),21(1)(b)

Thank you!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone 613-948-7283
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Cullen, Jennifer: CIO-BI
Sent: Friday, September 21, 2012 4:08 PM
To: DPM-AVE: Anti-Virus Engineering Team
Cc: IT Security; Hagarty, Richard: CIO-BI
Subject: 16(2)(c)

In light of the number of anomalous activities, the Cyber Flash issued by CTEC late this afternoon, and the CCIRC Advisory, 16(2)(c)

16(2)(c)

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone 613-948-4029
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: 16(2)(c)@ic.gc.ca
Sent: Wednesday, October 17, 2012 14:36
To: ITSec HEAT
Cc: IT Service Request / Demande de Service TI
Subject: 01282321: New Assignment / Nouvelle affectation

-----Request Description / Description de la demande-------------------------

Incident- IT Security Incident- Spyware

Service request # 01282321 has been assigned to you, IT Security or your group, IT Security / Sécurité TI. /
Demande de service # 01282321 a été assigné à toi, IT Security ou à ton équipe, IT Security / Sécurité TI.

User name / Nom du client : 19(1)

Email / Courriel : mailto:19(1)@ic.gc.ca

City / Ville : Dartmouth

Phone / Téléphone : 19(1)

Room / Pièce : N/A

Target Date & Time / Date & heure ciblée : 2012-10-17 @ 18:22:00

----------Call History / Historique de l'appel

2012-10-17 @ 14:27:07 by SDBotelJ - Called Lloyd and he said that he would call Robert and inform him about the alert
---
2012-10-17 @ 14:26:51 by SDBotelJ - Caled Lloyd and he said that he would call Robert and inform him about the alert
---
2012-10-17 @ 14:22:48 by SDBotelJ - Original Email follows:

From: Fournier, Denis: CIO-BI
Sent: Wednesday, October 17, 2012 1:18 PM
To: IT Service Desk - Centre de services TI
Cc: IT Security
Subject: "URGENT" infected computer 16(2)(c)

Service Desk,
Please create a ticket under the client name (Item 2) and assign a technician for immediate 16(2)(c)
The following action needs to be taken ASAP without any delays.

16(2)(c)

Client Name: 19(1)
Client Host:
Client Dept: CIPO

Client Local 19(1)

3. Security logs indicate clients workstation is trying to communicate with a known Malware site that is part of the Cyber Flash: IT Sec Flash SF009-12 Update #3: Canada Post Email Phishing Campaign
4. In the event the client is unreachable this email will also be released to the client. I have contacted the user, he has shutdown his computer.
5. Your immediate cooperation and response is appreciated.

16(2)(c)

Question can be directed to IT Security

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Automatic Notification by / Notification Automatique par HEAT Business Rule Manager

Lacroix, Lise: SBTMS-SMTPE

From: 16(2)(c)@ic.gc.ca
Sent: Thursday, November 1, 2012 12:24
To: ITSec HEAT
Cc: IT Service Request / Demande de Service TI
Subject: 01288291: New Assignment / Nouvelle affectation

-----Request Description / Description de la demande----------

Incident- IT Security Incident- Spyware

Service request # 01288291 has been assigned to you, IT Security or your group, IT Security / Sécurité TI. /
Demande de service # 01288291 a été assigné à toi, IT Security ou à ton équipe, IT Security / Sécurité TI.

User name / Nom du client : 19(1)

Email / Courriel : mailto:19(1)@ic.gc.ca

City / Ville : London

Phone / Téléphone : 19(1)

Room / Pièce : n/a

Target Date & Time / Date & heure ciblée : 2012-11-01 @ 16:02:00

----------Call History / Historique de l'appel----------

2012-11-01 @ 12:18:51 by SDSaumuP - Original Email follows:

From: Noga, Darek: CIO-BI (ONT)
Sent: Thursday, November 1, 2012 12:16 PM
To: IT Service Desk - Centre de services TI; Sodhi, Caroline: CIO-BI (ONT)
Subject: Re: "URGENT" infected computer 16(2)(c)

Hi Caroline,
In Dennis' absence can you please action this urgent request.

From: IT Service Desk - Centre de services TI
Sent: Thursday, November 01, 2012 12:11 PM
To: Noga, Darek: CIO-BI (ONT)
Subject: FW: "URGENT" infected computer 16(2)(c)

As request, ticket 01288291...

Joao-Ricardo Botelho
Chief Informatics Office | Bureau de l'informatique

Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Telephone | Téléphone 613-954-7916
Facsimile | Télécopieur 613-954-7994
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

2012-11-01 @ 12:10:52 by SDBotelJ - Called Darek Noga and inform him about the issue. said to e-mail him the request. sent e-mail

---

2012-11-01 @ 12:05:03 by SDBotelJ - Original Email follows:

From: Fournier, Denis: CIO-BI
Sent: Thursday, November 1, 2012 11:46 AM
To: IT Service Desk - Centre de services TI
Cc: IT Security
Subject: "URGENT" infected computer 16(2)(c)

Service Desk,
Please create a ticket under the client name (Item 2) and assign a technician for immediate 16(2)(c)
The following action needs to be taken ASAP without any delays.

16(2)(c)

Client Name:
Client Host: 19(1)
Client Dept:
Client Local do not have any info on her location

3. Security logs indicate clients workstation is trying to communicate with a known Malware site multiple times that is part of the Cyber Flash: IT Sec Flash SF009-12 Update #3: Canada Post Email Phishing Campaign. The mitigation for this infection is 16(2)(c)
4. In the event the client is unreachable this email will also be released to the client
5. Your immediate cooperation and response is appreciated.

16(2)(c)

Question can be directed to IT Security

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

-
Automatic Notification by / Notification Automatique par HEAT Business Rule Manager

Lacroix, Lise: SBTMS-SMTPE

From: 16(2)(c)@ic.gc.ca
Sent: Thursday, November 15, 2012 10:53
To: ITSec HEAT
Cc: IT Service Request / Demande de Service TI
Subject: 01294387: New Assignment / Nouvelle affectation

-----Request Description / Description de la demande-------------------------

Incident- IT Security Incident- Miscellaneous
Breach of Security

-

Service request # 01294387 has been assigned to you, IT Security or your group, IT Security / Sécurité TI. /
Demande de service # 01294387 a été assigné à toi, IT Security ou à ton équipe, IT Security / Sécurité TI.

User name / Nom du client : 19(1)

Email / Courriel : mailto:19(1)@ic.gc.ca

City / Ville : Gatineau

Phone / Téléphone : 19(1)

Room / Pièce : 19(1)

Target Date & Time / Date & heure ciblée : 2012-11-15 @ 14:34:00

-----------------------Call History / Historique de l'appel

2012-11-15 @ 10:45:01 by SDOliviA - - Attached log file.

2012-11-15 @ 10:44:44 by SDOliviA - - Client reported a 16(2)(c) alert and web browser stopped working.

16(2)(c)

-
Automatic Notification by / Notification Automatique par HEAT Business Rule Manager

Lacroix, Lise: SBTMS-SMTPE

From: 16(2)(c)@ic.gc.ca
Sent: Friday, February 15, 2013 12:40
To: ITSec HEAT
Cc: IT Service Request / Demande de Service TI
Subject: 01337859: New Assignment / Nouvelle affectation

-----Request Description / Description de la demande-------------------------

Incident- IT Security Incident- SCAM SPAM Hoax

-

Service request # 01337859 has been assigned to you, IT Security or your group, IT Security / Sécurité TI. /
Demande de service # 01337859 a été assigné à toi, IT Security ou à ton équipe, IT Security / Sécurité TI.

User name / Nom du client : 19(1)

Email / Courriel : mailto:19(1)@ic.gc.ca

City / Ville : Vancouver

Phone / Téléphone : 19(1)

Room / Pièce : 19(1)

Target Date & Time / Date & heure ciblée : 2013-02-15 @ 16:30:00

----------Call History / Historique de l'appel

2013-02-15 @ 12:31:46 by SDGagnM1 - TSO, if IT Security deems it necessary, please 16(2)(c)

2013-02-15 @ 12:31:01 by SDGagnM1 - Original Email follows:

From: 19(1)
Sent: Friday, February 15, 2013 12:09 PM
To: IT Service Desk - Centre de services TI
Subject: FW: possible phishing...

Hi. Please forward this to IT security so that they can see if they need to look into this. Has my IC email account been compromised and used to send phishing emails?

I have never given out my email password to anyone, on-line or otherwise…

Angela

From: Mail Delivery Subsystem [mailto:16(2)(c)
Sent: Friday, February 15, 2013 9:09 AM

To: 19(1)
Subject: Rejected: 16(2)(c)

Your message

To: 16(2)(c)
Subject: 16(2)(c)
Sent: 2013-02-15 9:05

was deleted without being read on 2013-02-15 9:09.

-
Automatic Notification by / Notification Automatique par HEAT Business Rule Manager

Lacroix, Lise: SBTMS-SMTPE

From: 16(2)(c) @ic.gc.ca
Sent: Thursday, March 7, 2013 11:46
To: ITSec HEAT
Cc: IT Service Request / Demande de Service TI
Subject: 01351254: New Assignment / Nouvelle affectation

-----Request Description / Description de la demande-------------------------

Incident- Incident de la Sécurité TI- Pourriel
ERREUR -Courriel d' ameçonnage

-

Service request # 01351254 has been assigned to you, IT Security or your group, IT Security / Sécurité TI. /
Demande de service # 01351254 a été assigné à toi, IT Security ou à ton équipe, IT Security / Sécurité TI.

User name / Nom du client : 19(1)

Email / Courriel : mailto: 19(1) @ic.gc.ca

City / Ville : Ottawa

Phone / Téléphone : 19(1)

Room / Pièce : 19(1)

Target Date & Time / Date & heure ciblée : 2013-03-07 @ 15:25:00

-----------------------Call History / Historique de l'appel

2013-03-07 @ 11:40:01 by SDCaseyB - - informed Pierre that PC is still on network
---
2013-03-07 @ 11:38:41 by SDCaseyB - - client has recieved two email's saying that messages were undeliverable, however client never sent those emails and they were sent on a day that client was not in the office

16(2)(c),21(1)(b)

-
Automatic Notification by / Notification Automatique par HEAT Business Rule Manager

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Friday, January 11, 2013 16:02
To: CIO IT Change Manager: CIO-BI (NCR-RCN)
Subject: Emergency Change Request

Hi all,

This is a confidential request from CTEC (GC's Cyber Threat Evaluation Centre), reference CE2-013-1602 which requires 16(2)(c),21(1)(b) 16(2)(c),21(1)(b) We request this work be performed this weekend which has been determined to be an acceptable timeframe to the client.

Details are with NSG Security (Rob Edwards).

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: McCloskey, Paul: CIO-BI (NCR-RCN)
Sent: Friday, January 11, 2013 16:14
To: Gosselin, Andrée: CIO-BI
Cc: CIO IT CAB Members; Corman, Chris: CIO-BI; CIO IT Problem Manager; Thibaudeau, Stéphane: CB-BC; IT Security
Subject: Emergency Virtual CAB to address confidential request from CTEC (GC's Cyber Threat Evaluation Centre) RFC # 105769

Importance: High

RFC: **105769**

IR: **105770**

DESCRIPTION OF CHANGE - This is a confidential request from CTEC (GC's Cyber Threat Evaluation Centre), reference CE2-013-1602 which requires 16(2)(c),21(1)(b) 16(2)(c),21(1)(b) We request this work be performed this weekend which has been determined to be an acceptable timeframe to the client.

Details are with NSG Security (Rob Edwards).

The above changes are user impacting and are being requested to be implemented this weekend

If anyone has any issues with these changes being implemented, please advise immediately.

Paul McCloskey
Manager, IT Service Management | Gestionnaire, Gestion des services
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Paul.McCloskey@ic.gc.ca
Telephone | Téléphone 613-954-5511
Facsimile | Télécopieur 613-946-3320
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, September 21, 2012 14:41
To: CTEC
Subject: Cyber Flash / Cybercapsule: GCCF12-006: 16(2)(c) activity

Importance: High

Classification: UNCLASSIFIED

La version francaise suivra.

==========
GC-CTEC - Cyber Flash GCCF12-006
Date: 21 September 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal government.

TITLE
=====
16(2)(c) activity

DETAILS
=======
GC-CTEC has noticed a significant amount of 16(2)(c) activity
16(2)(c) is a large
16(2)(c) which has been installed on millions of machines worldwide. The
is currently being used for various fraudulent moneymaking activities for the authors.

The primary distribution mechanisms of 16(2)(c) are:

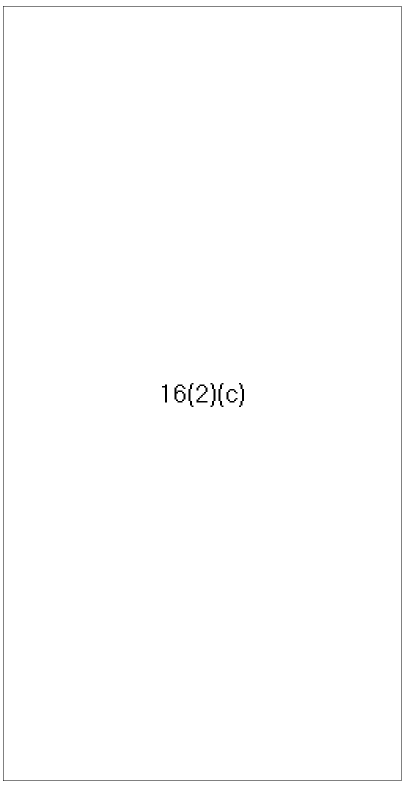
16(2)(c)

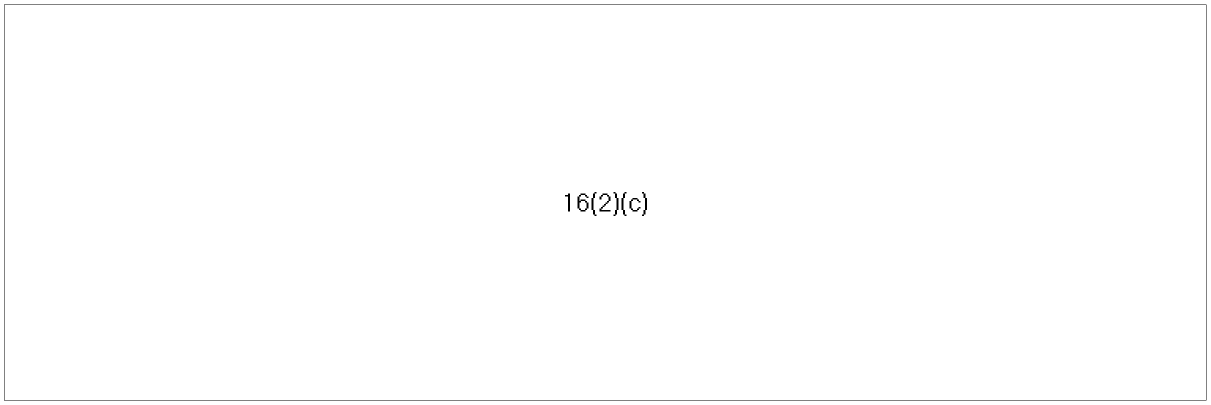
Currently, 16(2)(c) uses 4 static high ports that do not change. They are highly recommended to be 16(2)(c)

16(2)(c)

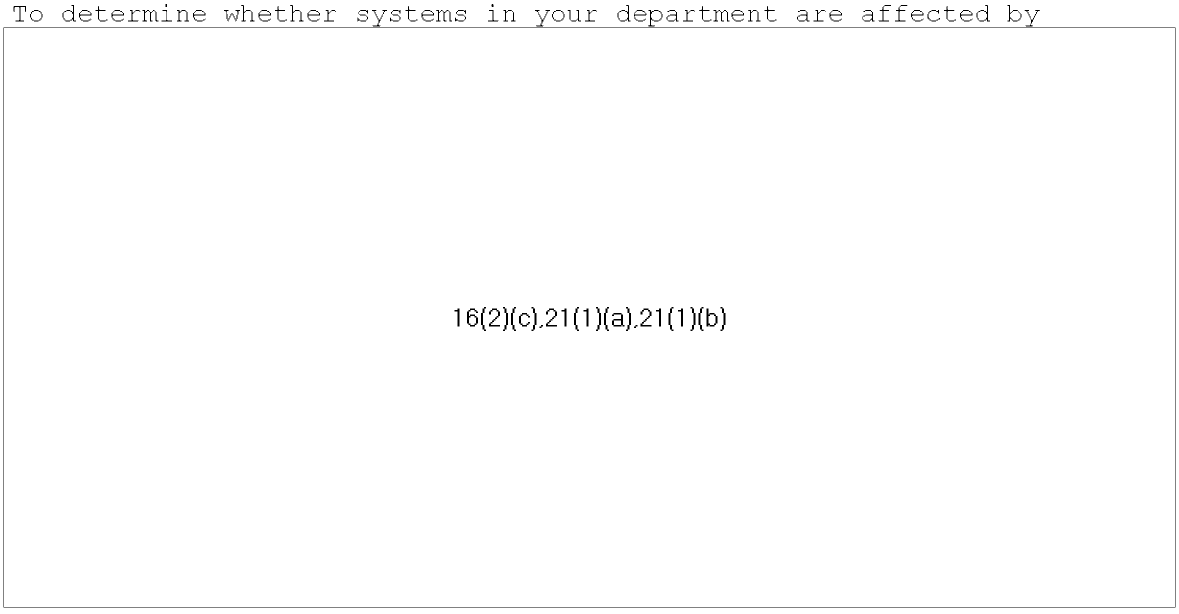
The below domains and IPs are known 16(2)(c) related and should be

16(2)(c)





MITIGATION
==========
To determine whether systems in your department are affected by



Identify infected hosts. Hosts with confirmed infections should be

16(2)(c)

Critical Note:
GC-CTEC provides this information and mitigation advice based on threats to Government of Canada Networks and does not recommend using this information for any other purpose.
The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

References:

16(2)(c)

REPORTING
=========
Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC.

NOTE TO READERS
===============
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC),

aims to strengthen the security of federal information and information systems.
To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca or (613)991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Tuesday, June 12, 2012 11:36
To: Fournier, Denis: CIO-BI
Subject: FW: [CE2012-766]: Login Credentials Exposed in Online Posting

Denis,
Did you get this as well or only IC's Network Security? If IT Security did get it, can you make sure that I am also included?
Thanks,
Jen

From: Phillips, James: SSC-SPC
Sent: Tuesday, June 12, 2012 9:29 AM
To: IT Security
Cc: Network Security - Securite De Reseau
Subject: FW: [CE2012-766]: Login Credentials Exposed in Online Posting

FYI....

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, June 12, 2012 9:25 AM
To: Network Security - Securite De Reseau
Cc: CTEC
Subject: [CE2012-766]: Login Credentials Exposed in Online Posting

Classification: UNCLASSIFIED

Hello,

Recently, it was revealed that a hacking group had broken into the website www.intelconsumerelectronics.com and posted some stolen client data onto another public website known as Pastebin.com.

Your agency is being contacted because someone working there has had their email address posted on Pastebin. The following data was exposed:

19(1)

GC-CTEC recommends that the affected employee be notified and that the employee should exercise heightened caution when opening unrecognized or suspicious emails.

Should you require further information please contact us.

CTEC

15(1)
GC-CTEC Cyber Duty Officer

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, February 6, 2013 10:53
To: Gorman, Joseph: CIO-BI (NCR-RCN); Fournier, Denis: CIO-BI
Subject: FW: CE2013-1703

Fyi. I have given this Cyber Event IT Security Incident number ITSINC-2013-027.
Thanks,
Jen

-----Original Message-----
From: Fournier, Denis: CIO-BI
Sent: Wednesday, February 6, 2013 9:34 AM
To: Cullen, Jennifer: CIO-BI
Subject: FW: CE2013-1703

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, February 5, 2013 4:49 PM
To: Fournier, Denis: CIO-BI
Cc: CTEC
Subject: CE2013-1703

Classification: PROTECTED B

Hello Denis,

Please find attached tipper for your action as soon as possible.

Regards,

15(1)

15(1)
GC-CTEC - Incident Handler
15(1)

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, August 23, 2012 13:27
To: Cullen, Jennifer: CIO-BI
Subject: FW: Cyber Event CE2012-1012 - Malicious email

Similar subject line at CE2012-994

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, August 23, 2012 1:19 PM
To: Pearson, Rod: SSC-SPC
Subject: RE: Cyber Event CE2012-994 - Malicious email

Hi Rod,
Thank you for the report below.

We have received a report that there may have been other attempts to send emails with the same subject line. Can you provide a report starting at the end time of the last report to present? If there are results, would you be able to confirm that the email was 16(2)(c),21(1)(a),21(1)(b) ?

Thank you,
Jennifer

From: Pearson, Rod: SSC-SPC
Sent: Monday, August 20, 2012 3:22 PM
To: Cullen, Jennifer: CIO-BI
Subject: RE: Cyber Event CE2012-994 - Malicious email

Hi Jennifer,

16(2)(c) Recipient list back to Aug 6 is attached. (1 email to 1 recipient)

<< File: CE2012-994_1.csv >>
Rod Pearson
Shared Services Canada | Industry Canada
Services partagés Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Rod.Pearson@ic.gc.ca
Telephone | Téléphone 613-960-8957
Facsimile | Télécopieur 613-946-4932
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Cullen, Jennifer: CIO-BI
Sent: Monday, August 20, 2012 2:05 PM
To: Pearson, Rod: SSC-SPC
Subject: Cyber Event CE2012-994 - Malicious email

Hi Rod,

NOTE: The information contained in this email is for internal user only and must not be disseminated or employed externally. 16(2)(c)
16(2)(c)

CSEC has requested that Industry Canada remove all instances of the following malicious email messages from

departmental email severs and workstations.

16(2)(c)

If you have any questions or concerns, please contact me.
Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Hagarty, Richard: CIO-BI
Sent: Thursday, January 10, 2013 19:08
To: Cullen, Jennifer: CIO-BI
Subject: FW: Ongoing Security Incidents

fyi

From: Hagarty, Richard: CIO-BI
Sent: Thursday, January 10, 2013 7:08 PM
To: Acton, Kelly: CIO-BI; Gosselin, Andrée: CIO-BI
Subject: Ongoing Security Incidents

Hi Kelly, Andrée,

We have received two (2) distinct requests from CSEC/CTEC this week that are consuming significant effort from my team.

The first one is a Cyber Flash requesting from government departments to ensure that GC systems are 16(2)(c),21(1)(a),21(1)(b) 16(2)(c),21(1)(a),21(1)(b) This request requires us to report back to CTEC the status of 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

For the second request, this one is also coming directly from CSEC/CTEC. This is a confidential request which I can not fully disclose. Yet, our current direction received from CTEC might impact the operational activities of Competition Bureau (CB). All the work was conducted in collaboration with the IT Lead at CB. 21(1)(a),21(1)(b)

21(1)(a),21(1)(b)

Have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Friday, September 21, 2012 16:41
To: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Cc: Fournier, Denis: CIO-BI
Subject: FW: 16(2)(c)

FYI Tom.
Thanks,
Jen

From: Brabant, Mathieu: CIO-BI
Sent: Friday, September 21, 2012 4:39 PM
To: Hagarty, Richard: CIO-BI; Cullen, Jennifer: CIO-BI
Cc: ITSec; DPM-AVE: Anti-Virus Engineering Team; ! IT Service Desk; Peters, Bernadette: CIO-BI; Rivard, Karen: CIO-BI; McCloskey, Paul: CIO-BI (NCR-RCN); Gosselin, Andrée: CIO-BI; Bernard, Mario: CIO-BI
Subject: 16(2)(c)

Hi,

16(2)(c),21(1)(a),21(1)(b)

Mathieu

From: Hagarty, Richard: CIO-BI
Sent: Friday, September 21, 2012 4:16 PM
To: Rivard, Karen: CIO-BI; McCloskey, Paul: CIO-BI (NCR-RCN); Gosselin, Andrée: CIO-BI; Bernard, Mario: CIO-BI
Cc: Cullen, Jennifer: CIO-BI; ITSec; DPM-AVE: Anti-Virus Engineering Team
Subject: Communication for 16(2)(c)

Hi Karen, Paul,

We were just advised that a high number of desktop were detected with a new virus. At the same time, we are told by CTEC aka CSEC that 16(2)(c) Although the two (2) incidents are not related, the level of risk suddenly increase requiring us to further assess the situation. That said, I'm instructing DPM 16(2)(c),21(1)(a),21(1)(b) 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Thank you!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389

From: Cullen, Jennifer: CIO-BI
Sent: Friday, September 21, 2012 4:08 PM
To: DPM-AVE: Anti-Virus Engineering Team
Cc: IT Security; Hagarty, Richard: CIO-BI
Subject: 16(2)(c)

In light of the number of anomalous activities, the Cyber Flash issued by CTEC late this afternoon, and the CCIRC Advisory, as a preventative measure, please begin a 16(2)(c) 16(2)(c)

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Monday, September 24, 2012 11:05
To: Fournier, Denis: CIO-BI
Subject: FW: SEP Report - Malware Coverage and Detection

Attachments: Cyber Flash / Cybercapsule: GCCF12-006: 16(2)(c)

Hi Denis,
As per the CTEC Cyber Flash GCCF12-006, we are to 16(2)(c)

16(2)(c)

I asked DPM-AVE: Anti-Virus Engineering Team to run a report to identify systems infected with 16(2)(c) (the result being the attached spreadsheet.

Could you please have Service Desk tickets opened to have the identified systems 16(2)(c) 16(2)(c)

Thanks,
Jen

Cyber Flash / Cybercapsule: GC...

From: Brabant, Mathieu: CIO-BI
Sent: Friday, September 21, 2012 1:16 PM
To: Cullen, Jennifer: CIO-BI
Cc: DPM-AVE: Anti-Virus Engineering Team
Subject: RE: SEP Report - Malware Coverage and Detection

Hi Jen,

If you look at this writeup from 16(2)(c), at the bottom, you will find the various antivirus signatures, 16(2)(c) 16(2)(c) that covers this threat, with their name:

16(2)(c)

Scrolling to 16(2)(c) in the following list, you will be able to see when 16(2)(c) discovered each variant and if you click on one you will get detailed information about it:

16(2)(c)

So far it has only been found on two computers at IC, between August 30th and September 13th. Here is the log:

16(2)(c)

Mathieu

From: Cullen, Jennifer: CIO-BI
Sent: Friday, September 21, 2012 12:30 PM
To: Lemire, Gilles: CIO-BI (NCR-RCN); Brabant, Mathieu: CIO-BI
Subject: SEP Report - Malware Coverage and Detection

Hi Mathieu and Gilles,

Could you please provide a report on what coverage we have in regards to the 16(2)(c)? I am looking for the latest virus definition package we have, all the variations that we are covered for, what version of the virus definitions our systems are covered with, and if there have been any detections.

If you have any questions, please give me a call.

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Hagarty, Richard: CIO-BI
Sent: Tuesday, January 29, 2013 14:08
To: Cullen, Jennifer: CIO-BI
Subject: FW: URGENT - 16(2)(c)

fyi

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

From: Hagarty, Richard: CIO-BI
Sent: Tuesday, January 29, 2013 2:08 PM
To: Thompson, Kim: CAS-SCA
Cc: Gosselin, Andrée: CIO-BI; Hagarty, Richard: CIO-BI
Subject: RE: URGENT - 16(2)(c)

Hi Kim,

It was agreed yesterday that the 16(2)(c) service should remain unavailable until a mitigation plan is put in place to address the current security risk inherent to the current implementation of 16(2)(c). Currently, both parties agreed that, to a minimum, 16(2)(c),21(1)(b)

16(2)(c),21(1)(b)

At this point, the next step is for SSC to provide a detail implementation plan to make 16(2)(c) widely available. The information is required for IC to establish its rollout strategy.

I'll keep you posted as the information comes in.

I understand that I'm providing just a high-level summary of what is currently undertaken. Please let me know if you need more detail. I will also provide our investigative report on the incident as we move forward.

Have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

From: Thompson, Kim: CAS-SCA
Sent: Monday, January 28, 2013 3:53 PM
To: Acton, Kelly: CIO-BI
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA; Strang Lindsey, Robin: CAS-SCA; Hagarty, Richard: CIO-BI; Lamoureux, Marie-Eve: CIO-BI
Subject: RE: URGENT - 16(2)(c)

Thank you for the update Kelly and Richard can keep me apprised of next steps.

Regards,

Kim Thompson
Director, Security and Emergency Management | Directrice de la gestion de la sécurité et des urgences,
Departmental Security Officer | Agent de sécurité ministérielle
Corporate Facilities and Security Branch, CAS | Direction générale de la gestion des installations et de la sécurité, SCA
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Kim.Thompson@ic.gc.ca
Telephone | Téléphone 613-960-6169
Facsimile | Télécopieur 613-957-6543
Teletypewriter | Téléimprimeur 1-866-694-8389

Government of Canada | Gouvernement du Canada

From: Acton, Kelly: CIO-BI
Sent: January 28, 2013 2:51 PM
To: Thompson, Kim: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA; Strang Lindsey, Robin: CAS-SCA; Hagarty, Richard: CIO-BI; Lamoureux, Marie-Eve: CIO-BI
Subject: RE: URGENT - 16(2)(c)

Hi Kim,
By way of an update, I can confirm that based on SSC's analysis over the weekend, no are no longer concerned about the two specific 16(2)(c) accounts; therefore, as was the case at the outset, this incident concerns a single compromised account, and the actions that were taken by SSC and IT Security in response to that account are already well documented.

The 16(2)(c) service remains unavailable and I'm being briefed this afternoon at 4pm by SSC on options for next steps and timelines and can update you further coming out of that discussion. You are welcome to attend the discussion if you wish, but Richard will be there and can debrief accordingly.

Kelly Acton
A/Director General, Planning and Customer Relations |
Directrice générale intérimaire, Planification et relations avec la clientèle
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise

Industry Canada | Industrie Canada
235 rue Queen Street, Ottawa ON K1A 0H5
Office/Room: 388B West Tower
613-941-3445

From: Hagarty, Richard: CIO-BI
Sent: Monday, January 28, 2013 1:06 PM
To: Thompson, Kim: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Acton, Kelly: CIO-BI; Gosselin, Andrée: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Subject: RE: URGENT - 16(2)(c)

Hi Kim,

As you may have seen on Friday, the decision was taken to 16(2)(c) service due to an increased level of phishing activity. An IT Bulletin was issued advising the department of the situation. Over the weekend, Shared Services Canada conducted a detail analysis to further assess the situation. It is expected that Shared Services Canada will provide a debrief of the findings before the end of the day.

I will provide further detail once we have been briefed and the situation is well understood.

Have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

From: Gosselin, Andrée: CIO-BI
Sent: Friday, January 25, 2013 1:57 PM
To: Thompson, Kim: CAS-SCA; Hagarty, Richard: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; IT Security
Subject: Re: URGENT - 16(2)(c) - High Security Risk

Kim,
We are currently discussing next steps. Will give you an update as soon as possible.
Andrée

From: Thompson, Kim: CAS-SCA
Sent: Friday, January 25, 2013 01:51 PM
To: Hagarty, Richard: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; IT Security
Subject: RE: URGENT - 16(2)(c) - High Security Risk

Ok, thanks Richard, I will advise Robin and Susan as a "heads-up" as we do here.

Can you provide me with a brief overview of what your next steps are as Susan will ask? What will CIO or SSC be undertaking? Timelines? Who is conducting the Injury Assessment on the possible security breach?

Thanks,

Kim Thompson
Director, Security and Emergency Management | Directrice de la gestion de la sécurité et des urgences,
Departmental Security Officer | Agent de sécurité ministérielle
Corporate Facilities and Security Branch, CAS | Direction générale de la gestion des installations et de la sécurité, SCA
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Kim.Thompson@ic.gc.ca
Telephone | Téléphone 613-960-6169
Facsimile | Télécopieur 613-957-6543
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada C:\Documents and Settings\THOMPSOK\Desktop\top100_b_2011_e_blk.jpg

---

From: Hagarty, Richard: CIO-BI
Sent: January 25, 2013 1:24 PM
To: Thompson, Kim: CAS-SCA; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; IT Security
Subject: FW: URGENT - 16(2)(c) - High Security Risk

Hi Kim,
Please note that we are currently investigating an internal incident that started as a typical Phishing campaign . We will send the update as we have more detail on it.
Have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Monday, June 4, 2012 10:41
To: 'CTEC'
Cc: IT Security
Subject: IC_IT_Sec07-12_IMP Cyber Incident Report

Attachments: IC_IT_Sec07-12_IMP Cyber Incident Report.doc; Possible Phishing Attempt; Possible Phishing attempt

Report issued on behalf of Industry Canada's IT Security Division. Report based on Possible Phishing Attempt entitled 16(2)(c)


IC_IT_Sec07-12_IM P Cyber Incid...


Possible Phishing Attempt


Possible Phishing attempt

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

Industry Canada IT Security 07-12 IMP Cyber Incident Report

1.0 Reporting Entity

Department or Agency:	Industry Canada

2.0 Contact Information

First name:	Thomas	Initials:	M
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 954-2796	Cell:	(613) 784-9671
Pager:	(613) 868-4784	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address: 235 Queen, Ottawa, On			

3.0 Incident Type (Delete any categories that do not apply)

Malicious code	N/A
Known vulnerability exploit	*N/A*
System compromise	Possible
Data compromise	Possible
Denial of service	N/A
Access violation	Possible
Accident or error	Unk
Other or unknown	Possible Phishing Attempt

4.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	HTTP
Application	Unknown

5.0 Incident Description and Impact

Date and time of incident:	Advised on 1549hrs 31st May 2012
Location of site affected by incident:	
Various IC Locations	
Estimated impact:	Possible client credentials exposed
Incident duration:	N/A
Estimated number of users affected:	573 affected users

Percentage of departmental systems affected:	N/A
Identify what departmental or public services were affected	N/A
Brief description of the incident:	
IT Security was advised of the circulation of a Possible Phishing attempt 1549hrs 31st May 2012. Suspected email was entitled 16(2)(c) with a link attached.	
Actions taken:	
Upon acknowledgement of Possible Phishing attempt, IT Security immediately 16(2)(c) 16(2)(c)	
Supporting documents attached:	
See attached emails	

6.0 Status of Mitigation Actions

Mitigation Actions:	List of recipients receive 0856hrs 1st June of who may have received this possible phishing attempt. Email sent to all clients at 0928hrs 1st June 2012 advising them if they clicked on the link to contact IT Security and that 16(2)(c) 16(2)(c)
Results:	N/A
Additional assistance required?	N/A

7.0 Apparent Origin of Incident or Attack

Source IP and port:	Secure fax	Protocol:	HTTP
URL:			

Note: Electronic data exchange details are available from the CCIRC.

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Tuesday, June 5, 2012 7:44
To: 'CTEC'
Cc: IT Security
Subject: IC_IT_Sec08-12_IMP Cyber Incident Report

Attachments: IC_IT_Sec08-12_IMP Cyber Incident Report.doc; 16(2)(c)

Report issued on behalf of Industry Canada's IT Security Division. Report based on Possible Phishing Attempt entitled 16(2)(c)

IC_IT_Sec08-12_IM
P Cyber Incid...

16(2)(c)

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Industry Canada IT Security 08-12 IMP Cyber Incident Report

1.0 Reporting Entity

Department or Agency:	Industry Canada

2.0 Contact Information

First name:	Denis	Initials:	M
Last name:	Fournier	Position:	IT Security Officer
Phone:	(613) 946-4343	Cell:	(613) 868-4784
Pager:	(613) 868-4784	Fax:	(613) 946-3367
Email:	Denis.fournier@ic.gc.ca		
Office address: 235 Queen, Ottawa, On			

3.0 Incident Type (Delete any categories that do not apply)

Malicious code	N/A
Known vulnerability exploit	*N/A*
System compromise	Possible
Data compromise	Possible
Denial of service	N/A
Access violation	Possible
Accident or error	Unknown
Other or unknown	Possible Phishing Attempt

4.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	HTTP
Application	Unknown

5.0 Incident Description and Impact

Date and time of incident:	Advised on 1351hrs 4th June 2012
Location of site affected by incident:	
Various IC Locations	
Estimated impact:	Possible client credentials exposed
Incident duration:	N/A
Estimated number of users affected:	258 affected users

Percentage of departmental systems affected:	N/A
Identify what departmental or public services were affected	N/A
Brief description of the incident:	
IT Security was advised of the circulation of a Possible Phishing attempt 1351hrs 4th June 2012. Suspected email was entitled " 16(2)(c) with a link attached.	
Actions taken:	
Upon acknowledgement of Possible Phishing attempt, IT Security immediately 16(2)(c) 16(2)(c)	
Supporting documents attached:	
See attached email	

6.0 Status of Mitigation Actions

Mitigation Actions:	List of recipients receive 1400hrs 4th June of who may have received this possible phishing attempt. Email sent to all clients at 0700hrs 5th June 2012 advising them if they clicked on the link to contact IT Security and that 16(2)(c) 16(2)(c)
Results:	N/A
Additional assistance required?	N/A

7.0 Apparent Origin of Incident or Attack

Source IP and port:	
URL:	16(2)(c)

Note: Electronic data exchange details are available from the CCIRC.

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Friday, June 22, 2012 13:09
To: 'CTEC'
Cc: IT Security
Subject: IC_IT_Sec10-12_IMP. IC_IT_Sec11-12_IMP IC_IT_Sec12-12_IMP Cyber Incident Reports

Attachments: IC_IT_Sec10-12_IMP Cyber Incident Report.doc; IC_IT_Sec11-12_IMP Cyber Incident Report.doc; IC_IT_Sec12-12_IMP Cyber Incident Report.doc

Reports issued on behalf of Industry Canada's IT Security Division

[C_IT_Sec10-12_IM P Cyber Incid... C_IT_Sec11-12_IM P Cyber Incid... C_IT_Sec12-12_IM P Cyber Incid...

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Industry Canada IT Security 10-12 IMP Cyber Incident Report

1.0 Reporting Entity

Department or Agency:	Industry Canada

2.0 Contact Information

First name:	Thomas	Initials:	M
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 954-2796	Cell:	(613) 784-9671
Pager:	(613) 868-4784	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address: 235 Queen, Ottawa, On			

3.0 Incident Type (Delete any categories that do not apply)

Malicious code	N/A
Known vulnerability exploit	*N/A*
System compromise	Possible
Data compromise	Possible
Denial of service	N/A
Access violation	Possible
Accident or error	N/A
Other or unknown	Possible Phishing Attempt

4.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	HTTP
Application	Unknown

5.0 Incident Description and Impact

Date and time of incident:	Advised on 1735hrs 11th June 2012
Location of site affected by incident:	
Various IC Locations	
Estimated impact:	Undetermined
Incident duration:	N/A
Estimated number of users affected:	Undetermined

Percentage of departmental systems affected:	N/A
Identify what departmental or public services were affected	N/A
Brief description of the incident:	
IT Security was advised of the circulation of a Possible Phishing attempt 1735hrs 11th June 2012. Suspected email v 16(2)(c) with a link attached. Approx 12 Industry Clients received the email.	
Actions taken:	
Upon acknowledgement of Possible Phishing attempt, IT Security immediately 16(2)(c) 16(2)(c) respectively Email was sent to all recipients advising them of this possible attempt. Clients were advised to contact IT they had clicked on the link associated with the email.	
Supporting documents attached:	
Copy of email received	

16(2)(c)

6.0 Status of Mitigation Actions

Mitigation Actions:	List of recipients received @ 0832hrs 12th June of who may have received this possible phishing attempt. Email sent to all clients at 0845hrs 12th June 2012 advising them if they clicked on the link to contact IT Security and that 16(2)(c)
Results:	N/A
Additional assistance required?	N/A

7.0 Apparent Origin of Incident or Attack

Source IP and port:	N/A	Protocol:	HTTP
URL:			

Note: Electronic data exchange details are available from the CCIRC.

Industry Canada IT Security 11-12 IMP Cyber Incident Report

1.0 Reporting Entity

Department or Agency:	Industry Canada

2.0 Contact Information

First name:	Thomas	Initials:	M
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 954-2796	Cell:	(613) 784-9671
Pager:	(613) 868-4784	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address: 235 Queen, Ottawa, On			

3.0 Incident Type (Delete any categories that do not apply)

Malicious code	N/A
Known vulnerability exploit	*N/A*
System compromise	Possible
Data compromise	Possible
Denial of service	N/A
Access violation	Possible
Accident or error	N/A
Other or unknown	Possible Phishing Attempt

4.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	HTTP
Application	Unknown

5.0 Incident Description and Impact

Date and time of incident:	Advised on 1607hrs 11th June 2012
Location of site affected by incident:	
Various IC Locations	
Estimated impact:	Undetermined
Incident duration:	N/A
Estimated number of users affected:	Undetermined

Percentage of departmental systems affected:	N/A
Identify what departmental or public services were affected	N/A
Brief description of the incident:	
IT Security was advised of the circulation of a Possible Phishing attempt 1735hrs 11th June 2012. Suspected e entitled 16(2)(c) with a link attached. Approx 47 Industry Clients received the email.	
Actions taken:	
Upon acknowledgement of Possible Phishing attempt, IT Security immediately 16(2)(c) 16(2)(c) respectively. Email was sent to all recipients advising them of this possible attempt. Clients were advised to contact IT if they had clicked on the link associated with the email.	
Supporting documents attached:	

16(2)(c)

6.0 Status of Mitigation Actions

Mitigation Actions:	List of recipients received @ 0830hrs 12th June of who may have received this possible phishing attempt. Email sent to all clients at 0845hrs 12th June 2012 advising them if they clicked on the link to contact IT Security and that 16(2)(c)
Results:	N/A
Additional assistance required?	N/A

7.0 Apparent Origin of Incident or Attack

Source IP and port:		Protocol:	HTTP
URL:			

Note: Electronic data exchange details are available from the CCIRC.

CTEC GC IT IMP Report Number: CE2012-766

Industry Canada IT Security Incident Number: ITSINC-2012-023

Industry Canada IT Security 12-12 IMP Cyber Incident Report

1.0 Reporting Entity

Name of organization:	Industry Canada (ITO-OTI)

2.0 Contact Information

First name:	Denis	Initials:	M.
Last name:	Fournier	Position:	IT Security Officer
Phone:	(613) 946-4343	Cell:	(613) 868-4784
Pager:	(613) 868-4784	Fax:	(613) 946-3367
Email:	Denis.fournier@ic.gc.ca		
Office address:	235 Queen, Ottawa, On		

3.0 Incident Description and Impact

Date and time of incident:	Advised on 0930hrs 12th June 2012

Location of site affected by incident: 235 Queen street, Ottawa, On, 7th floor

(if more than one site is affected, please list)

Estimated impact:	N/A
Incident duration:	N/A

Estimated number of systems affected:	1 Client/User
Percentage of departmental systems affected:	N/A

Brief description of the incident: Recently, it was revealed that a hacking group had broken into the

CTEC GC IT IMP Report Number: CE2012-766 **Industry Canada IT Security Incident Number: ITSINC-2012-023** Industry Canada IT Security 12-12 IMP Cyber Incident Report
website www.intelconsumerelectronics.com and posted some stolen client data onto another public website known as Pastebin.com. Industry Canada was contacted because someone working at IC has had their email address posted on Pastebin.
Actions taken: The client was contacted and informed of the situation. He was notified to exercise heightened caution when opening unrecognized or suspicious emails. Client did not take any chances and changed his network and Outlook passwords. He explained to me that he does not recognize the website.
(2012-06-12 @ 1300hrs)
Supporting documents attached:
N/A

4.0 Status of Mitigation Actions

Mitigation details to date:	Contacted client, he decided to change his network and Outlook passwords.
Results of mitigation:	Nil
Additional assistance required?	NO

5.0 Incident Type

Malicious code	N/A
Known vulnerability exploit	*CE2012-766 Login Credentials Exposed on Public Website*

CTEC GC IT IMP Report Number: CE2012-766 **Industry Canada IT Security Incident Number: ITSINC-2012-023** Industry Canada IT Security 12-12 IMP Cyber Incident Report	
System compromise	N/A
Data compromise	N/A
Denial of service	N/A
Access violation	None
Accident or error Other or unknown	Unknown N/A

6.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	SMTP
Application	Unknown

7.0 Apparent Origin of Incident or Attack

Source IP and port:	Unknown	Protocol:	SMTP
URL:	(if any)	Malware:	(if any)

Note: Electronic data exchange details are available from the CTEC.

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Tuesday, June 12, 2012 15:15
To: IT Security
Subject: IC_IT_Sec10-12_IMP Cyber Incident Report

Attachments: ITS_GCITIMP_ 10-12_IMP Cyber Incident Report.doc

Team

Please review and advise before I send out

Thanks

ITS_GCITIMP_
.0-12_IMP Cyber I..

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

CTEC GC IT IMP Report Number: CE2012-766

Industry Canada IT Security Incident Number: ITSINC-2012-023

1.0 Reporting Entity

Name of organization:	Industry Canada (ITO-OTI)

2.0 Contact Information

First name:	Denis	Initials:	M.
Last name:	Fournier	Position:	IT Security Officer
Phone:	(613) 946-4343	Cell:	(613) 868-4784
Pager:	(613) 868-4784	Fax:	(613) 946-3367
Email:	Denis.fournier@ic.gc.ca		
Office address:	235 Queen, Ottawa, On		

3.0 Incident Description and Impact

Date and time of incident:	Advised on 0930hrs 12th June 2012

Location of site affected by incident: 235 Queen street, Ottawa, On, 7th floor

(if more than one site is affected, please list)

Estimated impact:	N/A
Incident duration:	N/A

Estimated number of systems affected:	1 Client/User
Percentage of departmental systems affected:	N/A

Brief description of the incident: Recently, it was revealed that a hacking group had broken into the website www.intelconsumerelectronics.com and posted some stolen client data onto another public

CTEC GC IT IMP Report Number: CE2012-766 **Industry Canada IT Security Incident Number: ITSINC-2012-023**
website known as Pastebin.com. Industry Canada was contacted because someone working at IC has had their email address posted on Pastebin.
Actions taken: The client was contacted and informed of the situation. He was notified to exercise heightened caution when opening unrecognized or suspicious emails. Client did not take any chances and changed his network and Outlook passwords. He explained to me that he does not recognize the website.
(2012-06-12 @ 1300hrs)
Supporting documents attached:
N/A

4.0 Status of Mitigation Actions

Mitigation details to date:	Contacted client, he decided to change his network and Outlook passwords.
Results of mitigation:	Nil
Additional assistance required?	NO

5.0 Incident Type

Malicious code	N/A
Known vulnerability exploit	*CE2012-766 Login Credentials Exposed on Public Website*
System compromise	N/A

CTEC GC IT IMP Report Number: CE2012-766 Industry Canada IT Security Incident Number: ITSINC-2012-023	
Data compromise	N/A
Denial of service	N/A
Access violation	None
Accident or error	Unknown
Other or unknown	N/A

6.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	SMTP
Application	Unknown

7.0 Apparent Origin of Incident or Attack

Source IP and port:	Unknown	Protocol:	SMTP
URL:	(if any)	Malware:	(if any)

Note: Electronic data exchange details are available from the CTEC.

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Friday, June 22, 2012 13:26
To: 'CTEC'
Cc: IT Security
Subject: IC_IT_Sec13-12_IMP Cyber Incident Reports

Attachments: IC_IT_Sec13-12_IMP Cyber Incident Report.doc

Report issued on behalf of IC IT Securities Division

IC_IT_Sec13-12_IM
P Cyber Incid...

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

CTEC GC IT IMP Report Number: CE2012-766

Industry Canada IT Security Incident Number: ITSINC-2012-024

Industry Canada IT Security 13-12 IMP Cyber Incident Report

1.0 Reporting Entity

Name of organization:	Industry Canada (ITO-OTI)

2.0 Contact Information

First name:	Thomas	Initials:	M.
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 952-2796	Cell:	(613) 784-9571
Pager:	N/A	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address:	235 Queen, Ottawa, On		

3.0 Incident Description and Impact

Date and time of incident:	Advised on 1306hrs 21th June 2012
Location of site affected by incident: Various	
(if more than one site is affected, please list)	
Estimated impact:	N/A
Incident duration:	N/A
Estimated number of systems affected:	135
Percentage of departmental systems affected:	N/A
Brief description of the incident: IT Security was advised of the circulation of a Possible Phishing attempt	

CTEC GC IT IMP Report Number: CE2012-766 **Industry Canada IT Security Incident Number: ITSINC-2012-024** Industry Canada IT Security 13-12 IMP Cyber Incident Report
1306hrs 21st June 2012. Suspected email was entitled " 16(2)(c) with out quotes and with the following link attached "https://docs[dot]google[dot]com/spreadsheet/viewform?formkey=dEo0M1FkSk6oeHZGUVluUmFnYS1MTVc6MQ" without quotes Approx 135 Industry Clients received the email..
Actions taken: 16(2)(c) 16(2)(c) An email was sent to all IC clients who had received subj email advising them to contact IT Security if they clicked on the associated link
Supporting documents attached:
16(2)(c)

4.0 Status of Mitigation Actions

Mitigation details to date:	16(2)(c) clients advised of possible Phishing attempt
Results of mitigation:	Nil

CTEC GC IT IMP Report Number: CE2012-766 Industry Canada IT Security Incident Number: ITSINC-2012-024 Industry Canada IT Security 13-12 IMP Cyber Incident Report	
Additional assistance required?	NO
5.0 Incident Type	
Malicious code	N/A
Known vulnerability exploit	N/A
System compromise	Possible
Data compromise	Possible
Denial of service	N/A
Access violation	Possible
Accident or error	N/A
Other or unknown	Possible Phishing Attempt
6.0 Systems Affected	
Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	SMTP
Application	Unknown

CTEC GC IT IMP Report Number: CE2012-766 **Industry Canada IT Security Incident Number: ITSINC-2012-024** Industry Canada IT Security 13-12 IMP Cyber Incident Report			
Note: Electronic data exchange details are available from the CTEC.			

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Wednesday, June 27, 2012 14:12
To: Cullen, Jennifer: CIO-BI; Fewer, Art: CIO-BI; Fournier, Denis: CIO-BI; Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Subject: IC_IT_Sec14-12_IMP Cyber Incident Report

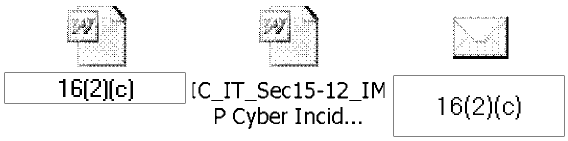
Attachments: smime.p7m

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Thursday, July 5, 2012 8:48
To: 'CTEC'
Cc: IT Security
Subject: IC_IT_Sec15-12_IMP Cyber Incident Reports

Attachments: 16(2)(c) IC_IT_Sec15-12_IMP Cyber Incident Report_V2.doc; 16(2)(c)

Report issued on behalf of IC IT Securities Division



Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

CTEC GC IT IMP Report Number:

Industry Canada IT Security Incident Number: ITSINC-2012-026

Industry Canada IT Security 15-12 IMP Cyber Incident Report

1.0 Reporting Entity

Name of organization:	Industry Canada (IC-DM-IC-SM)

2.0 Contact Information

First name:	Denis	Initials:	M.
Last name:	Fournier	Position:	IT Security Officer
Phone:	(613) 946-4343	Cell:	(613) 868-4784
Pager:	N/A	Fax:	(613) 946-3367
Email:	Denis.fournier@ic.gc.ca		
Office address:	235 Queen, Ottawa, On		

3.0 Incident Description and Impact

Date and time of incident:	Advised on 4th July 2012 at 1417hrs
Location of site affected by incident:	
(if more than one site is affected, please list) Ottawa	
Estimated impact:	N/A
Incident duration:	N/A
Estimated number of systems affected:	3

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-026** Industry Canada IT Security 15-12 IMP Cyber Incident Report	
Percentage of departmental systems affected:	N/A
Brief description of the incident:	
IT Security was advised of the circulation of a Possible Phishing attempt 1417hrs 4th July 2012. Suspected email was entitled 16(2)(c) with out quotes and with the following link attached 16(2)(c) without quotes Approx 3 Industry Clients received the email..	
Actions taken:	
16(2)(c) 16(2)(c) An email was sent to all IC clients who had received subj email advising them to contact IT Security if they clicked on the associated link	
Supporting documents attached: Header and email is attached	

4.0 Status of Mitigation Actions

Mitigation details to date:	16(2)(c) clients advised of possible Phishing attempt
Results of mitigation:	Nil
Additional assistance required?	NO

5.0 Incident Type

Malicious code	N/A

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-026** Industry Canada IT Security 15-12 IMP Cyber Incident Report	
Known vulnerability exploit	N/A
System compromise	Possible
Data compromise	Possible
Denial of service	N/A
Access violation Accident or error	Possible N/A
Other or unknown	Possible Phishing Attempt

6.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	SMTP
Application	Unknown

Note: Electronic data exchange details are available from the CTEC.

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Wednesday, July 4, 2012 15:03
To: IT Security
Subject: IC_IT_Sec15-12_IMP Cyber Incident Report.doc

Attachments: IC_IT_Sec15-12_IMP Cyber Incident Report.doc

Please review before sending toi CTEC

IC_IT_Sec15-12_IM
P Cyber Incid...

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

CTEC GC IT IMP Report Number:

Industry Canada IT Security Incident Number: ITSINC-2012-026

Industry Canada IT Security 15-12 IMP Cyber Incident Report

1.0 Reporting Entity

Name of organization:	Industry Canada (IC-DM-IC-SM)

2.0 Contact Information

First name:	Denis	Initials:	M.
Last name:	Fournier	Position:	IT Security Officer
Phone:	(613) 946-4343	Cell:	(613) 868-4784
Pager:	N/A	Fax:	(613) 946-3367
Email:	Denis.fournier@ic.gc.ca		
Office address:	235 Queen, Ottawa, On		

3.0 Incident Description and Impact

Date and time of incident:	Advised on 4th July 2012 at 1417hrs

Location of site affected by incident: Ottawa

(if more than one site is affected, please list)

Estimated impact:	N/A
Incident duration:	N/A

Estimated number of systems affected:	3
Percentage of departmental systems affected:	N/A

Brief description of the incident: IT Security was advised of the circulation of a Possible Phishing

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-026** Industry Canada IT Security 15-12 IMP Cyber Incident Report
attempt 1417hrs 4th July 2012. Suspected email was entitled 16(2)(c) with out quotes and with the following link attached 16(2)(c) without quotes Approx 3 Industry Clients received the email..
Actions taken: 16(2)(c) 16(2)(c) An email was sent to all IC clients who had received subj email advising them to contact IT Security if they clicked on the associated link
Supporting documents attached: Header and email is attached

4.0 Status of Mitigation Actions

Mitigation details to date:	16(2)(c) clients advised of possible Phishing attempt
Results of mitigation:	Nil
Additional assistance required?	NO

5.0 Incident Type

Malicious code	N/A
Known vulnerability exploit	N/A
System compromise	Possible

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-026** Industry Canada IT Security 15-12 IMP Cyber Incident Report	
Data compromise	Possible
Denial of service	N/A
Access violation	Possible
Accident or error	N/A
Other or unknown	Possible Phishing Attempt

6.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	SMTP
Application	Unknown

Note: Electronic data exchange details are available from the CTEC.

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Wednesday, July 11, 2012 12:11
To: IT Security
Subject: IC_IT_Sec16-12_IMP Cyber Incident Report

Attachments: IC_IT_Sec16-12_IMP Cyber Incident Report.doc

Please review. Will release at 1500hrs

IC_IT_Sec16-12_IM
P Cyber Incid...

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-027** Industry Canada IT Security 16-12 IMP Cyber Incident Report

1.0 Reporting Entity

Name of organization:	Industry Canada (IC-DM-IC-SM)

2.0 Contact Information

First name:	Thomas	Initials:	M.
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 952-2796	Cell:	(613) 784-9571
Pager:	N/A	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address:	235 Queen, Ottawa, On		

3.0 Incident Description and Impact

Date and time of incident:	Advised on 11th July 2012 at 0943hrs
Location of site affected by incident: Ottawa	
(if more than one site is affected, please list)	
Estimated impact:	N/A
Incident duration:	N/A
Estimated number of systems affected:	7
Percentage of departmental systems affected:	N/A

CTEC GC IT IMP Report Number:

Industry Canada IT Security Incident Number: ITSINC-2012-027

Industry Canada IT Security 16-12 IMP Cyber Incident Report

Brief description of the incident: IT Security was advised of the circulation of a Possible Phishing @ 1823hrs 10th July 2012 a possible Phishing attempt was conducted on an IC mail address. Suspected email entitled 16(2)(c) with out quotes was received by a client within IC. IT Security was advised at 0943hrs 11th July of offending emails and 16(2)(c) 16(2)(c) (Please see actions taken. The email was received by 7 Industry Canada clients.

Actions taken: 16(2)(c) 16(2)(c) all 7 IC clients who had received subj email advising them to contact IT Security if they clicked on the associated link.

CTEC GC IT IMP Report Number: Industry Canada IT Security Incident Number: ITSINC-2012-027 Industry Canada IT Security 16-12 IMP Cyber Incident Report
Supporting documents attached:

16(2)(c)

4.0 Status of Mitigation Actions

Mitigation details to date:	16(2)(c) clients advised of possible Phishing attempt

CTEC GC IT IMP Report Number: Industry Canada IT Security Incident Number: ITSINC-2012-027 Industry Canada IT Security 16-12 IMP Cyber Incident Report	
Results of mitigation:	16(2)(c)
Additional assistance required?	NO

5.0 Incident Type

Malicious code	N/A
Known vulnerability exploit	N/A
System compromise	TBD
Data compromise	N/A
Denial of service	N/A
Access violation	TBD
Accident or error	N/A
Other or unknown	Possible Phishing Attempt

6.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	SMTP

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-027** Industry Canada IT Security 16-12 IMP Cyber Incident Report			
Application	Unknown		
Note: Electronic data exchange details are available from the CTEC.			

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Thursday, July 12, 2012 7:49
To: 'CTEC'
Cc: IT Security
Subject: IC_IT_Sec16-12_IMP Cyber Incident Report

Attachments: IC_IT_Sec16-12_IMP Cyber Incident Report.doc

Report issued on behalf of Industry Canada's IT Securities Division

IC_IT_Sec16-12_IM
P Cyber Incid...

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-027** Industry Canada IT Security 16-12 IMP Cyber Incident Report

1.0 Reporting Entity

Name of organization:	Industry Canada (IC-DM-IC-SM)

2.0 Contact Information

First name:	Thomas	Initials:	M.
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 952-2796	Cell:	(613) 784-9571
Pager:	N/A	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address:	235 Queen, Ottawa, On		

3.0 Incident Description and Impact

Date and time of incident:	Advised on 11th July 2012 at 0943hrs
Location of site affected by incident: Ottawa	
N/A	
Estimated impact:	N/A
Incident duration:	N/A
Estimated number of systems affected:	7
Percentage of departmental systems affected:	N/A

CTEC GC IT IMP Report Number:

Industry Canada IT Security Incident Number: ITSINC-2012-027

Industry Canada IT Security 16-12 IMP Cyber Incident Report

Brief description of the incident:

@ 1823hrs 10th July 2012 a possible Phishing attempt was conducted on an IC mail address. Suspected email entitled 16(2)(c) with out quotes was received by a client within IC. IT Security was advised at 0943hrs 11th July of offending emails and 16(2)(c)

16(2)(c)

Actions taken:

16(2)(c)

CTEC GC IT IMP Report Number:

Industry Canada IT Security Incident Number: ITSINC-2012-027

Industry Canada IT Security 16-12 IMP Cyber Incident Report

16(2)(c)

4.0 Status of Mitigation Actions

Mitigation details to date:	16(2)(c)
	16(2)(c) No further action required

CTEC GC IT IMP Report Number: Industry Canada IT Security Incident Number: ITSINC-2012-027 Industry Canada IT Security 16-12 IMP Cyber Incident Report	
Results of mitigation:	16(2)(c)
Additional assistance required?	NO
5.0 Incident Type	
Malicious code	N/A
Known vulnerability exploit	N/A
System compromise	TBD
Data compromise	N/A
Denial of service	N/A
Access violation	TBD
Accident or error	N/A
Other or unknown	Possible Phishing Attempt
6.0 Systems Affected	
Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	SMTP

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-027** Industry Canada IT Security 16-12 IMP Cyber Incident Report			
Application	Unknown		
Note: Electronic data exchange details are available from the CTEC.			

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Wednesday, May 16, 2012 17:37
To: 'CTEC'
Cc: IT Security
Subject: IMP Cyber Incident Report IC IT_Sec 05-12

Attachments: IC_IT_Sec05-12_IMP Cyber Incident Report.doc; [CE2012-615]: University of New Brunswick Compromised - Information Posted to Public Forum

Report issued on behalf of Industry Canada's IT Security based on CSEC's CE2012-615: University of New Brunswick Compromised - Information Posted to Public Forum

IC_IT_Sec05-12_IM
P Cyber Incid...

[CE2012-615]:
University of Ne...

Questions can be directed to the undersigned.

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

Industry Canada IT Security 05-12 IMP Cyber Incident Report

1.0 Reporting Entity

Department or Agency:	Industry Canada

2.0 Contact Information

First name:	Thomas	Initials:	M
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 954-2796	Cell:	(613) 784-9671
Pager:	(613) 868-4784	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address: 235 Queen, Ottawa, On			

3.0 Incident Type (Delete any categories that do not apply)

Malicious code	N/A
Known vulnerability exploit	*CE2012-615 UNB hacked resulting in privileged information being posted to a known public website.*
System compromise	Unknown
Data compromise	Unknown
Denial of service	N/A
Access violation	Possible
Accident or error	N/A
Other or unknown	N/A

4.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	HTTP
Application	Unknown

5.0 Incident Description and Impact

Date and time of incident:	Advised on 1559hrs 16th May 2012
Location of site affected by incident:	
N/A	
Estimated impact:	Possible data leak
Incident duration:	N/A
Estimated number of systems affected:	1 Client/User

Percentage of departmental systems affected:	N/A
Identify what departmental or public services were affected	N/A
Brief description of the incident:	
Industry Canada was advised of possible stolen electronic data from UNB. The stolen data was possibly posted on a public website. An email resembling one that could be associated to IC was realized and information was forwarded on to IC IT Security.	
Actions taken:	
A review of the possible email and varieties thereof was conducted and found to be invalid. No further action required.	
Supporting documents attached:	

6.0 Status of Mitigation Actions

Mitigation Actions:	Nil
Results:	Nil
Additional assistance required?	N/A

7.0 Apparent Origin of Incident or Attack

Source IP and port:	Secure fax	Protocol:	HTTP
URL:			

Note: Electronic data exchange details are available from the CCIRC.

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, May 16, 2012 15:59
To: IT Security
Cc: CTEC
Subject: [CE2012-615]: University of New Brunswick Compromised - Information Posted to Public Forum

Classification: UNCLASSIFIED

Hello,

Earlier this week, it was revealed that a hacking group had broken into a computer system at the University of New Brunswick. This group then posted some of the stolen data onto a public website known as Pastebin.com. Details of this story can be found at the CBC link here:

http://www.cbc.ca/news/canada/new-brunswick/story/2012/05/15/nb-unb-hacked.html

Your agency is being contacted because someone working there has had their contact information as an employer and/or their user names and passwords posted on Pastebin and may be at risk.

Anyone who's login credentials were exposed should take the following precautions:

16(2)(c),21(1)(a),21(1)(b)

Those whose contact information was exposed may be targeted by cyber criminals pretending to be from UNB or related agencies.

Contact Information Exposed:

<none>

Login Credentials Exposed:

19(1)

Should you require further information please contact us.

<---------------->

15(1)
GC-CTEC Cyber Duty Officer
Cyber Threat Evaluation Centre
Tel# 15(1)

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal

response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems. 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

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Friday, June 1, 2012 18:10
To: 'CTEC'
Cc: IT Security
Subject: IMP Cyber Incident Report IC IT_Sec 06-12

Attachments: IC_IT_Sec06-12_IMP Cyber Incident Report.doc; [CE2012-698]: Login Credentials Exposed on Public Website

Report issued on behalf of Industry Canada's IT Security Division. Report based on CSEC's CE2012-698: Login Credentials Exposed on Public Website.

IC_IT_Sec06-12_IM
P Cyber Incid...

[CE2012-698]:
Login Credential...

Questions can be directed to the undersigned

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

Industry Canada IT Security 05-12 IMP Cyber Incident Report

1.0 Reporting Entity

Department or Agency:	Industry Canada

2.0 Contact Information

First name:	Thomas	Initials:	M
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 954-2796	Cell:	(613) 784-9671
Pager:	(613) 868-4784	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address: 235 Queen, Ottawa, On			

3.0 Incident Type (Delete any categories that do not apply)

Malicious code	N/A
Known vulnerability exploit	*CE2012-698 Login Credentials Exposed on Public Website.*
System compromise	Possible
Data compromise	Possible
Denial of service	N/A
Access violation	Possible
Accident or error	Unk
Other or unknown	N/A

4.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	HTTP
Application	Unknown

5.0 Incident Description and Impact

Date and time of incident:	Advised on 1527hrs 1st June 2012
Location of site affected by incident:	
N/A	
Estimated impact:	Possible data leak
Incident duration:	N/A
Estimated number of systems affected:	1 Client/User

Percentage of departmental systems affected:	N/A
Identify what departmental or public services were affected	N/A
Brief description of the incident:	
Industry Canada was advised of possible exposed login credentials. Clients information was possibly posted on the Pastebin website. IC Service Desk has been advised to immediately reset clients account	
Actions taken:	
A review of the possible email and varieties thereof was conducted and found to be valid. IC Service desk has been directed to immediately reset clients accounts. Client will have to contact the service desk in order to log in again.	
Supporting documents attached:	

6.0 Status of Mitigation Actions

Mitigation Actions:	Will follow up with client on 4th June
Results:	Nil
Additional assistance required?	N/A

7.0 Apparent Origin of Incident or Attack

Source IP and port:	Secure fax	Protocol:	HTTP
URL:			

Note: Electronic data exchange details are available from the CCIRC.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Friday, September 28, 2012 9:01
To: Fournier, Denis: CIO-BI
Subject: ITSINC-2012-060 - FW: CE2012-1150

Hi Denis,
I have put this as incident number 060 for us. Correspondence, reports etc can go into:

16(2)(c)

I have added it to the spreadsheet.

Can you let me know the first report date?

Thanks,
Jen

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Friday, September 28, 2012 7:34 AM
To: IT Security
Cc: 15(1)
Subject: CE2012-1150

Classification: UNCLASSIFIED

Good Morning,

I have a secure fax to send over when someone is available. Thanks.

15(1)
Cyber Threat Evaluation Centre
15(1)
ctec@cse-cst.gc.ca

http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/itimp-pgimti/itimp-pgimti06-eng.asp#Toc324324211

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Wednesday, August 29, 2012 11:54
To: 'CTEC'
Cc: IT Security
Subject: Possible Phishing Attempt_IC_IT_Sec26-12_IMP Cyber Incident

Attachments: IC_IT_Sec26-12_IMP Cyber Incident Report.doc

Good Morning Folks

Please see attached IC IT Security IMP report.

IC_IT_Sec26-12_IM
P Cyber Incid...

Kind Regards

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-049** Industry Canada IT Security 26-12 IMP Cyber Incident Report

1.0 Reporting Entity

Name of organization:	Industry Canada (SBTMS-SMTPE)

2.0 Contact Information

First name:	Thomas	Initials:	M.
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 952-2796	Cell:	(613) 784-9571
Pager:	N/A	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address:	235 Queen, Ottawa, On		

3.0 Incident Description and Impact

Date and time of incident:	29 Aug 2012 @ 0956hrs
Location of site affected by incident:	
Ottawa	
Estimated impact:	N/A
Incident duration:	N/A
Estimated number of clients affected:	74
Percentage of departmental systems affected:	N/A

CTEC GC IT IMP Report Number:

Industry Canada IT Security Incident Number: ITSINC-2012-049

Industry Canada IT Security 26-12 IMP Cyber Incident Report

Brief description of the incident:

16(2)(c)

Actions taken:

16(2)(c)

From: 19(1) CAS-SCA
Sent: Wednesday, August 29, 2012 9:56 AM
To: IT Security
Subject: FW: 16(2)(c)

Good morning,

I am forwarding an email that I received this morning (below). At first I thought it came from your shop because I get notices frequently that my mailbox is full but when I went into the link it looked very suspicious. Don't know how many other have received this email hoax.

19(1)
Comptrollership and Administration Sector
235 Queen Street, Ottawa, ON K1A 0H5
Tel: 19(1)
Fax:
Government of Canada
19(1)@ic.gc.ca

-----Original Message-----
16(2)(c)

CTEC GC IT IMP Report Number:

Industry Canada IT Security Incident Number: ITSINC-2012-049

Industry Canada IT Security 26-12 IMP Cyber Incident Report

16(2)(c)

CTEC GC IT IMP Report Number:

Industry Canada IT Security Incident Number: ITSINC-2012-049

Industry Canada IT Security 26-12 IMP Cyber Incident Report

4.0 Status of Mitigation Actions

Mitigation details to date:	16(2)(c)
Results of mitigation:	
Additional assistance required?	NO

5.0 Incident Type

Malicious code	N/A
Known vulnerability exploit	N/A
System compromise	TBD
Data compromise	N/A
Denial of service	N/A
Access violation	TBD
Accident or error	N/A
Other or unknown	Possible Phishing Attempt

6.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system	Windows XP

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-049** Industry Canada IT Security 26-12 IMP Cyber Incident Report			
(specify version)			
Protocols or services	SMTP		
Application	Unknown		
Note: Electronic data exchange details are available from the CTEC.			

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, June 1, 2012 15:27
To: IT Security
Cc: CTEC
Subject: [CE2012-698]: Login Credentials Exposed on Public Website

Classification: UNCLASSIFIED

Hello,

Earlier this week, it was revealed that a hacking group had broken into a "Canada Email" website and posted some of the stolen data onto a public website known as Pastebin.com.

Your agency is being contacted because someone working there has had their user name and password from this website posted on Pastebin and may be at risk.

Anyone who's login credentials were exposed should take the following precautions:

16(2)(c),21(1)(a)

Login Credentials Exposed:

19(1)

Should you require further information please contact us.

15(1)
<------------>
15(1)
GC-CTEC - Cyber Duty Officer
15(1)
--
The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems. 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

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Thursday, August 30, 2012 8:40
To: 'CTEC'
Cc: IT Security
Subject: Possible Phishing Attempt_IC_IT_Sec27-12IMP Cyber Incident

Attachments: IC_IT_Sec27-12_IMP Cyber Incident Report.doc

Good Morning Folks

Please see attached IC IT Security IMP report.

IC_IT_Sec27-12_IM
P Cyber Incid...

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-050** Industry Canada IT Security 27-12 IMP Cyber Incident Report

1.0 Reporting Entity

Name of organization:	Industry Canada (SBTMS-SMTPE)

2.0 Contact Information

First name:	Thomas	Initials:	M.
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 952-2796	Cell:	(613) 784-9571
Pager:	N/A	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address:	235 Queen, Ottawa, On		

3.0 Incident Description and Impact

Date and time of incident:	29 Aug 2012 @ 1233hrs
Location of site affected by incident:	
Ottawa	
Estimated impact:	N/A
Incident duration:	N/A
Estimated number of clients affected:	??
Percentage of departmental systems affected:	N/A

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-050** Industry Canada IT Security 27-12 IMP Cyber Incident Report
Brief description of the incident:
16(2)(c)
Actions taken:
16(2)(c)
4.0 Status of Mitigation Actions

Mitigation details to date:	16(2)(c)

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-050** Industry Canada IT Security 27-12 IMP Cyber Incident Report	
	16(2)(c)
Results of mitigation:	
Additional assistance required?	NO
5.0 Incident Type	
Malicious code	N/A
Known vulnerability exploit	N/A
System compromise	TBD
Data compromise	N/A
Denial of service	N/A
Access violation	TBD
Accident or error	N/A
Other or unknown	Possible Phishing Attempt
6.0 Systems Affected	
Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	SMTP

CTEC GC IT IMP Report Number: **Industry Canada IT Security Incident Number: ITSINC-2012-050** Industry Canada IT Security 27-12 IMP Cyber Incident Report			
Application	Unknown		
Note: Electronic data exchange details are available from the CTEC.			

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Friday, April 20, 2012 14:17
To: Fournier, Denis: CIO-BI
Cc: IT Security; CTEC
Subject: RE: [CE2012-514]: Canada Post "Phishing" Email Leads to System Compromises

Classification: UNCLASSIFIED

Hi Denis,

I will check for more information and get back to you.

Regards,

15(1)

<---------------->
15(1)
GC-CTEC Cyber Analyst
Cyber Threat Evaluation Centre
Tel# 15(1)

-----Original Message-----
From: Denis.Fournier@ic.gc.ca [mailto:Denis.Fournier@ic.gc.ca]
Sent: April 19, 2012 11:00 AM
To: CTEC
Cc: 16(2)(c)
Subject: RE: [CE2012-514]: Canada Post "Phishing" Email Leads to System Compromises

Good morning,

The searches where done for that URL in our logs during that time frame. We have no users that went to that site. I made 2 different searches and nothing came up. 16(2)(c)
16(2)(c)

If you have information on a user or an IP address please send it to us so we can investigate.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI Chief Informatics Office | Bureau de l'informatique Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca Telephone | Téléphone 613-946-4343 Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389 Government of Canada | Gouvernement du Canada

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, April 17, 2012 4:13 PM

To: CTEC
Subject: [CE2012-514]: Canada Post "Phishing" Email Leads to System Compromises

Classification: UNCLASSIFIED

A recent Pastebin posting describes a Canada Post "Phishing" email for a 16(2)(c) 16(2)(c). Those receiving this fake notice are prompted to visit a link in order to reschedule; but the link actually leads to an executable pif file that tries to install malware onto the visiting system. 16(2)(c) 16(2)(c)) The Pastebin posting can be found here: http://pastebin.com/pnBjzPMN

At least one system within your organization was observed visiting this link between 3 April and 6 April, 2012 and therefore your threat exposure is rated by GC-CTEC as very high . GCCTEC highly recommends that you 16(2)(c),21(1)(a)

16(2)(c),21(1)(a)

Incidents affecting GC infrasturectures should be reported to GC-CTEC at ctec@cse-cst.gc.ca. Any government department suspecting cyber incidents should provide a written report to GC-CTEC (see below).

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

This email is for the purpose of protecting Government of Canada computer networks. It may be disseminated within your department for the protection of your networks. No further dissemination is permitted without approval from GC-CTEC.

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Tuesday, June 12, 2012 12:58
To: Fournier, Denis: CIO-BI
Subject: RE: [CE2012-766]: Login Credentials Exposed in Online Posting

Thank you.

From: Fournier, Denis: CIO-BI
Sent: Tuesday, June 12, 2012 12:49 PM
To: Cullen, Jennifer: CIO-BI
Subject: Re: [CE2012-766]: Login Credentials Exposed in Online Posting

Hi Jen, I'm on this one. I don't know why it went to NSG. When sending back the IMP report I will remind them to send it to IT Security and not NSG

From: Cullen, Jennifer: CIO-BI
Sent: Tuesday, June 12, 2012 11:36 AM
To: Fournier, Denis: CIO-BI
Subject: FW: [CE2012-766]: Login Credentials Exposed in Online Posting

Denis,
Did you get this as well or only IC's Network Security? If IT Security did get it, can you make sure that I am also included?
Thanks,
Jen

From: Phillips, James: SSC-SPC
Sent: Tuesday, June 12, 2012 9:29 AM
To: IT Security
Cc: Network Security - Securite De Reseau
Subject: FW: [CE2012-766]: Login Credentials Exposed in Online Posting

FYI....

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, June 12, 2012 9:25 AM
To: Network Security - Securite De Reseau
Cc: CTEC
Subject: [CE2012-766]: Login Credentials Exposed in Online Posting

Classification: UNCLASSIFIED

Hello,

Recently, it was revealed that a hacking group had broken into the website www.intelconsumerelectronics.com and posted some stolen client data onto another public website

known as Pastebin.com.

Your agency is being contacted because someone working there has had their email address posted on Pastebin. The following data was exposed:

19(1)

GC-CTEC recommends that the affected employee be notified and that the employee should exercise heightened caution when opening unrecognized or suspicious emails.

Should you require further information please contact us.

CTEC

15(1)
GC-CTEC Cyber Duty Officer

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Tuesday, November 20, 2012 9:07
To: Fournier, Denis: CIO-BI; IT Security
Cc: CTEC
Subject: RE: [CE2012-1429]: Login Credentials Exposed in Online Posting

Classification: UNCLASSIFIED

Hi Denis,

Perfect - Thanks for the prompt action and reply.

Cheers,

15(1)
<---------------->
15(1)
GC-CTEC Cyber Duty Officer
Cyber Threat Evaluation Centre
CTEC@CSE-CST.GC.CA
15(1)

-----Original Message-----
From: Denis.Fournier@ic.gc.ca [mailto:Denis.Fournier@ic.gc.ca]
Sent: November 20, 2012 9:02 AM
To: CTEC; 16(2)(c)
Subject: RE: [CE2012-1429]: Login Credentials Exposed in Online Posting

Good day,

I communicated with the user. She has informed me that this is an old password and all her other ones are not the same.

She explained that this password was not for work related purposes.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI Chief Informatics Office | Bureau de l'informatique Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca Telephone | Téléphone 613-946-4343 Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389 Government of Canada | Gouvernement du Canada

-----Original Message-----
From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Tuesday, November 20, 2012 8:15 AM
To: IT Security
Cc: CTEC
Subject: [CE2012-1429]: Login Credentials Exposed in Online Posting

Classification: UNCLASSIFIED

Hello,

A hacking group has broken into an unknown website and posted information stolen from it to Pastebin.com.

Your agency is being contacted because someone working there has had their user name and password posted online and may be at risk. The following information was exposed:

Email : password

19(1)

GC-CTEC recommends the following precautions be taken:

16(2)(c),21(1)(a)

Should you require further information please contact us.

Thank you,

15(1)
<---------->
15(1)
GC-CTEC Cyber Duty Officer
Cyber Threat Evaluation Centre
CTEC@CSE-CST.GC.CA
(613) 15(1)
--

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems. To report incidents affecting GC infrastructures, please complete this form: http://publiservice.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimt-eng.rtf and contact GC-CTEC at ctec@cse-cst.gc.ca or (613)991-2300.

Lacroix, Lise: SBTMS-SMTPE

From: IT Service Desk - Centre de services TI
Sent: Monday, November 19, 2012 11:18
To: Fournier, Denis: CIO-BI
Cc: IT Security
Subject: RE: "URGENT" infected computer 16(2)(c)

Please see ticket 01295660

Joao-Ricardo Botelho
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Telephone | Téléphone 613-954-7916
Facsimile | Télécopieur 613-954-7994
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Fournier, Denis: CIO-BI
Sent: Monday, November 19, 2012 11:13 AM
To: IT Service Desk - Centre de services TI
Cc: IT Security
Subject: "URGENT" infected computer 16(2)(c)

Service Desk,

Please create a ticket under the client name (Item 2) and assign a technician for immediate re-image of computer

The following action needs to be taken **ASAP** without any **delays**.

16(2)(c)

Client Name: 19(1)

Client Host: 19(1)

Client Dept: MC

Client Local 232 Yorktech Drive, Markham, Ontario

I was able to reach the user and he is waiting for the TSO

3. Security logs indicate clients workstation is trying to communicate with a known Malware site multiple times that is part of the Cyber Flash: IT Sec Flash SF009-12 Update #3: Canada Post & Airline Company Email Phishing Campaign. The mitigation for this infection is 16(2)(c)

4. In the event the client is unreachable this email will also be released to the client

5. Your immediate cooperation and response is appreciated.

16(2)(c)

Question can be directed to IT Security

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Fewer, Art: CIO-BI
Sent: Thursday, March 8, 2012 12:13
To: Fournier, Denis: CIO-BI
Cc: Cullen, Jennifer: CIO-BI; IT Security
Subject: Re: Call from CSIS

Agreed,

Art Fewer CD, CISSP
Team Leader, IT Security | Chef d'equipe, Securité. TI
Chief Informatics Office / Bureau de l'informatique
Small Business and Marketplace Services / Services axes sur le marche et les petites entreprises
Industry Canada / industrie Canada
235 Queen Street / rue 235 Queen
Ottawa, On
Canada K1A 0H5
Telephone / Telephone 613 960-5260 Facsimile / Telecopieure 613 946-3367
Art.Fewer@ic.gc.ca
Government of Canada / Gouvernenment du Canada

From: Fournier, Denis: CIO-BI
Sent: Thursday, March 08, 2012 12:12 PM
To: Fewer, Art: CIO-BI
Cc: Cullen, Jennifer: CIO-BI; IT Security
Subject: RE: Call from CSIS

Yes it has been taken care of. I have talked with Nigel and he is waiting for further instruction from us.

We need to determine if this call is valid.

From: Fewer, Art: CIO-BI
Sent: Thursday, March 8, 2012 12:10 PM
To: Fournier, Denis: CIO-BI
Cc: Cullen, Jennifer: CIO-BI
Subject: Re: Call from CSIS

16(2)(c),21(1)(a),21(1)(b) TBD based on contact with CSIS.

All yours,

Art

Art Fewer CD, CISSP
Team Leader, IT Security | Chef d'equipe, Securité. TI

Chief Informatics Office / Bureau de l'informatique
Small Business and Marketplace Services / Services axes sur le marche et les petites entreprises
Industry Canada / industrie Canada
235 Queen Street / rue 235 Queen
Ottawa, On
Canada K1A 0H5
Telephone / Telephone 613 960-5260 Facsimile / Telecopieure 613 946-3367
Art.Fewer@ic.gc.ca
Government of Canada / Gouvernenment du Canada

From: Fournier, Denis: CIO-BI
Sent: Thursday, March 08, 2012 12:07 PM
To: Fewer, Art: CIO-BI
Cc: Cullen, Jennifer: CIO-BI
Subject: RE: Call from CSIS

Hi,

Contacted Nigel and he will 16(2)(c)

I called the CSIS number and got the voice mail. I will take care of it.

Thanks

Denis

From: Fewer, Art: CIO-BI
Sent: Thursday, March 8, 2012 12:00 PM
To: Fournier, Denis: CIO-BI
Cc: Cullen, Jennifer: CIO-BI
Subject: Fw: Call from CSIS

Denis,

16(2)(c)

I will follow up with CSIS.

Art

Art Fewer CD, CISSP
Team Leader, IT Security | Chef d'equipe, Securité. TI
Chief Informatics Office / Bureau de l'informatique
Small Business and Marketplace Services / Services axes sur le marche et les petites entreprises
Industry Canada / industrie Canada
235 Queen Street / rue 235 Queen
Ottawa, On
Canada K1A 0H5

Telephone / Telephone 613 960-5260 Facsimile / Telecopieure 613 946-3367
Art.Fewer@ic.gc.ca
Government of Canada / Gouvernenment du Canada

From: Fewer, Art: CIO-BI
Sent: Thursday, March 08, 2012 11:51 AM
To: Cullen, Jennifer: CIO-BI
Subject: Re: Call from CSIS

I have a contact at CSIS. I will follow up.

Thanks,

Art

Art Fewer CD, CISSP
Team Leader, IT Security | Chef d'equipe, Securité. TI
Chief Informatics Office / Bureau de l'informatique
Small Business and Marketplace Services / Services axes sur le marche et les petites entreprises
Industry Canada / industrie Canada
235 Queen Street / rue 235 Queen
Ottawa, On
Canada K1A 0H5
Telephone / Telephone 613 960-5260 Facsimile / Telecopieure 613 946-3367
Art.Fewer@ic.gc.ca
Government of Canada / Gouvernenment du Canada

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, March 08, 2012 11:50 AM
To: Fewer, Art: CIO-BI
Subject: Fw: Call from CSIS

Hi Art,

Assuming you are acting for Rob this week, can you lead this (as I am not in the office)?

Please let me know the expected course of action?

Thanks,
Jen

From: Green, Nigel: CIO-BI (ONT)
Sent: Thursday, March 08, 2012 10:58 AM
To: Cullen, Jennifer: CIO-BI
Cc: Johnson, Denis: CIO-BI (NCR-RCN)
Subject: Call from CSIS

Hi Jennifer,

I received a call from CSIS regarding a cyber intrusion on 16(2)(c) located out of our Windsor site. I left a message with the CSIS contact 15(1) 15(1) to contact you…….don't have any other information.

Nigel Green
Team Leader, Regional Operations (Ontario) | Chef d'équipe, opérations régionales (Ontario)
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
151 Yonge Street, Toronto ON M5C 2W7 | 151, rue Yonge, Toronto ON M5C 2W7
Nigel.Green@ic.gc.ca
Telephone | Téléphone 416-952-8249
Facsimile | Télécopieur 416-973-6272
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Fewer, Art: CIO-BI
Sent: Thursday, March 8, 2012 12:08
To: Fournier, Denis: CIO-BI
Cc: Cullen, Jennifer: CIO-BI
Subject: Re: Call from CSIS

Thanks Denis

Art Fewer CD, CISSP
Team Leader, IT Security | Chef d'equipe, Securité. TI
Chief Informatics Office / Bureau de l'informatique
Small Business and Marketplace Services / Services axes sur le marche et les petites entreprises
Industry Canada / industrie Canada
235 Queen Street / rue 235 Queen
Ottawa, On
Canada K1A 0H5
Telephone / Telephone 613 960-5260 Facsimile / Telecopieure 613 946-3367
Art.Fewer@ic.gc.ca
Government of Canada / Gouvernenment du Canada

From: Fournier, Denis: CIO-BI
Sent: Thursday, March 08, 2012 12:07 PM
To: Fewer, Art: CIO-BI
Cc: Cullen, Jennifer: CIO-BI
Subject: RE: Call from CSIS

Hi,

Contacted Nigel and he will 16(2)(c)

I called the CSIS number and got the voice mail. I will take care of it.

Thanks

Denis

From: Fewer, Art: CIO-BI
Sent: Thursday, March 8, 2012 12:00 PM
To: Fournier, Denis: CIO-BI
Cc: Cullen, Jennifer: CIO-BI
Subject: Fw: Call from CSIS

Denis,

16(2)(c)

I will follow up with CSIS.

Art

Art Fewer CD, CISSP
Team Leader, IT Security | Chef d'equipe, Securité. TI
Chief Informatics Office / Bureau de l'informatique
Small Business and Marketplace Services / Services axes sur le marche et les petites entreprises
Industry Canada / industrie Canada
235 Queen Street / rue 235 Queen
Ottawa, On
Canada K1A 0H5
Telephone / Telephone 613 960-5260 Facsimile / Telecopieure 613 946-3367
Art.Fewer@ic.gc.ca
Government of Canada / Gouvernenment du Canada

From: Fewer, Art: CIO-BI
Sent: Thursday, March 08, 2012 11:51 AM
To: Cullen, Jennifer: CIO-BI
Subject: Re: Call from CSIS

I have a contact at CSIS. I will follow up.

Thanks,

Art

Art Fewer CD, CISSP
Team Leader, IT Security | Chef d'equipe, Securité. TI
Chief Informatics Office / Bureau de l'informatique
Small Business and Marketplace Services / Services axes sur le marche et les petites entreprises
Industry Canada / industrie Canada
235 Queen Street / rue 235 Queen
Ottawa, On
Canada K1A 0H5
Telephone / Telephone 613 960-5260 Facsimile / Telecopieure 613 946-3367
Art.Fewer@ic.gc.ca
Government of Canada / Gouvernenment du Canada

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, March 08, 2012 11:50 AM
To: Fewer, Art: CIO-BI
Subject: Fw: Call from CSIS

Hi Art,

Assuming you are acting for Rob this week, can you lead this (as I am not in the office)?

Please let me know the expected course of action?

Thanks,
Jen

From: Green, Nigel: CIO-BI (ONT)
Sent: Thursday, March 08, 2012 10:58 AM
To: Cullen, Jennifer: CIO-BI
Cc: Johnson, Denis: CIO-BI (NCR-RCN)
Subject: Call from CSIS

Hi Jennifer,

I received a call from CSIS regarding a cyber intrusion on 16(2)(c) located out of our Windsor site. I left a message with the CSIS contact 15(1) 15(1) to contact you…….don't have any other information.

Nigel Green
Team Leader, Regional Operations (Ontario) | Chef d'équipe, opérations régionales (Ontario)
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
151 Yonge Street, Toronto ON M5C 2W7 | 151, rue Yonge, Toronto ON M5C 2W7
Nigel.Green@ic.gc.ca
Telephone | Téléphone 416-952-8249
Facsimile | Télécopieur 416-973-6272
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Thursday, March 8, 2012 12:15
To: Green, Nigel: CIO-BI (ONT); Robinson-Kenner, Dennis: CIO-BI (ONT)
Cc: Johnson, Denis: CIO-BI (NCR-RCN); IT Security
Subject: RE: Call from CSIS

Hi Nigel,

As soon as we get more info we will keep you informed. 16(2)(c) until we reach CSIS.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Green, Nigel: CIO-BI (ONT)
Sent: Thursday, March 8, 2012 12:12 PM
To: Robinson-Kenner, Dennis: CIO-BI (ONT)
Cc: Fournier, Denis: CIO-BI; Johnson, Denis: CIO-BI (NCR-RCN)
Subject: Call from CSIS

Hi Denis,

Due to a potential security issue linked to 16(2)(c)
16(2)(c) Please arrange locally and visit if required.

N.g

From: Green, Nigel: CIO-BI (ONT)
Sent: Thursday, March 8, 2012 10:59 AM
To: Cullen, Jennifer: CIO-BI
Cc: Johnson, Denis: CIO-BI (NCR-RCN)
Subject: Call from CSIS

Hi Jennifer,

I received a call from CSIS regarding a cyber intrusion on 16(2)(c) located out of our Windsor site. I left a message with the CSIS contact 15(1) to contact you…….don't have any other information.

Nigel Green
Team Leader, Regional Operations (Ontario) | Chef d'équipe, opérations régionales (Ontario)
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
151 Yonge Street, Toronto ON M5C 2W7 | 151, rue Yonge, Toronto ON M5C 2W7
Nigel.Green@ic.gc.ca
Telephone | Téléphone 416-952-8249
Facsimile | Télécopieur 416-973-6272
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, March 22, 2012 16:25
To: Thompson, Kim: CAS-SCA
Cc: Gosselin, Andrée: CIO-BI; Fournier, Denis: CIO-BI
Subject: FW: Inquiry-Ontario Region

Hi Kim,

As requested, here are the details regarding the system in Windsor office.

Background:

On March 8, IT Security was contacted by Nigel Green from our Ontario Regional Office stating that he

16(2)(c),21(1)(a),21(1)(b)

Misstep in the Government of Canada Information Technology Incident Management Plan (GC IT IMP):

16(2)(c),21(1)(a),21(1)(b)

Actions Taken:

Denis (Fournier) contacted Nigel to request that 16(2)(c) 16(2)(c)

16(2)(c)

As of end of day March 21, IT Security still had not been contacted by CTEC. Denis emailed CTEC this morning requesting an update. The contact at CTEC is unaware of this incident and is looking into it within his office.

Current Status:

16(2)(c),21(1)(a),21(1)(b)

IT Security is awaiting further instructions from CTEC as to whether CTEC wants 16(2)(c)

With the information given to IT Security to date, this incident is considered to pose low risk to Industry Canada.

If you have any further questions or concerns, please contact me.
Thank you,
Jennifer

From: Cullen, Jennifer: CIO-BI
Sent: Wednesday, March 21, 2012 4:24 PM
To: Thompson, Kim: CAS-SCA
Cc: Fournier, Denis: CIO-BI
Subject: RE: Inquiry-Ontario Region

Hi Kim,
Yes, I will work with Denis to iron out the details and provide a report to you tomorrow.
Thank you,
Jennifer

From: Thompson, Kim: CAS-SCA
Sent: Wednesday, March 21, 2012 4:16 PM
To: Cullen, Jennifer: CIO-BI
Cc: Fournier, Denis: CIO-BI
Subject: FW: Inquiry-Ontario Region

Hi Jennifer, can you please provide me with the details as to what has occurred with 16(2)(c) since it left the Windsor office and who is involved in this investigation?

16(2)(c),21(1)(a),21(1)(b)

Thank you,

Kim Thompson
Director, Security and Emergency Management | Directrice de la gestion de la sécurité et des urgences,
Departmental Security Officer | Agent de sécurité ministérielle
Corporate Facilities and Security Branch, CAS | Direction générale de la gestion des installations et de la sécurité, SCA
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Kim.Thompson@ic.gc.ca
Telephone | Téléphone 613-960-6169
Facsimile | Télécopieur 613-957-6543
Teletypewriter | Téléimprimeur 1-866-694-8389

From: Fournier, Denis: CIO-BI
Sent: March 9, 2012 2:28 PM
To: Fewer, Art: CIO-BI; Thompson, Kim: CAS-SCA
Cc: Green, Nigel: CIO-BI (ONT); Robinson-Kenner, Dennis: CIO-BI (ONT); Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA; Gosselin, Andrée: CIO-BI; IT Security
Subject: RE: Inquiry-Ontario Region

Yes it was.

Denis

From: Fewer, Art: CIO-BI
Sent: Friday, March 9, 2012 2:25 PM
To: Fournier, Denis: CIO-BI; Thompson, Kim: CAS-SCA
Cc: Green, Nigel: CIO-BI (ONT); Robinson-Kenner, Dennis: CIO-BI (ONT); Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA; Gosselin, Andrée: CIO-BI; IT Security
Subject: RE: Inquiry-Ontario Region

OK,

Just to verify , the 'misunderstanding" is between CTEC and CSIS reference their process?

Art

From: Fournier, Denis: CIO-BI
Sent: Friday, March 9, 2012 2:22 PM
To: Fewer, Art: CIO-BI; Thompson, Kim: CAS-SCA
Cc: Green, Nigel: CIO-BI (ONT); Robinson-Kenner, Dennis: CIO-BI (ONT); Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA; Gosselin, Andrée: CIO-BI; IT Security
Subject: RE: Inquiry-Ontario Region

Hi Art,

16(2)(c),21(1)(a),21(1)(b)

Thanks

Denis

From: Fewer, Art: CIO-BI
Sent: Friday, March 9, 2012 9:43 AM
To: Thompson, Kim: CAS-SCA

Cc: Green, Nigel: CIO-BI (ONT); Robinson-Kenner, Dennis: CIO-BI (ONT); Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA; Gosselin, Andrée: CIO-BI; IT Security; Fournier, Denis: CIO-BI
Subject: RE: Inquiry-Ontario Region

Hi Kim,

That is correct IT Security will take lead with respect to response/providing information to the Agency that reported this incident to IC.

Next Steps:

- Denis (our Incident Response Lead) will coordinate with the reporting agency and provide any technical support/information they require. this will include access to 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

If you have any additional concerns or questions do not hesitate to contact me.

Sincerely,

Art

Art Fewer CD, CISSP
Team Leader, IT Security | Chef d'equipe, Securité. TI
Chief Informatics Office / Bureau de l'informatique
Small Business and Marketplace Services / Services axes sur le marche et les petites entreprises
Industry Canada / industrie Canada
235 Queen Street / rue 235 Queen
Ottawa, On
Canada K1A 0H5
Telephone / Telephone 613 960-5260 Facsimile / Telecopieure 613 946-3367
Art.Fewer@ic.gc.ca
Government of Canada / Gouvernenment du Canada

From: Thompson, Kim: CAS-SCA
Sent: Friday, March 9, 2012 8:48 AM
To: Fewer, Art: CIO-BI
Cc: Green, Nigel: CIO-BI (ONT); Robinson-Kenner, Dennis: CIO-BI (ONT); Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Subject: Inquiry-Ontario Region

Art, last night I briefed Kelly Gillis and Sylvain Laporte on this matter. Sandy advised this morning that the 21(1)(a),21(1)(b) have now advised both Kelly and Sylvain.

So in terms of next steps, your team (CIO) will 16(2)(c),21(1)(a),21(1)(b)

16(2)(c),21(1)(a),21(1)(b)

Please advise!

Kim Thompson
Director, Security and Emergency Management | Directrice de la gestion de la sécurité et des urgences,
Departmental Security Officer | Agent de sécurité ministérielle
Corporate Facilities and Security Branch, CAS | Direction générale de la gestion des installations et de la sécurité, SCA
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Kim.Thompson@ic.gc.ca
Telephone | Téléphone 613-960-6169
Facsimile | Télécopieur 613-957-6543
Teletypewriter | Téléimprimeur 1-866-694-8389

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Friday, March 30, 2012 16:40
To: Hagarty, Richard: CIO-BI; Cullen, Jennifer: CIO-BI
Subject: Re: CE2012-339

Hi,

I have worked on the IMP report today for CTEC. It should be ok to go on Monday. Then we will be able to complete our incident report in our template.

Thanks

Denis

From: Hagarty, Richard: CIO-BI
Sent: Friday, March 30, 2012 04:24 PM
To: Cullen, Jennifer: CIO-BI
Cc: Fournier, Denis: CIO-BI
Subject: RE: CE2012-339

Ok - Thanks and please take the time to present the final draft of your template at a team meeting so we can all provide some feedback.

Have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, March 29, 2012 3:45 PM
To: Hagarty, Richard: CIO-BI
Cc: Fournier, Denis: CIO-BI
Subject: RE: CE2012-339

Hi Richard,

I have discussed with Denis. The faxes we received yesterday and today are related to the cyber event which began March 8th.

Attached is the summary up to March 22nd. Denis will create a report to include the attached info and update with the activities from March 22nd to present.

Denis and I will work together next week to discuss creating incident report templates that we can use depending on the scenario.

Thanks,
Jen

From: Hagarty, Richard: CIO-BI
Sent: Wednesday, March 28, 2012 4:03 PM
To: Cullen, Jennifer: CIO-BI
Cc: Fournier, Denis: CIO-BI
Subject: FW: CE2012-339

Hi Jen,

Can you follow-up with Denis and CTEC to better understand the nature of the fax we received late today. Basically, is this a new event or is this related to one that was already opened?

Thanks!

From: Fewer, Art: CIO-BI
Sent: Wednesday, March 28, 2012 3:11 PM
To: Hagarty, Richard: CIO-BI
Subject: Fw: CE2012-339

FYI

Art Fewer CD, CISSP
Team Leader, IT Security | Chef d'equipe, Securité. TI
Chief Informatics Office / Bureau de l'informatique
Small Business and Marketplace Services / Services axes sur le marche et les petites entreprises
Industry Canada / industrie Canada
235 Queen Street / rue 235 Queen
Ottawa, On
Canada K1A 0H5
Telephone / Telephone 613 960-5260 Facsimile / Telecopieure 613 946-3367
Art.Fewer@ic.gc.ca
Government of Canada / Gouvernenment du Canada

From: 15(1) @CSE-CST.GC.CA]
Sent: Wednesday, March 28, 2012 02:55 PM
To: Fewer, Art: CIO-BI; Pilipchuk, Robert: CIO-BI; Fournier, Denis: CIO-BI
Cc: 15(1) @CSE-CST.GC.CA>
Subject: CE2012-339

Classification: UNCLASSIFIED

I would like to send IC a secure fax. Can someone pls advise when you are ready to receive it?

15(1)

Cyber Threat Evaluation Centre
Communications Security Establishment Canada
Centre d'évaluation des cybermenaces
Centre de la sécurité des télécommunications Canada

15(1) 613.949.5377

SECURE FAX: 15(1) before sending a secure fax]
15(1) @cse-cst.gc.ca

Contactez/reach CTEC? ctec@cse-cst.gc.ca

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Friday, February 8, 2013 8:52
To: Fournier, Denis: CIO-BI
Subject: RE: CE2013-1703

Thank you,
Jen

From: Fournier, Denis: CIO-BI
Sent: Thursday, February 7, 2013 7:21 PM
To: Cullen, Jennifer: CIO-BI
Subject: RE: CE2013-1703

Just so you know everything was done for this one. 16(2)(c)

There was just 1 recipient and the account does not exist

Talk to you on Monday

Denis

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, February 07, 2013 3:49 PM
To: Fournier, Denis: CIO-BI
Cc: IT Security
Subject: RE: CE2013-1703

Hi Denis,
Thanks for the follow-up. I have received the fax.
Jen

From: Fournier, Denis: CIO-BI
Sent: Thursday, February 7, 2013 3:44 PM
To: Cullen, Jennifer: CIO-BI
Subject: Fw: CE2013-1703

Jen, you can go see Stephane Lacelle to get the secure fax at CAS

From: CTEC [mailto:CTEC@CSE-CST.GC.CA]
Sent: Thursday, February 07, 2013 03:19 PM Eastern Standard Time
To: IT Security
Cc: CTEC <CTEC@CSE-CST.GC.CA>
Subject: CE2013-1703

Classification: UNCLASSIFIED

Previous e-mail mislabelled. Treat as Unclassified.

We have a secure fax to send. Please advise when someone is available to receive it.

Thank you,

15(1)

15(1)
GC-CTEC Cyber Duty Officer
Cyber Threat Evaluation Centre
CTEC@CSE-CST.GC.CA
15(1)

Lacroix, Lise: SBTMS-SMTPE

From: Cullen, Jennifer: CIO-BI
Sent: Thursday, August 23, 2012 13:19
To: Pearson, Rod: SSC-SPC
Subject: RE: Cyber Event CE2012-994 - Malicious email

Hi Rod,
Thank you for the report below.

We have received a report that there may have been other attempts to send emails with the same subject line. Can you provide a report starting at the end time of the last report to present? If there are results, would you be able to confirm that the email was blocked or delivered?

Thank you,
Jennifer

From: Pearson, Rod: SSC-SPC
Sent: Monday, August 20, 2012 3:22 PM
To: Cullen, Jennifer: CIO-BI
Subject: RE: Cyber Event CE2012-994 - Malicious email

Hi Jennifer,

16(2)(c) Recipient list back to Aug 6 is attached. (1 email to 1 recipient)

<< File: CE2012-994_1.csv >>
Rod Pearson
Shared Services Canada | Industry Canada
Services partagés Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Rod.Pearson@ic.gc.ca
Telephone | Téléphone 613-960-8957
Facsimile | Télécopieur 613-946-4932
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

From: Cullen, Jennifer: CIO-BI
Sent: Monday, August 20, 2012 2:05 PM
To: Pearson, Rod: SSC-SPC
Subject: Cyber Event CE2012-994 - Malicious email

Hi Rod,

NOTE: The information contained in this email is for internal user only and must not be disseminated or employed externally. Any mitigation activities 16(2)(c)
16(2)(c)

CSEC has requested that Industry Canada remove all instances of the following malicious email messages from departmental email severs and workstations.

16(2)(c) advise who may have received this email:

16(2)(c)

If you have any questions or concerns, please contact me.

Thank you,
Jennifer

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Thursday, June 7, 2012 13:34
To: Fournier, Denis: CIO-BI; IT Security
Subject: RE: IC_IT_Sec09-12_IMP Cyber Incident Report

Looks good

As discussed remove the type O next to June

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

From: Fournier, Denis: CIO-BI
Sent: Thursday, June 7, 2012 12:25 PM
To: IT Security
Subject: IC_IT_Sec09-12_IMP Cyber Incident Report

Team

Please review and advise before I send out

Thanks

<< File: IC_IT_Sec09-12_IMP Cyber Incident Report.doc >>

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Sent: Wednesday, July 4, 2012 15:16
To: Fournier, Denis: CIO-BI; IT Security
Subject: Re: IC_IT_Sec15-12_IMP Cyber Incident Report.doc

Denis

Can't see it on the BB did you advise in the réport that an email was sent to X number of users

Tom

From: Fournier, Denis: CIO-BI
Sent: Wednesday, July 04, 2012 03:03 PM
To: IT Security
Subject: IC_IT_Sec15-12_IMP Cyber Incident Report.doc

Please review before sending toi CTEC

<<IC_IT_Sec15-12_IMP Cyber Incident Report.doc>>

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Lacroix, Lise: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, May 16, 2012 17:44
To: Rodden-Aubut, Thomas: CIO-BI (NCR-RCN)
Cc: IT Security; CTEC
Subject: RE: IMP Cyber Incident Report IC IT_Sec 05-12

Classification: UNCLASSIFIED

Thank you Tom for your submission. Glad to see that the emails were invalid.

regards,
15(1)

15(1)
GC-CTEC Cyber Duty Officer

From: Thomas.Rodden-Aubut@ic.gc.ca [mailto:Thomas.Rodden-Aubut@ic.gc.ca]
Sent: May 16, 2012 17:37
To: CTEC
Cc: 16(2)(c)
Subject: IMP Cyber Incident Report IC IT_Sec 05-12

Report issued on behalf of Industry Canada's IT Security based on CSEC's CE2012-615: University of New Brunswick Compromised - Information Posted to Public Forum

<<IC_IT_Sec05-12_IMP Cyber Incident Report.doc>>

<<[CE2012-615]: University of New Brunswick Compromised - Information Posted to Public Forum>>
Questions can be directed to the undersigned.

Tom Rodden-Aubut
IT Security Officer | Officier en Securite TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen St, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Thomas.Rodden-Aubut@ic.gc.ca
Telephone | Téléphone 613-952-2796
Facsimile | Télécopieur 613-946-3367
Government of Canada | Gouvernement du Canada

16(2)(c)

Never trouble trouble till trouble troubles you!!!

Industry Canada Industrie Canada

Canada

Industry Canada IT Security 05-12 IMP Cyber Incident Report

1.0 Reporting Entity

Department or Agency:	Industry Canada

2.0 Contact Information

First name:	Thomas	Initials:	M
Last name:	Rodden-Aubut	Position:	IT Security Officer
Phone:	(613) 954-2796	Cell:	(613) 784-9671
Pager:	(613) 868-4784	Fax:	(613) 946-3367
Email:	Thomas.rodden-aubut@ic.gc.ca		
Office address: 235 Queen, Ottawa, On			

3.0 Incident Type (Delete any categories that do not apply)

Malicious code	N/A
Known vulnerability exploit	*CE2012-615 UNB hacked resulting in privileged information being posted to a known public website.*
System compromise	Unknown
Data compromise	Unknown
Denial of service	N/A
Access violation	Possible
Accident or error	N/A
Other or unknown	N/A

4.0 Systems Affected

Network zone affected	Operational
Type of system affected	PC
Operating system (specify version)	Windows XP
Protocols or services	HTTP
Application	Unknown

5.0 Incident Description and Impact

Date and time of incident:	Advised on 1559hrs 16th May 2012
Location of site affected by incident:	
N/A	
Estimated impact:	Possible data leak
Incident duration:	N/A
Estimated number of systems affected:	1 Client/User

Percentage of departmental systems affected:	N/A
Identify what departmental or public services were affected	N/A
Brief description of the incident:	
Industry Canada was advised of possible stolen electronic data from UNB. The stolen data was possibly posted on a public website. An email resembling one that could be associated to IC was realized and information was forwarded on to IC IT Security.	
Actions taken:	
A review of the possible email and varieties thereof was conducted and found to be invalid. No further action required.	
Supporting documents attached:	

6.0 Status of Mitigation Actions

Mitigation Actions:	Nil
Results:	Nil
Additional assistance required?	N/A

7.0 Apparent Origin of Incident or Attack

Source IP and port:	Secure fax	Protocol:	HTTP
URL:			

Note: Electronic data exchange details are available from the CCIRC.

Lacroix, Lise: SBTMS-SMTPE

From: 15(1) @CSE-CST.GC.CA]
Sent: Thursday, March 22, 2012 11:13
To: Fournier, Denis: CIO-BI
Cc: IT Security; CTEC
Subject: RE: Incident in Windsor

Classification: UNCLASSIFIED

Good Morning Denis,

This is the first I have heard about this, let me do a little digging and see if I can find any information. I will get back to you shortly. Thank you.

15(1)
Cyber Threat Evaluation Centre
15(1)
ctec@cse-cst.gc.ca

To report incidents affecting GC infrastructures contact GC-CTEC at ctec@cse-cst.gc.ca. Any government department suspecting cyber incidents should provide a written report to GC-CTEC (see below).

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

---

From: Denis.Fournier@ic.gc.ca [mailto:Denis.Fournier@ic.gc.ca]
Sent: March 22, 2012 10:30 AM
To: 15(1)
Cc: 16(2)(c)
Subject: Incident in Windsor

15(1)

We had an incident on the 8th of March. A CSIS Toronto investigator contacted a team leader in our Toronto office saying that one of our IP addresses in Windsor was doing peer to peer with multiple addresses in other countries.

16(2)(c),21(1)(a),21(1)(b)

I have not heard anything yet. Is somebody from CSE-C going to 16(2)(c) or can we consider this case closed.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Industry Canada Industrie Canada

Canada

Rusenstrom, Sashsha: SBTMS-SMTPE

From: CTEC [CTEC@CSE-CST.GC.CA]
Sent: Wednesday, May 16, 2012 15:59
To: IT Security
Cc: CTEC
Subject: [CE2012-615]: University of New Brunswick Compromised - Information Posted to Public Forum

Classification: UNCLASSIFIED

Hello,

Earlier this week, it was revealed that a hacking group had broken into a computer system at the University of New Brunswick. This group then posted some of the stolen data onto a public website known as Pastebin.com. Details of this story can be found at the CBC link here:

http://www.cbc.ca/news/canada/new-brunswick/story/2012/05/15/nb-unb-hacked.html

Your agency is being contacted because someone working there has had their contact information as an employer and/or their user names and passwords posted on Pastebin and may be at risk.

Anyone who's login credentials were exposed should take the following precautions:

16(2)(c),21(1)(a),21(1)(b)

Those whose contact information was exposed may be targeted by cyber criminals pretending to be from UNB or related agencies.

Contact Information Exposed:

<none>

Login Credentials Exposed:

19(1)@ic.gc.ca

Should you require further information please contact us.

<---------------->
15(1)
GC-CTEC Cyber Duty Officer
Cyber Threat Evaluation Centre
Tel# 15(1)

The Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. GC-CTEC helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal

response to cyber security incidents of national interest. The GC-CTEC team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems. 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

Lacroix, Lise: SBTMS-SMTPE

From: Fournier, Denis: CIO-BI
Sent: Thursday, March 22, 2012 11:40
To: 15(1)
Cc: IT Security; CTEC
Subject: RE: Incident in Windsor

Hi 15(1)

No problem it is already started.

Denis

From: 15(1) @CSE-CST.GC.CA]
Sent: Thursday, March 22, 2012 11:18 AM
To: Fournier, Denis: CIO-BI
Cc: IT Security; CTEC
Subject: RE: Incident in Windsor

Classification: UNCLASSIFIED

Denis,

In the meantime can you please fill in an incident report so we have some background information on this. Thanks the url is in my signature block.

15(1)
Cyber Threat Evaluation Centre
15(1)
ctec@cse-cst.gc.ca

To report incidents affecting GC infrastructures contact GC-CTEC at ctec@cse-cst.gc.ca. Any government department suspecting cyber incidents should provide a written report to GC-CTEC (see below).

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

---

From: Denis.Fournier@ic.gc.ca [mailto:Denis.Fournier@ic.gc.ca]
Sent: March 22, 2012 10:30 AM
To: 15(1)
Cc: 16(2)(c)
Subject: Incident in Windsor

Hi 15(1)

We had an incident on the 8th of March. A CSIS Toronto investigator contacted a team leader in our Toronto office saying that one of our IP addresses in Windsor was doing peer to peer with multiple addresses in other countries.

16(2)(c),21(1)(a),21(1)(b)

I have not heard anything yet. Is somebody from CSE-C going to 16(2)(c) or can we consider this case closed.

Thanks

Denis Fournier, CISSP CCNA
IT Security Officer | Agent de Securité des TI
Chief Informatics Office | Bureau de l'informatique
Small Business and Marketplace Services | Services axés sur le marché et les petites entreprises
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0C8
Denis.Fournier@ic.gc.ca
Telephone | Téléphone 613-946-4343
Facsimile | Télécopieur 613-946-3367
Blackberry 613-868-4784
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

16(2)(c)

Industry Canada Industrie Canada

Canada

Lacroix, Lise: SBTMS-SMTPE

From: Pilipchuk, Robert: CIO-BI
Sent: Monday, September 24, 2012 8:23
To: Cullen, Jennifer: CIO-BI
Cc: IT Security; Hagarty, Richard: CIO-BI; DPM-AITL: Application Integration Test Lab Team; Keith, Julie: CIO-BI (NCR-RCN); DPM-WE: Workstation Engineering Team; Lin, Stanley: CIO-BI (NCR-RCN); Peters, Bernadette: CIO-BI
Subject: RE: 16(2)(c)

Hi Jennifer,

I spoke with Stanley today and this effort began last Friday and the teams are working with priority to hopefully complete work by the end of this week. It will be an excellent accomplishment if they complete this week as it almost a week faster than the typical Fast-Track processes.

Cheers,

Rob
Robert.Pilipchuk@ic.gc.ca
Telephone | Téléphone **613-946-8184**

From: Cullen, Jennifer: CIO-BI
Sent: Friday, September 21, 2012 05:00 PM
To: DPM-WE: Workstation Engineering Team
Cc: IT Security; Hagarty, Richard: CIO-BI
Subject: 16(2)(c)

Hello,

At this time we are seeing a number of anomalous activities within Industry Canada and the GC such as a higher than usual number of virus detections at IC, a Cyber Flash issued by CTEC late this afternoon, and the attached CCIRC Advisory informing of a 16(2)(c)

16(2)(c),21(1)(a),21(1)(b)

Thank you,
Jennifer

<< Message: CCIRC ADVISORY AV12-038: 16(2)(c) / CCRIC AVIS AV12-038 : 16(2)(c) 16(2)(c) >>

Jennifer Cullen
Team Lead, IT Security | Chef d'équipe, Sécurité TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Jennifer.Cullen@ic.gc.ca
Telephone | Téléphone **613-948-4029**
Facsimile | Télécopieur 613-946-3367
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Gosselin, Andrée: CIO-BI
Sent: Friday, January 25, 2013 13:57
To: Thompson, Kim: CAS-SCA; Hagarty, Richard: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; IT Security
Subject: Re: URGENT - 16(2)(c) - High Security Risk

Kim,
We are currently discussing next steps. Will give you an update as soon as possible.
Andrée

From: Thompson, Kim: CAS-SCA
Sent: Friday, January 25, 2013 01:51 PM
To: Hagarty, Richard: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; IT Security
Subject: RE: URGENT - 16(2)(c) - High Security Risk

Ok, thanks Richard, I will advise Robin and Susan as a "heads-up" as we do here.

Can you provide me with a brief overview of what your next steps are as Susan will ask? What will CIO or SSC be undertaking? Timelines? Who is conducting the Injury Assessment on the possible security breach?

Thanks,

Kim Thompson
Director, Security and Emergency Management | Directrice de la gestion de la sécurité et des urgences,
Departmental Security Officer | Agent de sécurité ministérielle
Corporate Facilities and Security Branch, CAS | Direction générale de la gestion des installations et de la sécurité, SCA
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Kim.Thompson@ic.gc.ca
Telephone | Téléphone 613-960-6169
Facsimile | Télécopieur 613-957-6543
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada 19(1)
19(1)

From: Hagarty, Richard: CIO-BI
Sent: January 25, 2013 1:24 PM
To: Thompson, Kim: CAS-SCA; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; IT Security
Subject: FW: URGENT - 16(2)(c) - High Security Risk

Hi Kim,
Please note that we are currently investigating an internal incident that started as a typical Phishing

campaign, which could lead to some significant security breach.

We will send the update as we have more detail on it.
Have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

From: Hagarty, Richard: CIO-BI
Sent: Friday, January 25, 2013 1:19 PM
To: Rinholm, Rick: CIO-BI; Acton, Kelly: CIO-BI; Basque Spickett, Diane: CIO-BI; Gosselin, Andrée: CIO-BI
Cc: Bullock, Sarah: CIO-BI; Rivard, Karen: CIO-BI; Hagarty, Richard: CIO-BI; Bernard, Mario: CIO-BI; ITSec
Subject: URGENT - 16(2)(c) - High Security Risk

Hi Rick,

Earlier this week, a Phishing incident was reported, which led the investigation to discover that this attack was actually originating from Industry Canada targeting both internal and external clients (both Private and Public sectors). Members of Industry Canada and Shared Services Canada just completed a joint meeting and agreed that the current finding is telling us that the 16(2)(c) was the tool used to initiate the attack.

Furthermore, Shared Services Canada reported that they have the evidence to support that other IC employee accounts have been compromised and used to access the 16(2)(c) service.

At this point, I am unsure of the extent of the damage and the impact this might have for Industry Canada and its portfolios. Therefore, **I would strongly recommend** 16(2)(c),21(1)(a),21(1)(b) 16(2)(c),21(1)(a),21(1)(b) until further notice.

If the recommendation is approved, I would also suggest 21(1)(a),21(1)(b) 21(1)(a),21(1)(b)

- 16(2)(c),21(1)(a),21(1)(b)

We are awaiting further direction before proceeding with any further action.

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Chief Informatics Office | Bureau de l'informatique
Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**
Facsimile | Télécopieur 613-946-3367

Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Lacroix, Lise: SBTMS-SMTPE

From: Thompson, Kim: CAS-SCA
Sent: Monday, January 28, 2013 15:53
To: Acton, Kelly: CIO-BI
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA; Strang Lindsey, Robin: CAS-SCA; Hagarty, Richard: CIO-BI; Lamoureux, Marie-Eve: CIO-BI
Subject: RE: URGENT - 16(2)(c)

Thank you for the update Kelly and Richard can keep me apprised of next steps.

Regards,

Kim Thompson
Director, Security and Emergency Management | Directrice de la gestion de la sécurité et des urgences, Departmental Security Officer | Agent de sécurité ministérielle
Corporate Facilities and Security Branch, CAS | Direction générale de la gestion des installations et de la sécurité, SCA
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Kim.Thompson@ic.gc.ca
Telephone | Téléphone 613-960-6169
Facsimile | Télécopieur 613-957-6543
Teletypewriter | Téléimprimeur 1-866-694-8389

Government of Canada | Gouvernement du Canada

From: Acton, Kelly: CIO-BI
Sent: January 28, 2013 2:51 PM
To: Thompson, Kim: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA; Strang Lindsey, Robin: CAS-SCA; Hagarty, Richard: CIO-BI; Lamoureux, Marie-Eve: CIO-BI
Subject: RE: URGENT - 16(2)(c)

Hi Kim,
By way of an update, I can confirm that based on SSC's analysis over the weekend, no are no longer concerned about the two specific 16(2)(c) accounts; therefore, as was the case at the outset, this incident concerns a single compromised account, and the actions that were taken by SSC and IT Security in response to that account are already well documented.

The 16(2)(c) service remains unavailable and I'm being briefed this afternoon at 4pm by SSC on options for next steps and timelines and can update you further coming out of that discussion. You are welcome to attend the discussion if you wish, but Richard will be there and can debrief accordingly.

Kelly Acton
A/Director General, Planning and Customer Relations |
Directrice générale intérimaire, Planification et relations avec la clientèle
Chief Informatics Office | Bureau de l'informatique

Small Business, Tourism and Marketplace Services | Services axés sur le marché, le tourisme et la petite entreprise
Industry Canada | Industrie Canada
235 rue Queen Street, Ottawa ON K1A 0H5
Office/Room: 388B West Tower
613-941-3445

From: Hagarty, Richard: CIO-BI
Sent: Monday, January 28, 2013 1:06 PM
To: Thompson, Kim: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Acton, Kelly: CIO-BI; Gosselin, Andrée: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Subject: RE: URGENT - 16(2)(c)

Hi Kim,

As you may have seen on Friday, the decision was taken to 16(2)(c) due to an increased level of phishing activity. An IT Bulletin was issued advising the department of the situation. Over the weekend, Shared Services Canada conducted a detail analysis to further assess the situation. It is expected that Shared Services Canada will provide a debrief of the findings before the end of the day.

I will provide further detail once we have been briefed and the situation is well understood.

Have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

From: Gosselin, Andrée: CIO-BI
Sent: Friday, January 25, 2013 1:57 PM
To: Thompson, Kim: CAS-SCA; Hagarty, Richard: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; IT Security
Subject: Re: URGENT - 16(2)(c) - High Security Risk

Kim,
We are currently discussing next steps. Will give you an update as soon as possible.
Andrée

From: Thompson, Kim: CAS-SCA
Sent: Friday, January 25, 2013 01:51 PM
To: Hagarty, Richard: CIO-BI; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; IT Security
Subject: RE: URGENT - 16(2)(c) - High Security Risk

Ok, thanks Richard, I will advise Robin and Susan as a "heads-up" as we do here.

Can you provide me with a brief overview of what your next steps are as Susan will ask? What will CIO or SSC be undertaking? Timelines? Who is conducting the Injury Assessment on the possible security breach?

Thanks,

Kim Thompson
Director, Security and Emergency Management | Directrice de la gestion de la sécurité et des urgences,
Departmental Security Officer | Agent de sécurité ministérielle
Corporate Facilities and Security Branch, CAS | Direction générale de la gestion des installations et de la sécurité, SCA
Industry Canada | Industrie Canada
235 Queen Street, Ottawa ON K1A 0H5 | 235, rue Queen, Ottawa ON K1A 0H5
Kim.Thompson@ic.gc.ca
Telephone | Téléphone 613-960-6169
Facsimile | Télécopieur 613-957-6543
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada 19(1)
19(1)

From: Hagarty, Richard: CIO-BI
Sent: January 25, 2013 1:24 PM
To: Thompson, Kim: CAS-SCA; Potvin, François: CAS-SCA; Little, Sandy: CAS-SCA
Cc: Cullen, Jennifer: CIO-BI; Gosselin, Andrée: CIO-BI; IT Security
Subject: FW: URGENT - 16(2)(c) - High Security Risk

Hi Kim,
Please note that we are currently investigating an internal incident that started as a typical Phishing campaign . We will send the update as we have more detail on it.
Have a nice day!

Richard Hagarty
Manager, IT Security | Gestionnaire, Sécurité de la TI
Industry Canada | Industrie Canada
Richard.Hagarty@ic.gc.ca
Telephone | Téléphone **613-948-7283**

Lacroix, Lise: SBTMS-SMTPE

From: Hagarty, Richard: CIO-BI
Sent: Sunday, January 13, 2013 11:08
To: Rinholm, Rick: CIO-BI; Gosselin, Andrée: CIO-BI; Acton, Kelly: CIO-BI; Basque Spickett, Diane: CIO-BI; Peters, Bernadette: CIO-BI
Cc: IT Security
Subject: RE: Sorry to intrude - Java issue

Hi Rick,

I have verified the background on this item and found the following.

At 1:55:59 PM Friday, CCIRC advised departments that a vulnerability was identified in Java, which allows remote attackers to execute arbitrary code by the user visiting a specially crafted webpage.

At 2:34:47 PM, IT Security was notified by SSC that 16(2)(c) 16(2)(c)

At 2:47:46 PM, IT Security communicated the relevant information with the rest of the organization (using the "IT Security Advisory / Avis Sécurité TI" distribution list)to ensure that proper action can be taken where necessary.

At this time, my understanding is that 16(2)(c)

The following is the actual mitigation strategy published by CCIRC through the Cyber Flash CF13-001 Oracle Java Zero-day Vulnerability :

16(2)(c)

Presently, the situation seems to be under control. This is one of many alerts we get on a weekly basis. In light of the current security measures now in place, 21(1)(a),21(1)(b) 21(1)(a),21(1)(b).

We will review our situation with our counterparts both in IC and SSC on Monday and determine based on the information available at that time if the situation warrants further action(s).

We will keep you posted if additional steps are necessary.

Have a nice day!

Richard

-----Original Message-----
From: Rinholm, Rick: CIO-BI
Sent: Sunday, January 13, 2013 9:50 AM
To: Gosselin, Andrée: CIO-BI; Hagarty, Richard: CIO-BI; Acton, Kelly: CIO-BI; Basque Spickett, Diane: CIO-BI; Peters, Bernadette: CIO-BI
Subject: Fw: Sorry to intrude - Java issue

Aware of this?

----- Original Message -----
From: Spurling, Brian: CMB-DGCM
Sent: Sunday, January 13, 2013 09:45 AM
To: Rinholm, Rick: CIO-BI
Subject: Sorry to intrude - Java issue

Anything needed to communicate to staff on this?

Disable Java to avoid potential hacking: U.S. Department of Homeland Security

This April 23, 2007 file photo shows the Java logo at Sun Microsystems' offices in Menlo Park, Calif. The U.S. Department of Homeland Security is...more
A+
BY THE ASSOCIATED PRESS, JANUARY 12, 2013
WASHINGTON — The U.S. Department of Homeland Security is advising people to temporarily disable the Java software on their computers to avoid potential hacking attacks.

The recommendation came in an advisory issued late Thursday, following up on concerns raised by computer security experts.

Experts believe hackers have found a flaw in Java's coding that creates an opening for criminal activity and other high-tech mischief.

Follow this links for instructions on disabling Java from Gizmodo.

Java is a widely used technical language that allows computer programmers to write a wide variety of Internet applications and other software programs that can run on just about any computer's operating system.

Oracle Corp. bought Java as part of a $7.3 billion acquisition of the software's creator, Sun Microsystems, in 2010.

Oracle, which is based in Redwood Shores, Calif., had no immediate comment late Friday.