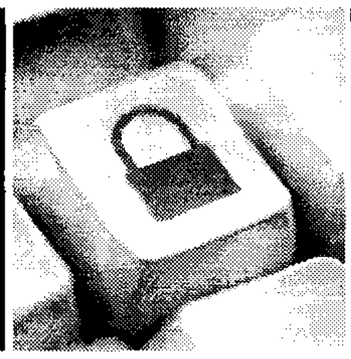
Public Safety Canada | Sécurité publique Canada



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CCIRC CYBER OPERATIONAL SUMMARY

REPORTING PERIOD: SEPTEMBER 16 – SEPTEMBER 29, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-015

PURPOSE

This product is intended to provide cyber information to partners and operators of vital systems in public and private sectors, in order to support operational and security decision-making in these organizations. It is based on information reported to and researched by the Canadian Cyber Incident Response Centre (CCIRC), and may not be indicative of the cyber environment in Canada.[1] This report also provides background information on the technical products released by CCIRC over the reporting period.

OVERVIEW

During this reporting period, CCIRC handled 65 incidents. Some of those reported to CCIRC include:

- A cyber intrusion targeted an industrial control systems (ICS) manufacturer;
- Default credentials found in industrial control system;
- Discovery of a vulnerability in a municipal Internet voting system by an independent researcher;
- ZeroAccess botnet affected an energy organization; and
- Public and private sector organizations infected with ZeuS, Conficker, and/or Flashback malicious software (malware).

Highlights

- Distributed denial-of-service attacks targeting United States (U.S.) financial institutions

- Official fix for vulnerabilities in Microsoft Internet Explorer released

In the news:

- Canadian energy organizations reportedly targeted by cyber espionage campaign

- Microsoft disrupts Nitol botnet

- Over half of Android devices said to have unpatched vulnerabilities

PRODUCTS RELEASED

CCIRC regularly issues information products to inform its partners of potential, imminent or actual cyber threats. During the reporting period, CCIRC issued four cyber awareness products, including one alert, one advisory, and two cyber flashes.

To address the vulnerability discovered in Internet Explorer, CCIRC issued an Alert (*AL12-001* - *Microsoft Security Advisory - Internet Explorer Vulnerability*) and an Advisory (*AV12-038* -

[1] Additional reporting by partners would help CCIRC contribute to a more accurate Canadian picture.

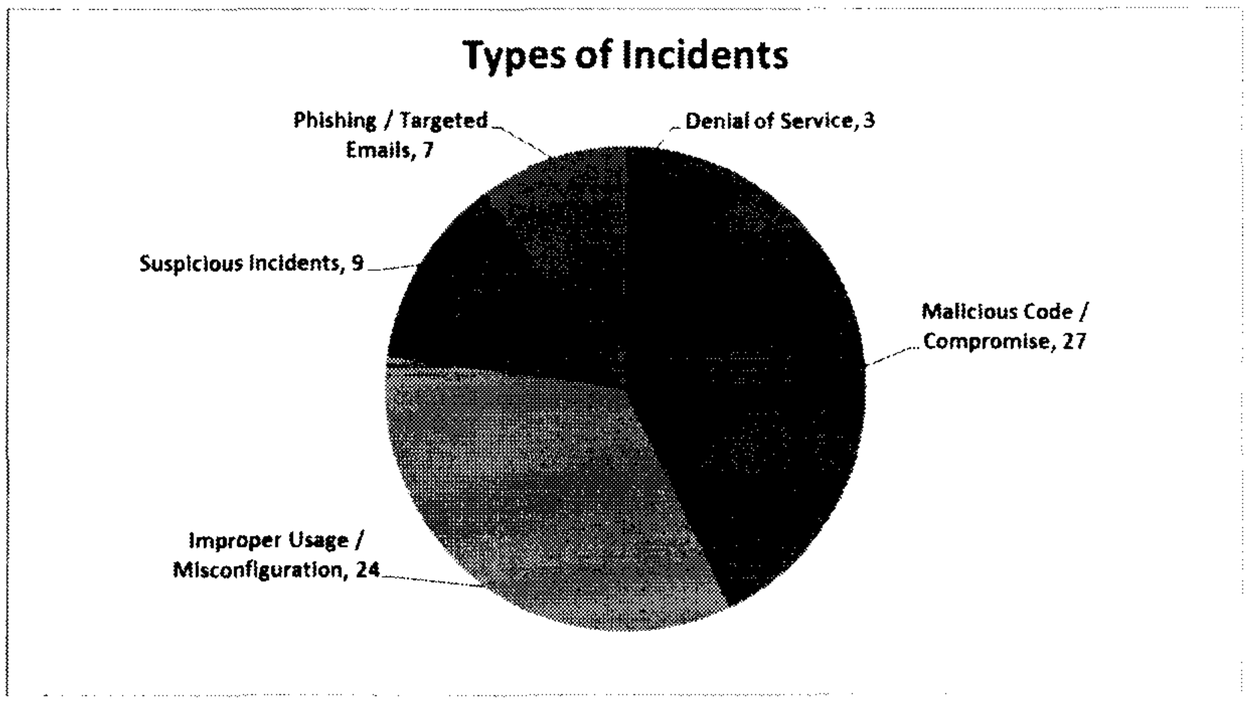
Microsoft Out-of-Band Security Bulletin) to its website. Additionally, CCIRC released a Cyber Flash (*CF12-015 - Internet Explorer Zero Day Vulnerability*) to provide its partners with details about this vulnerability, which allows an attacker to run arbitrary code in the context of the current user within Internet Explorer.

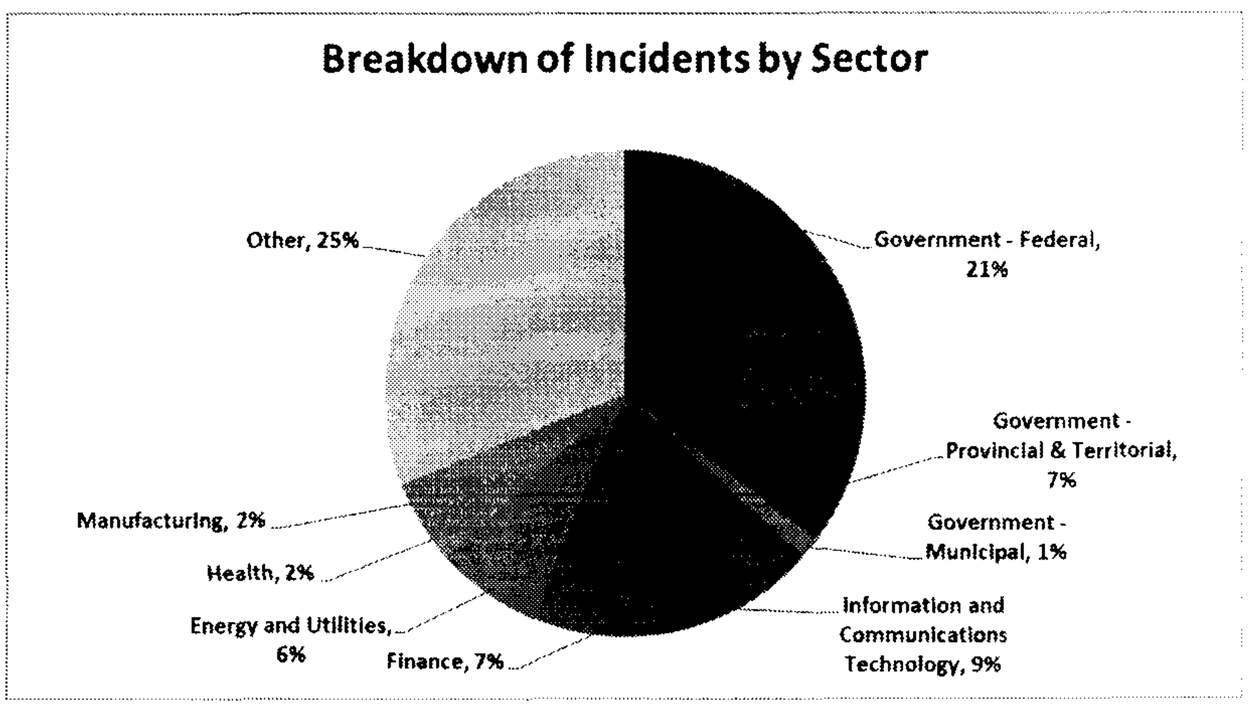
CCIRC also issued a Cyber Flash (*CF12-016 – ZeroAccess Botnet Activity*) to its partners to bring attention to the significant increase in the amount of ZeroAccess botnet activity, and to highlight this botnet's primary distribution mechanisms and detection indicators.

NEW INCIDENTS

Private Sector

Cyber intrusion targets ICS manufacturer – Open sources reported that a Canadian manufacturing company was targeted by a cyber intrusion. This intrusion reportedly affected its operations in several countries, including in Canada. The affected company has provided CCIRC with technical information related to the compromise, and has also notified its customers of the situation. CCIRC continues to work collaboratively with its domestic and international partners in order to provide mitigation assistance to this ICS manufacturer.





Distributed denial-of-service (DDoS) attacks targeting U.S. financial institutions – DDoS attacks have been targeting several United States financial institutions nearly every business day since September 21, 2012. Affected U.S. financial institutions, which include J.P. Morgan Chase, Bank of America, U.S. Bank, Wells Fargo, PNC, and Citigroup, have acknowledged experiencing intermittent service interruptions to their websites.

> *Comment: At this time, CCIRC is not aware of any Canadian organizations which have been affected by these attacks, and continues to monitor this situation. Open sources indicate that these DDoS attacks are expected to continue throughout October 2012.*
>
> *Background: Denial of service (DoS) and DDoS attacks are common, albeit rarely reported, malicious network actions aimed at disrupting the availability of computing resources from legitimate users. The affected systems are not infiltrated or infected, and data and information are not stolen.*

Malicious code infections and hosted DDoS tools – CCIRC identified a web server which was hosting DDoS tools, as well as several which were hosting Trojan-based malware. In all of these

cases, CCIRC issued a code removal request (CRR) to the relevant hosting providers. CCIRC's CRRs inform Internet Service Providers that they are hosting malicious content, website forgeries, and/or personal information.

Canadian energy organization affected by ZeroAccess – Following the release of the Cyber Flash (CF12-016, detailed above) regarding ZeroAccess botnet activity, an energy sector organization reported to CCIRC that it had found a host infected with ZeroAccess on its network. CCIRC provided mitigation advice to the affected organization, thereby enabling the removal of the malware.

Default credentials found in industrial control system – An independent security researcher discovered that a vulnerability involving default login credentials that, if exploited, could be used to perform actions on the system commensurate with the privileges associated with the default account, up to and including system modification and system shutdown. CCIRC contacted the affected organizations to advise them of this vulnerability, and offered mitigation advice.

Victim notifications – During the reporting period, CCIRC sent 675 notifications to some of its partners in Canadian public and private sector organizations whose computers were infected with the ZeuS, Conficker, and/or Flashback malware. These notifications also contained detection indicators and mitigation advice. In the case of specific incidents, individual notifications were sent to affected organizations.

Industrial Control Systems Security Best Practices

In recognition of the risks facing industrial control systems (ICS), CCIRC has published the *Industrial Control Systems (ICS) Security Best Practice Guide* (September 2012, v.1.5), which includes the following advice for ICS owners and operators:

- Define responsibilities for ICS cyber security;
- Develop an access control policy;
- Segregate sensitive ICS data from the corporate network;
- Use network segmentation to partition the system into distinct security zones;
- Minimize ICS exposure to the Internet;
- Classify all information and safeguard it accordingly;
- Require multi-factor authentication for remote access; and
- Monitor trusted computer emergency readiness team (CERT) websites (e.g. CCIRC, ICS-CERT) for advisory information on newly disclosed vulnerabilities in ICS products.

** A full version of this best practice guide is available from CCIRC.*

If you suspect your system has been compromised, critical infrastructure owners and operators are encouraged to contact CCIRC.

Phishing attempts – CCIRC responded to seven phishing attempts during the reporting period. Criminals impersonated financial institutions, an organization in the energy sector, and federal government organizations to solicit personal information, financial credentials, and/or other sensitive information from users via email. In all instances, CCIRC notified the phishing intake centres of the impersonated institutions. CCIRC also notified a third party phishing reporting service to add these sites to Internet browsers' list of untrusted websites.

Public Sector

Federal, Provincial, and Territorial Governments

Open resolver notifications – CCIRC obtained data from a trusted source which indicated that provincial and federal organizations were operating with open domain name system (DNS) resolvers. CCIRC notified the affected organizations and in certain cases, also notified the federal computer security incident response team (CSIRT).

Municipal Governments

Vulnerability discovered in municipal Internet voting system – An independent security researcher discovered these vulnerabilities, which if exploited, could have resulted in spoofing and thereby the disclosure of voters' personal information. CCIRC worked with the municipality and the voting system vendor to address the concerns raised by the independent researcher. The election took place, and the municipality reported to CCIRC that no unusual activities were observed.

UPDATE ON PREVIOUSLY REPORTED INCIDENTS

Official fix for vulnerabilities in Microsoft Internet Explorer –Microsoft issued a Security Bulletin (MS12-063) on September 21, 2012 that resolved the Internet Explorer vulnerabilities that were previously mentioned. If exploited, these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. As detailed above, CCIRC issued an Alert (AL12-001), a Cyber Flash (CF12-015) and an Advisory (AV12-038) relating to these vulnerabilities.

NOTEWORTHY ITEMS IN THE NEWS

Hacktivists' DDoS attacks target U.S., United Kingdom, and Swedish governments – All three governments reported intermittent website service interruptions, and several government websites were completely unavailable for short periods of time. Denial of service (DoS) and DDoS attacks are increasingly common malicious network actions aimed at disrupting the availability of computing resources from legitimate users.

Microsoft disrupts emerging Nitol botnet – The globally pervasive Nitol botnet, which used 500 different strains of malware hosted on more than 70,000 sub-domains, was disrupted when Microsoft was granted a court order to host the Nitol domain, which Microsoft's Digital Crimes Unit promptly took offline. In their study of the Nitol botnet, Microsoft reported that delivery mechanisms for Nitol-related malware included removable media (e.g. USB flash drives) and insecure supply chains, and that the botnet was used to enable DDoS attacks, among other uses.

Canadian energy organization targeted by cyber espionage campaign– Independent security researchers at Dell SecureWorks reported that a Canadian energy organization had been the victims of cyber espionage, which had involved spear phishing as a delivery mechanism for malware.

Over half of Android devices have unpatched vulnerabilities – Security company Duo Security reported that their "X-ray scanner" application has uncovered numerous vulnerabilities in Android related to malware and rootkits, many of which grant access commensurate with the privileges of the legitimate user.

New 'CRIME' attack method could exploit weakness in HTTPS – Independent security researchers uncovered an attack method that grants access to a user's session cookie, used to remember authenticated users, and thereby enabling access to that user's account. Most websites use HTTPS (Hypertext Transfer Protocol Secure, which is more secure than the standard HTTP) protocol to authenticate users and encrypt session cookies, but this new attack method is able to circumvent this security feature.

PUBLISHED INTERNET THREAT REPORTS

IBM X-Force: 2012 Mid-year Trend and Risk Report (September 2012) – In this biannual report, IBM reported on the threats, operational security practices, software development security practices, and the emerging trends in security it saw in the first half of 2012. While pointing out that they have seen over 4,400 new vulnerabilities thus far in 2012, and that this year is on track for breaking the record for the number of discovered vulnerabilities, IBM stressed that "systems' interconnectedness, poor policy enforcement, and human error [are] far more influential than any single security vulnerability" (page six).

IBM's X-Force also reported that, in the first half of 2012, SQL injections remained the top attack technique and that cross-scripting vulnerabilities for web applications accounted for approximately half of known web application vulnerabilities. Bright spots highlighted by IBM included the lower levels of spam and phishing, which are in part due to the takedown of the Grum botnet by security company FireEye in July 2012.

FEEDBACK

Your feedback is appreciated and critical to making this product useful for you. Please email any feedback you have to Ken Bendelier, Manager, Operational Analysis and Support Section, at kenneth.bendelier@ps-sp.gc.ca.

OUR ORGANIZATION

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber events. It does this by providing authoritative advice and support, and coordinating information sharing and event response.

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators who wish to report cyber incidents may send associated email reports to cyber-incident@ps-sp.gc.ca, using the CCIRC Cyber Duty Officer PGP encryption key, available at the following address: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

Beaudoin, Luc

From: [redacted]
Sent: Tuesday, October 09, 2012 1:15 PM
To: CCIRC-CCRIC; [redacted]
Cc: [redacted]
Subject: RE: CCIRC CE-12-003695 [Halifax Internet Voting]

Good day . Electronic voting has been proceeding well since Saturday am. Just over 5% of eligible voters across HRM have cast their ballots with just under 10% casting their ballots by phone.

Most sincerely;

[redacted]

-----Original Message-----
From: CCIRC-CCRIC [mailto:[redacted]
Sent: October-09-12 11:32 AM
To: [redacted]
Cc: [redacted]
Subject: CCIRC CE-12-003695 [Halifax Internet Voting]

Dear [redacted]

We appreciate your feedback. How was the vote on Saturday, October 6th, 2012?

Thank you,

Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
www.publicsafety.gc.ca

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

----Original Message----
From:
Sent: October-05-12 11:07 AM
To: CCIRC-CCRIC
Cc:
Subject: Re: CCIRC CE-12-003695 [Halifax Internet Voting]

Dear Mr(s),

Find here under our feedback to your concerns about the overall security of our solution for the HRM Elections 2012.

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

[redacted]

In the event you need any further information, please don't hesitate to contact us again.

Kind regards,

[redacted]

Senior Consultant

[redacted]

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

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

On Thu, 10/04/2012 05:18 PM, "CCIRC-CCRIC" < [redacted] wrote:

Greetings,

CCIRC would like to raise the following concerns with your organization:

[redacted]

4

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

[redacted]

Acknowledging that this is not the first time such system is used in Canada. Due to the Poll will be open on October 6th, 2012; we appreciate your taking the time to get back to us with a response.

Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]

s.16(2)(c)

http://www.publicsafety.gc.ca

Reference:

s.16(2)(c)

Beaudoin, Luc

From: [redacted]
Sent: Wednesday, October 03, 2012 11:40 AM
To: CCIRC-CCRIC
Cc: [redacted]
Subject: Fw: CCIRC CE-12-003695 [Halifax Internet Voting]

Attention Virvak Phlek,

As per our conversation this morning, please send any concerns regarding the Halifax Region Municipal election. Please copy all on this email, as they will be addressing the concerns.

Thank you,

[redacted]

From: Election, HRM
Sent: October 2, 2012 4:37 PM
To: [redacted]
Subject: FW: CCIRC CE-12-003695 [Halifax Internet Voting]

-----Original Message-----
From: CCIRC-CCRIC [mailto:[redacted]
Sent: October 2, 2012 4:37 PM
To: Election, HRM
Subject: CCIRC CE-12-003695 [Halifax Internet Voting]

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

Good Day,

The Canadian Cyber Incident Response Centre (CCIRC)* has received a report that raise some concerns regard to Internet Voting Campaign. Would it be possible for you to contact CCIRC to discuss those issues? Please provide this reference number CE12-003695 for any further correspondence relate to this matter.

Kind Regards,

Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
www.publicsafety.gc.ca

-

[redacted]

14

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

[redacted]

s.20(1)(c)

[redacted]

Beaudoin, Luc

From: Beaudoin, Luc
Sent: Tuesday, October 02, 2012 1:18 PM
To: Phlek, Vireak
Cc: CYBERDO
Subject: CE12-003695

I need you to take this on for me. See event number. There is a PDF attached. I need you to contact the vote system developer and walk them through this so they improve their implementation.

This is URGENT. Their election is 6 October !!!!!

ictsd@halifax.ca or (902) 490-4444

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574

luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>

PublicSafety.gc.ca | securitepublique.gc.ca

Government of Canada | Gouvernement du Canada

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

CCIRC Internal Portal - CDO Watch and Operations » Ops Log: Municipal election system potential vulnerability

The content of this item will be sent as an e-mail message to the person or group assigned to the item.

CE-Number	CE12-003695
CCIRC Handler	Phlek, Vireak
Title	Municipal election system potential vulnerability
Status	Closed
Entry Type	INCIDENT - Cat 4 - IMPROPER USAGE / MISCONFIG
Summary	A researcher identified a potential vulnerability in the voting system of a municipality.
Updates	Phlek, Vireak (10/9/2012 11:13 AM): Organization responded with their feedback. They took steps to mitigate some of our concerns. Closed Phlek, Vireak (10/4/2012 3:38 PM): Email with CCIRC concerns was sent to the project manager. He will get back to us with theirs answers. Phlek, Vireak (10/2/2012 6:02 PM): CCIRC request information from Halifax voting. In the same time CCIRC learns that Halifax used that internet voting in 2008. http://en.wikipedia.org/wiki/Electronic_voting_in_Canada Beaudoin, Luc S (9/28/2012 3:19 PM): The municipality is halifax. The contact information is: We will follow up on Monday. Description of the issue in Cyberdo mail.
CI Sector Affected	1b. Government (Municipal)
Reporting Organization	
Response	Mitigation - Advice to affected organization
Related product	
Response - Team	Mitigation - Team - Victim
Escalation - Risk Assessment	
Review and Lessons Learned	
Date Closed	
Related Log Entries	
Primary Contact	
_NOT_USED_Daily_summary	CE12-003695 Municipal election system potential vulnerability Summary: Status: Closed Owner:
_NOT_USED_REF_COL_LOOKUP	CE12-003695 [Municipal election system potential vulnerability]
_NOT_USED_Secondary Contact	
_NOT_USED_Take-down	No
_NOT_USED_IATFF Category	Event
_NOT_USED_Notification	No
_NOT_USED_Primary Event	No
_NOT_USED_Related Event(s)	
_NOT_USED_Assigned To	
Not_Used_ Severity	Normal
_NOT_USED_Priority	(2) Normal
_NOT_USED_Due Date	9/28/2012 4:00 PM
NOT_USED_INCIDENT_Category	Cat 0 - EXERCISE
NOT-USED_Impact	Unknown
NOT-USED_CCIRC/GOC Related Product Number	
Exempt from Policy	No exemption. Exempt from policy...
Related Log Entries:CE-Number	
Attachments	CCIRC Halifax Election Concerns.pdf

Version: 6.0
Created at 9/28/2012 3:19 PM by Beaudoin, Luc S
Last modified at 10/9/2012 11:13 AM by Phlek, Vireak

[Close]

s.16(2)(c)

Beaudoin, Luc

From: [redacted]
Sent: Friday, September 28, 2012 2:46 PM
To: CYBERDO
Subject: See message
Attachments: CCIRC Halifax Election Concerns.pdf.pgp

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG/MacGPG2 v2.0.17 (Darwin)
Comment: GPGTools - http://gpgtools.org
Comment: Using GnuPG with Mozilla - http://www.enigmail.net/

hQIOA4v7Lo5QmG2hEAgA5Q5uLhnSm+vT8+xC6mcc7SGmn0X1zDtqk2ggpdTZMVCr
gugTo0dHGe1hw0v+ayyC5etItAc0/N9u0y1jgZISsSX2Jf5vknEKsooGg69mCzZn
gYZb4IMFvHyKwRNJN0Ngfd+WmSTRr4uwMqHyqe8tcZJNjE3MipSTXNZLNVLTN114
uO7x88lHjX1+NFxJOK335uTOktoU1+WnLmgUHDGF3UlHEsE58aK56SGUlhS1X2w1
AluX+tijdTIq/XYxFXzyP0TVft4puEj2IdAQzGvHYBH088TxZC/K9Zmx7vqdcsLw
4WbnhvXE5z2l5eV+sEQBPl9lycGRg14+BMo/+cpM4Qf/XviBDtYZQ1aEogWZnFF2
tEG2jStlSu5V1SylQFn6QLKcwXlGn0jPuj1/+dXKanlUWxOlOkNbhfN+DgNSpyc/
sgvsmYexsrso7lB2xr9KANHBUJFe/GuQSZ9dU0bPRO8ksV9zt5tnW9EHWV6uJKhQ
gXT2bwSqVktV32t6OcGKDm7x8ECnh52XSFQs32vOkPxFBFaNQN2SOIu2lJSu8XER
3ZsF1xVef7v7y9QlXw9GUoQQefyGE5Bh6TR49eDeA2spF1ecfeMX7nWlF00t5n/F
x9ul+p0aaylevzqlaXHF5ohgLs8YK9GKCtI3fXz63YKlSCBCuoHzVU+pN5SpVnBo
AlUCDANKlOyj5bX7NQEP/1zXDsBG3DmuMZ4a5cDeJYcDNgNr5q6G7N90wYW4B7zz
P771QcUXqMBmOwKWikNUCIz1ll9NJYScb+s5xPBJfSHOB2BnQKEJWEtl6cbJrdGn
IMDKlJPnGlM+gtsHdVlltA70LvZpJRAWadMJz+1ydyDJ7ZbrltSkAdyZ21CSSAOf
cQJ7zFVEDuPKJ/eCMk/nsxlgodoo5srLXQmmfXKUfe8azM97MTCLDXxRDGvr7aRz
h73tM1zAE9WIlszL10Jl2zhOKOu/EYln2QRoREXzLocT1x19oGGSLDfhBg/eyK2h
k021doZM8j8FveH7RxM9u5MZYjShpaG+jam+34zJlEFKklvwwkv4ZkjDhrBsagaj
sLB/kKlIet7vO+q1aW+ET6el0+Y31E/IMVdw2UEMXwgTphEso5L2rU6lvgvT+qog
WL5StPa3h7+20lhzn+fTd+zLSdkBulAjpxJaeuz25fXdOW8gMtbKlYNxD+/dUcp9
choGVCF1DplREYL2fLQcsd6TQncYK1la6oOlBWkQ3hp3bmWgcHLHTO10HX3ylplJ
Xnb879FsxXGXn47CP3LRflOT89LSlHOLjlYZnOtGhE2ocVpM5Hx13KSKhF3FhmYj
4AZfJ3mcO0G9pY8OAC0Bj9W9ouGwHVN/GOldzDuAvCEvt+HUhGX1olZMWSov0NYm
0oYBERQkSPlFV2Fi5k4CH6gev9puPlhNVCFGwkjf5b3FdR2HGAPAqcB7KrNhPb0F
nOpkYe+1V4Plulvrrd2QD9sej/lpav8s5koZJJAaV0+olV1uex06YlocBJbxXlRW
33qaw5gO1W0YKld6DeC5LbPaUFK3v4uHxSbHl0rq+LHqrSSDRg2MUQ==
=Lr5P
-----END PGP MESSAGE-----

s.19(1)

[redacted]

September 28, 2012

ATTN: Candian Cyber Incident Response Centre (CCIRC)
FROM: [redacted]

[redacted]

[redacted] **Before election day voters are provided a card directing them to visit "vote.halifax.ca". The voting card example found at http://www.halifax.ca/election/evoting12.html does not contain instructions to use a HTTPS url or instructions on how to verify the polling site identity presented to the voter. All major browsers will interpret a voter input of 'vote.halifax.ca' to mean http://vote.halifax.ca.**

[redacted]

[redacted]

[redacted]

[redacted]

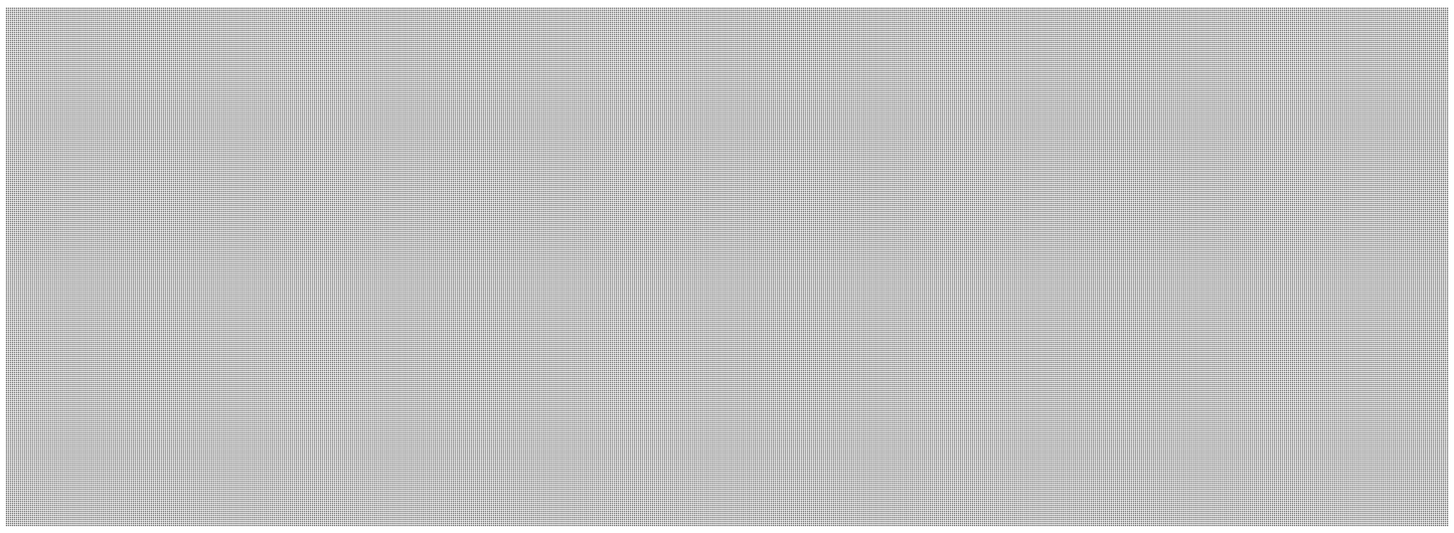
s.16(2)(c)

[redacted]

As of 10 Sep 2012, the Halifax election site presents the login link as a third-party domain, with voters being directed from the vote.halifax.ca site to securevote.ca.

[redacted]

s.16(2)(c)



s.16(2)(c)

Beaudoin, Luc

From: [redacted]
Sent: Thursday, September 27, 2012 6:03 PM
To: Beaudoin, Luc
Subject: Updated CCIRC contact

Hey Luc,

Are you still in this role? May have some vulnerability info for you affecting the Halifax online election coming up.

–

[redacted]

s.19(1)

Beaudoin, Luc

From: [redacted]
Sent: Tuesday, September 04, 2012 4:40 PM
To: [redacted]
Cc: Beaudoin, Luc
Subject: RE: Under attack - N1-U1

Hi [redacted]

Any significant anomalies in traffic get picked up by netflow monitoring, and go to the NOC for action. Good luck!

[redacted]

From: [redacted]
Sent: September 4, 2012 02:37 PM
To: [redacted]
Cc: [redacted] Luc.Beaudoin@ps-sp.gc.ca
Subject: RE: Under attack - N1-U1

Hi [redacted]

Just came out of a meeting on this. They have installed an IPS in rush over the weekend to add a layer of protection. They should be OK.
At this point, not sure I could (they couldn't) be specific on what to look for except for anything that seems to be triggered to news agencies in the province of Quebec. That's too large for a request but if any of you happens to see anything... [redacted] will be on a proactive bridge with them to this subject tonight and keep us posted should anything occur.

Thanks again,

[redacted]

[redacted]

Devez-vous imprimer ce courriel ?

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

2012-09-04 12:20

A

"Luc.Beaudoin@ps-sp.gc.ca" <Luc.Beaudoin@ps-sp.gc.ca>

cc

Objet

RE: Under attack - N1-U1

Hi

I'll see what I can dig up in flow records w/ PfSP.

Do you recommend/request us to watch for traffic like tonight?

From:
Sent: September 1, 2012 01:23 PM
To: ; Luc.Beaudoin@ps-sp.gc.ca
Subject: Under attack - N1-U1

Hi all.

N1 - U1

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

[redacted] **is under attack since yesterday 20h00. Might be a UDP bomb on port 80. One of the attacking address seems to be** [redacted]
The attacked addresses are [redacted].
The fear is that it might be a practice for next Tuesday's election night
Have you seen anything throu your monitoring tools or other means ?

Thanks

[redacted]

[redacted]

Devez-vous imprimer ce courriel ?

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