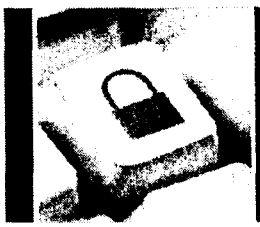


Canadian Cyber Incident Response Centre

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

2012 Cyber Operational Report

Canadian Cyber Incident Response Centre

March 8, 2013

DISCLAIMER

Produced by Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC), the *2012 Cyber Operational Report* is UNCLASSIFIED and is the property of the Government of Canada and has been provided to your organization in confidence. This report is not to be distributed without the consent of CCIRC.

REPORTING CYBER INCIDENTS

The CCIRC Cyber Duty Officer is the point of contact for partners and operators of vital cyber systems of national importance, including the critical infrastructure community, to report cyber incidents to CCIRC and to receive assistance in managing these incidents.

CCIRC Cyber Duty Officer Email: CCIRC-CCRIC@ps-sp.gc.ca

For secure communications, the CCIRC public Entrust Key is available upon request. Alternatively, the CCIRC Public Pretty Good Privacy (PGP) key (Text format 3KB) is also available for download.

Canada

Executive Summary

The purpose of the Canadian Cyber Incident Response Centre's (CCIRC) inaugural *2012 Cyber Operational Report* is to provide an overview of the noteworthy trends and incidents observed by CCIRC in 2012, and to highlight several case studies and security best practices.

As Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents affecting Canada's vital cyber systems, CCIRC is well positioned to report on these trends and incidents for the benefit of its partners. In 2012, CCIRC observed several noteworthy trends and incidents related to malware and exploit kits, advanced persistent threat (APT) attacks, hacktivism, and risks to industrial control systems (ICS).

Most of the 924 incidents handled by CCIRC in 2012 affected the finance, information and communication technology (ICT), and energy and utilities sectors, while malicious software (malware) and phishing emails were the two most prevalent incident categories overall. Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or to install malware. Most of the phishing reported to CCIRC in 2012 impersonated organizations in the finance sector.

Throughout 2012, CCIRC observed the prevalent use of exploit kits that automate the exploitation of system vulnerabilities in order to install malware. These exploit kits, such as Blackhole, allow malicious actors to spread malware with relative ease and, as a result, gain access to the affected computing devices. Exploiting vulnerabilities was also essential to the spread of crimeware such as Zeus, which is typically used to steal banking credentials.

In 2012, CCIRC observed that hacktivists, which are ideologically or politically motivated hackers, continued to broaden the scope of their targets beyond governments and the defence industrial base subsector, and made improvements to their tradecraft. As in previous years, CCIRC observed that distributed denial-of-service (DDoS) attacks were commonly carried out by hacktivists.

Over the past few years, CCIRC has observed an increase in the number of reported APT attacks targeting Canada's vital cyber systems. The malicious actors who carry out these attacks, which have the level of capability and intent generally associated with but not limited to those possessed by a nation state, have continued to improve their methods and have targeted organizations of all sizes in an increasing number of sectors.

In 2012, there was an increase in the number of incidents involving ICS handled by CCIRC, and CCIRC became aware of an increase in the number of Internet accessible ICS devices. Connecting ICS to the Internet provides a vector through which a malicious actor can gain access to and subsequently disrupt the ICS. As ICS are used to automate processes such as the generation and transmission of electricity, discrete manufacturing, and wastewater treatment, disruptions of ICS have the potential to impact human health and safety.

2012 Timeline of Noteworthy Events

MAR | FEB | JAN

- Malicious data exfiltrated from a multinational defence industrial base subsector organization
- Department of Homeland Security (DHS) reported an increase in threats to energy sector ICS
- CCIRC and the Canadian Internet Registration Authority developed www.dns-ok.ca to help identify Canadian victims of Domain Name System (DNS) Changer malware
- Increased reporting of ransomware impersonating the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS)
- Take down of a Zeus botnet led by Microsoft and associated victim notifications by CCIRC
- Canadian energy sector organization targeted by APT actors

JUN | MAY | APR

- Apple Trojan Flashback first reported
- Oracle Java exploits increased
- Surge in Zeus information theft crimeware activity
- Hacktivists targeted Government of Canada and critical infrastructure organizations
- Flame/sKyWIper advanced malware discovered
- Shamoon/DistTrack malware targeted energy organization based in the Middle East
- Internet Explorer vulnerability used in watering hole tactics discovered[1]
- Gauss information theft malware uncovered
- Provincial government websites targeted by a DDoS attack in support of student protests

SEP | AUG | JUL

- Grum botnet taken down
- Surge in ZeroAccess crimeware activity
- Internet Explorer vulnerabilities discovered and subsequent out-of-cycle patch issued[2]
- Mirage remote access Trojan campaign reported
- Canadian ICS manufacturer targeted by APT actors
- Microsoft Corporation disrupted Nitol botnet's 3322.org
- DDoS attacks targeted U.S. financial institutions
- Version 2 of the Blackhole exploit kit discovered

DEC | NOV | OCT

- Another wave of DDoS attacks targeted the U.S. finance sector
- Spear phishing campaign focussed at energy sector
- Canadian oil and gas company targeted by APT actors
- 'Dexter' malware targeting point-of-sale systems reported
- A second Internet Explorer vulnerability used in watering hole tactics discovered[3]
- Phishing campaign impersonating Canada Post or Air Canada to spread Zeus crimeware ran throughout 2012

[1] Reference(s): AV12-027 (see MS12-037); CVE-2012-1875.
[2] Reference(s): AV12-038; CVE-2012-1529, CVE-2012-2546, CVE-2012-2548, CVE-2012-2557, and CVE-2012-4969.
[3] Reference(s): AV13-001; CVE-2012-4792.

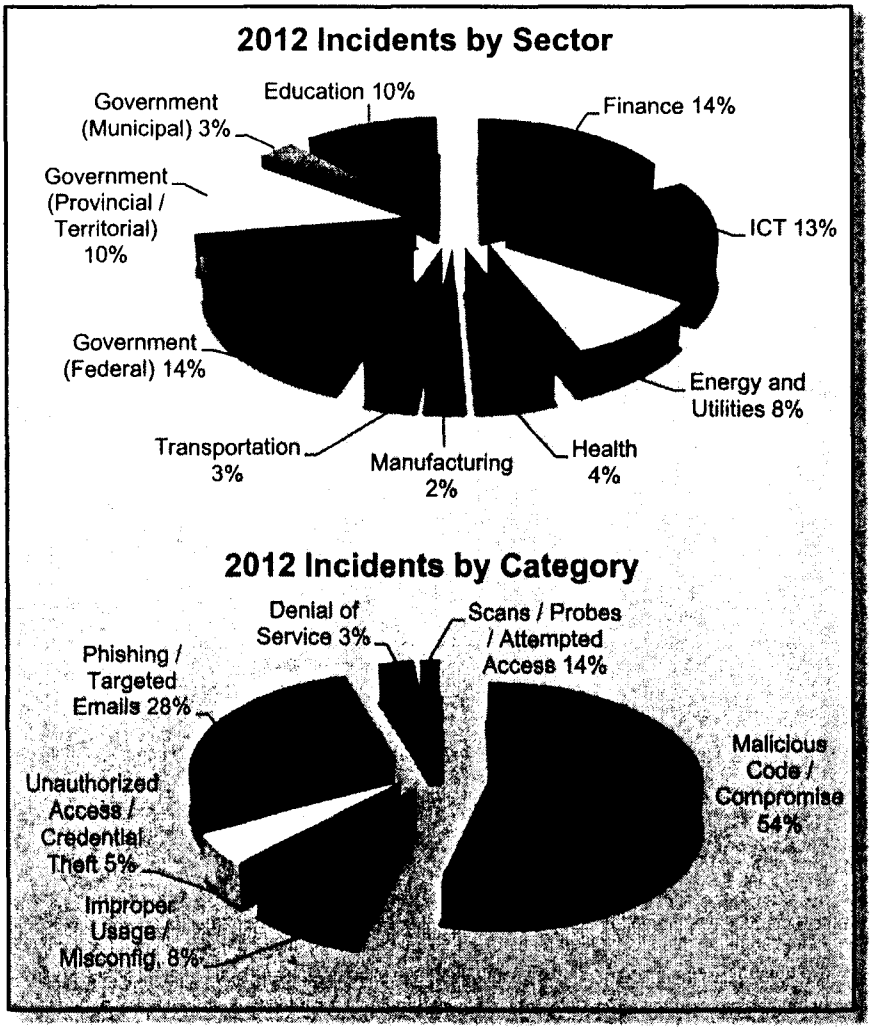
Contents

Noteworthy Trends in 2012

In 2012, Public Safety Canada's CCIRC observed several noteworthy trends and incidents which affected the operators of Canada's vital cyber systems. This section begins by summarizing the sectoral and incident category breakdown of the incidents handled by CCIRC and, in turn, discusses these incidents and the trends these represent in terms of malware and exploit kits, APT, hacktivism, and risk to ICS.

Most of the 924 incidents handled by CCIRC in 2012 affected the finance, ICT, and energy and utilities sectors, in that order. CCIRC defines an incident as a single or series of unwanted or unexpected information security events that have a significant probability of compromising the business operations or information security of Canada's vital cyber systems.

It should be noted that the relatively high number of incidents handled by CCIRC which affected the ICT sector is largely due to the fact that all vital cyber system operators rely upon the services of an ICT organization, and is not solely indicative of the state of security of the ICT sector itself. Similarly, the relatively high number of incidents in the finance sector is due to the fact that this sector is the most commonly impersonated sector in phishing emails, and is thereby not indicative of the state of security of the finance sector itself.



Malware / malicious code, and phishing / targeted emails were the two most prevalent incident categories (incident categories are defined in Annex C) handled by CCIRC in 2012. Zeus, Conficker, ZeroAccess, Sality, and Flashback were among the most pervasive malware families observed by CCIRC throughout the year.

Phishing / targeted emails was the second highest incident category in 2012. Most of the phishing observed by CCIRC throughout the year impersonated the finance, safety, and government sectors. While CCIRC observed steady levels of phishing throughout the year, there was an increase in the amount of spear phishing.

Malware and Exploit Kits

The use of exploit kits, which automate the exploitation of known web browser, application or system vulnerabilities in order to install malware, was a prevalent cyber security trend throughout 2012. As exploit kits can be leased on the crimeware market, they enable malicious actors to spread malware by exploiting vulnerabilities with relative ease and, in turn, gaining access to the infected computing devices.

One prevalent exploit kit observed by CCIRC throughout 2012 was Blackhole, which first appeared in 2010 and uses either phishing emails or infected legitimate websites to unknowingly redirect users to websites hosting its exploit code. Often leased by its authors, Blackhole was the exploit kit used in many of the malware infections handled by CCIRC throughout 2012. A second version of Blackhole, which caused many previous detection mechanisms to become ineffective, was discovered in September 2012. As a result, CCIRC issued a Cyber Flash (CF12-018) containing time sensitive indicators of compromise and detailed mitigation information for Blackhole version 2.0. CCIRC issues Cyber Flashes to its partners to provide them with mitigation information regarding immediate security issues.

Exploiting vulnerabilities was also key to the spread of the prevalent ZeroAccess rootkit, which functions by concealing its presence on a computing device in order to add it to a botnet. ZeroAccess has infected millions of computing devices worldwide and continues to be used for various fraudulent moneymaking activities for its authors. Its primary distribution mechanisms include exploit kits such as Blackhole, drive-by downloads from seeded websites, malicious advertising (malvertising), and phishing emails. CCIRC issued a Cyber Flash (CF12-016) describing ZeroAccess and providing mitigation advice to partners.

The upsurge in the use of exploit kits was facilitated, in part, by the prevalence of highly exploitable vulnerabilities discovered in Java and in commonly used applications, such as those produced by Microsoft and Adobe. For example, CCIRC released several cyber awareness products regarding two separate highly exploitable Internet Explorer vulnerabilities, the latter of which was found to have been used in watering hole attacks (detailed below). A list of the vulnerabilities that CCIRC observed being actively exploited in Canada in 2012 is included in Annex B.

Throughout 2012, CCIRC sent numerous victim notifications to organizations which were found to be operating with an open DNS resolver. Operating with an open DNS resolver can have a number of adverse consequences, such as allowing outsiders to consume resources that do not belong to them, potentially allowing attackers to exploit DNS flaws for the purpose of poisoning the cache of the open DNS resolver, or the inadvertent use of the affected computing device in a DDoS attack. Additionally, a malicious actor can leverage an open DNS resolver to conceal some of their malicious activities.

Additional information on malware can be found in Annex D, while mitigation information can be found in CCIRC's Technical Report (TR11-001) *Malware Infection Recovery Guide*.

Case Study: Domain Name System (DNS) Changer

The DNS Changer malware was a massive online fraud that infected approximately four million computers globally with various types of malware. The authors of this malware managed to infect victims' computers with malicious code that changed the victims' DNS configurations to forward all their DNS requests to a rogue DNS server rather than the legitimate one typically provided by their Internet service provider (ISP).

The U.S. Federal Bureau of Investigation conducted a two-year investigation that led to several arrests in the U.S. and to the seizure of the malicious DNS Changer infrastructure. CCIRC led Canada's response and participation in this global mitigation effort.

Initial assessments indicated that approximately 100,000 Canadian computers were potentially infected. CCIRC sent notifications to owners of infected computing devices and provided mitigation advice to Canadian stakeholders. CCIRC also posted Information Note (IN11-002) *DNS Changer Infrastructure and TDSS/ Alureon/ TidServ/ TDL4 Malware* to its website to raise awareness and provide mitigation information regarding DNS Changer and its related malware strains. Following the release of this Information Note, CCIRC observed a significant increase of activity on its website.

CCIRC also led work with Canadian ISPs and with the Canadian Internet Registration Authority (CIRA) to identify and notify victims. In February 2012, this collaboration led to the launch of the www.dns-ok.ca website (which is no longer needed and is now inactive), which allowed visitors to check if their computer was affected by DNS Changer. Overall, these efforts significantly reduced the number of infected computers in Canada.

Advanced Persistent Threats

Over the past few years, the number of reported APT attacks against Canadian organizations in the public and private sectors reported to CCIRC has increased. These malicious actors have continued to improve their methods and have targeted organizations of all sizes in an increasing number of sectors.

Often using social engineering in combination with Web or email techniques to infiltrate and subsequently steal information from targeted organizations, the intent and level of capability of APT actors is generally associated with those possessed by a nation state. While APT actors may use sophisticated techniques, such as advanced malware which exploits previously unpatched system, application, or browser vulnerabilities, it is the overall methodology employed by APT attackers which makes these operations unique.

APT actors carefully select their targets and refine each attack such that the targeted individuals become the conduit to their organization's information assets. Once a foothold is established,

APT actors move laterally throughout the network to exfiltrate sensitive information, or to take control of aspects of the network itself.

Spear phishing, which targets key personnel within an organization, was a common APT attack technique in 2012. One spear phishing campaign observed by CCIRC, which mainly targeted the energy and utilities sector, ran throughout the year. CCIRC received multiple reports of this campaign from targeted organizations, and from domestic and international partners.

As a result, CCIRC provided impacted organizations with mitigation advice based on its technical analysis of these phishing emails and their malicious attachments. Throughout 2012, CCIRC released multiple iterations of a Cyber Flash (CF12-003) with time sensitive mitigation information to its partners as the malicious group changed its approach over time in an effort to outpace the security community's efforts to detect and mitigate this campaign. CCIRC continues to monitor this situation.

Watering hole tactics were another advanced attack method observed by CCIRC. This tactic involves concealing malicious code on legitimate websites which are frequently visited by employees of the targeted organization, such as the website of a partner in their supply chain. When the potential victim visits a compromised website, they are involuntarily redirected to the malicious infrastructure which delivers malware onto their system and, in turn, allows the attacker to gain access to the affected computing device commensurate with that of the victim.

Top Five Mitigation Actions

Implementing the following recommended actions will help prevent the majority of reported cyber incidents. CCIRC strongly recommends that all organizations use them.

1. Undertake **application whitelisting** of permitted/ trusted programs, to prevent execution of malicious or unapproved programs.
2. **Patch applications** such as Adobe PDF viewers and Flash Player, Microsoft Office, and Java Runtime Environment. Patch or mitigate high risk vulnerabilities within two days.
3. **Patch operating system** vulnerabilities. Patch or mitigate high risk vulnerabilities within two days.
4. **Minimize the number of users with domain or local administrative privileges.** Such users should use a separate unprivileged account for email and web browsing.
5. **Disable local administrator accounts** to prevent network propagation using compromised credentials that are shared by several computers.

Developed by the Government of Australia for addressing targeted cyber intrusions, Annex A contains a complete list of the 35 mitigation actions for which there is a broad international consensus.

In 2012, CCIRC notified several Canadian ISPs of IP addresses which were found to be hosting malware for APT campaigns using watering hole tactics. In addition, vulnerabilities discovered in commonly used software, including Microsoft Internet Explorer in the latter half of 2012 were found to be exploited primarily by advanced attackers using watering hole tactics. CCIRC posted several Alerts and Advisories to its website to raise awareness and provide mitigation information regarding these vulnerabilities, and issued a Cyber Flash (CF12-022) to its partners that contained additional time sensitive details and mitigation advice.

These are just two examples of APT campaigns observed by CCIRC in 2012. Given the success of APT actors with spear phishing and watering hole techniques, CCIRC expects these types of attacks to continue. Additional background information and mitigation advice can be found in CCIRC's Technical Report (TR11-002) *Mitigation Guidelines for Advanced Persistent Threats.*

Hacktivism

Activist hackers, or hacktivists, are ideologically or politically motivated hackers who target governments, private firms and individuals whose activities or purposes appear to be in conflict with the principles espoused by the group. In 2012, hacktivist collectives continued to broaden the scope of their targets beyond governments and the defence industrial base subsector, and made improvements to their tradecraft.

Denial-of-service (DoS) attacks have been used pervasively by hacktivist groups, such as 'Anonymous', for several years, and 2012 was no different. The affected systems are not infiltrated or infected with malware, and data is not stolen.

A distributed denial-of-service (DDoS) attack aims multiple computers (often hundreds or thousands) simultaneously at a single target. Mitigation actions against a DDoS attack are more difficult to coordinate than against a DoS attack, and associated traffic is potentially more damaging to the target. DoS and DDoS attacks are common, albeit infrequently reported, cyber incidents.

Mitigation Guidelines for Denial-of-Service Attacks

DoS and DDoS attacks have become a common threat for many organizations. An overview of these attack types and related mitigation information, including a checklist of the recommended mitigation phases, can be found in CCIRC's Technical Report (TR12-001) *Mitigation Guidelines for Denial-of-Service Attacks.*

In late 2011, hacktivists infiltrated the network of a U.S.-based global intelligence company to steal personal information. In early 2012, the organization's client list, including emails, passwords, home and office addresses, and client credit card information were posted publically by these hacktivists. This information allegedly included approximately tens of

thousands of credit card numbers and upwards of a million login credentials. The organization notified all of its clients regarding this breach.

Throughout late 2011 and early 2012, CCIRC worked with its federal partners and the available data from law enforcement to identify and notify Canadian organizations which had been affected by this breach. The issue was mitigated by spring 2012, and this event highlights the growing capabilities of some hacktivist groups.

In mid-2012, open sources indicated that a hacktivist collective targeted the websites of the Province of Québec and Québec political parties in response to the passage of *An Act to enable students to receive instruction from the postsecondary institutions they attend* (Bill 78, 2012, c. 12, May 18, 2012) by Québec's National Assembly. This emergency Act, which was passed in response to the disruptions caused by student protests throughout the Province of Québec, was perceived as an arbitrary measure by several activist groups. During this incident, CCIRC coordinated cyber watch and warning efforts with the Province of Québec, and further collaborated with the province to provide mitigation advice to targeted and affected organizations.

The security company and the Québec government incidents detailed above demonstrated a use of hacktivism *in* cyberspace and *through* cyberspace, respectively. The first consists of pursuing ideological or political goals solely in cyberspace, while the second consists of a combination of hacktivism and traditional demonstrations. Throughout 2012, actions which have traditionally brought about protests, instead tended to trigger both activism and hacktivism.

Other noteworthy hacktivist actions in 2012 included coordinated DDoS attacks targeting the websites of critical infrastructure organizations and governments of all levels, and several alleged leaks of personal information affecting millions of individuals.

Additionally, international counterparts, including the U.S. DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), have reported that hacktivist groups have developed the capability to conduct cyber attacks against ICS, which if successful have the potential to impact the physical world, including human health and safety. [§]

Industrial Control Systems

Throughout 2012, CCIRC observed ongoing risks faced by the Canadian operators of ICS. There was an increase in the number of ICS incidents handled by CCIRC, and an ongoing discovery of known Internet accessible ICS components, which can be identified with specialized search engines.

ICS automate the monitoring and management of physical processes, such as the generation and transmission of electricity, wastewater treatment, discrete and continuous manufacturing, food production, as well as the air quality and temperature in many commercial and high rise

[§] See, for example: ICS-CERT. October 25, 2012. ICS-ALERT-12-046-01A-(Update) – Increasing Threat to Industrial Control Systems.

buildings. ICS can be confined within a single location such as a factory, or can be interconnected to control geographically dispersed assets across multiple jurisdictions, such as the flow of oil across the Canada – U.S. border. Supervisory control and data acquisition (SCADA) systems are an example of the latter.

One noteworthy incident in early 2012 consisted of a compromise at a Canadian ICS operator in the energy and utilities sector. The organization contacted CCIRC after it was made aware of the breach of its network by law enforcement. CCIRC provided mitigation advice and worked with the company in its recovery effort. Additionally, CCIRC sent an updated Cyber Flash (CF12-003) to its partners that contained time sensitive detection indicators and mitigation information. Several recipients of this Cyber Flash subsequently discovered and reported being affected by the same campaign to CCIRC, which then worked with them to mitigate their respective compromises.

In the latter half of 2012, CCIRC coordinated the Government of Canada's response to a cyber intrusion at a Canadian ICS manufacturing company, whose products are used in several critical infrastructure sectors throughout North America. Following a law enforcement notification, the affected organization promptly informed its clients, and CCIRC subsequently obtained network logs and other supporting information related to this compromise. Based on its analysis of this information, CCIRC provided further assistance to affected organizations in collaboration with the Government of Canada's cyber operations community.

Many ICS operators utilize Internet accessible devices throughout their ICS network to improve efficiency and realize cost savings. Connecting ICS to the Internet or corporate networks, either directly or through the transfer of data between these systems via removable media (e.g. a USB device), provides a vector through which a malicious actor can gain access to and subsequently disrupt the ICS.

Industrial Control Systems Security Best Practices

In recognition of the risks facing ICS, CCIRC posted Technical Report (TR12-002) *Industrial Control System (ICS) Cyber Security: Recommended Best Practices* to its website, which includes the following advice for ICS 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; and
- Require multi-factor authentication for remote access.

The SHINE Project

In the ongoing SHINE (SHodan Intelligence Extraction) Project, vulnerability researchers at a U.S.-based security company compiled a list of approximately 500,000 Internet accessible ICS devices globally as of the end of 2012, of which approximately 10,000 were found to be in Canada. The purpose of project SHINE is to raise the ICS operator community's awareness of the pervasive nature of this issue. The project uses SHODAN, a computer search engine that allows users to search for computing devices based on software, geography, operating system, IP address, as well as other criteria.

CCIRC collaborated with ICS-CERT on the mitigation of the vulnerabilities identified by the SHINE project. CCIRC has notified the Canadian owners of these ICS devices based on the project's data.

Looking Ahead

While not an exhaustive list, CCIRC recommends that partners and operators of vital cyber systems consider the following technological trends.

Data Mobility

A demand for quickly accessing data from anywhere has become prevalent in the public and private sectors, and this demand has spurred the emergence and rapid growth of cloud and mobile computing. While corporate data was traditionally held within an organization's physical and cyber security perimeter, data is now highly mobile via cloud infrastructure, mobile devices, and removable media.

Cloud Computing

Cloud computing is a transformative technology that has emerged to meet the demand for easily accessing data and applications from anywhere.

While the consolidation of corporate data in the cloud can result in better security overall, a breach of such a complex system and its aggregated data has the potential to have a much higher impact. Depending on how it is configured, cloud computing can represent not only an out-sourcing of applications and data storage, but also an outsourcing of security. For example, a cloud infrastructure that depends on numerous applications, such as web browsers, assumes the risks and vulnerabilities of these applications. As noted above in the Malware and Exploit Kits subsection, the automation of web exploits as a technique for spreading malware was prevalent throughout 2012 and into early 2013.

Autonomy and control over access to data in the cloud depends upon the legislative framework of the jurisdiction in which the physical cloud infrastructure is located, including the jurisdictions

which contain the communications cables transmitting this data. The risks to storing sensitive corporate or government data in other jurisdictions need to be carefully considered.

Mobile Computing

The demand for easy access to the data stored on corporate networks or in the cloud has resulted in an increase in the number of devices being connected to these networks. In particular, the increasing popularity of connecting personal computing devices to corporate networks (termed bring your own device, or BYOD) means that corporate data is being accessed remotely by devices neither owned nor protected by the organization. Similarly, employees assume additional personal risk by connecting their own device to the corporate network. A key takeaway is that smart phones, tablets and other mobile devices are computing devices which face the same risks as desktop and laptop computers, and as a result need to be secured as such.

Potential Risks in Networking Everyday Devices

Everyday devices, such as medical devices and corporate alarm systems, are increasingly being networked with each other and the Internet, thereby exposing them to the same risks which face all other networked computing devices. For example, personal medical devices, such as cardiac pacemakers which interface wirelessly with monitoring equipment, can be interfered with by a malicious actor who gained access to that device's wireless connection. Such unauthorized access can lead to an exfiltration of confidential patient information or even a disruption of the medical device, which may have an adverse effect on the patient's health.

Other everyday devices such as smart electricity and water utility meters, and home automation systems, are also at risk, and unauthorized access to these devices can potentially result in privacy infringements, or even the disruption of essential services. Partners and operators of vital cyber systems need to identify where these types of everyday devices are in their organization and, in turn, assess and mitigate the risk these devices pose to their business.

End of Support for Microsoft Windows XP Service Pack 3 and Office 2003

Microsoft Corporation will end its support for Windows XP Service Pack 3 (SP3) and Office 2003 effective April 8, 2014. Running Windows XP SP3 or Office 2003 after this date may expose your organization to security and compliance risks, as Microsoft will no longer provide automatic fixes, security updates, or online technical assistance for these products. Microsoft's support for Windows XP Professional for embedded systems, which are computer systems embedded within other electronic equipment and machines, will continue to the end of 2016.

Responding to Cyber Incidents

Since it was established in 2005, CCIRC has been responding to reports of cyber incidents from the operators of vital cyber systems, its international counterparts, and federal partners. In 2012, CCIRC received 182 reports from public and private sector partners directly affected by a cyber incident. The remaining 742 (approximately 80%) incidents handled by CCIRC in 2012 came as a result of CCIRC acting on available information such as malware feeds, notifications from domestic and international federal partners, and other actionable information.

Recognizing that cyber security is a shared responsibility and can be enhanced through information sharing, CCIRC encourages Canadian operators of vital cyber systems in the public and private sectors to report cyber incidents to CCIRC at CCIRC-CCRIC@ps-sp.gc.ca.

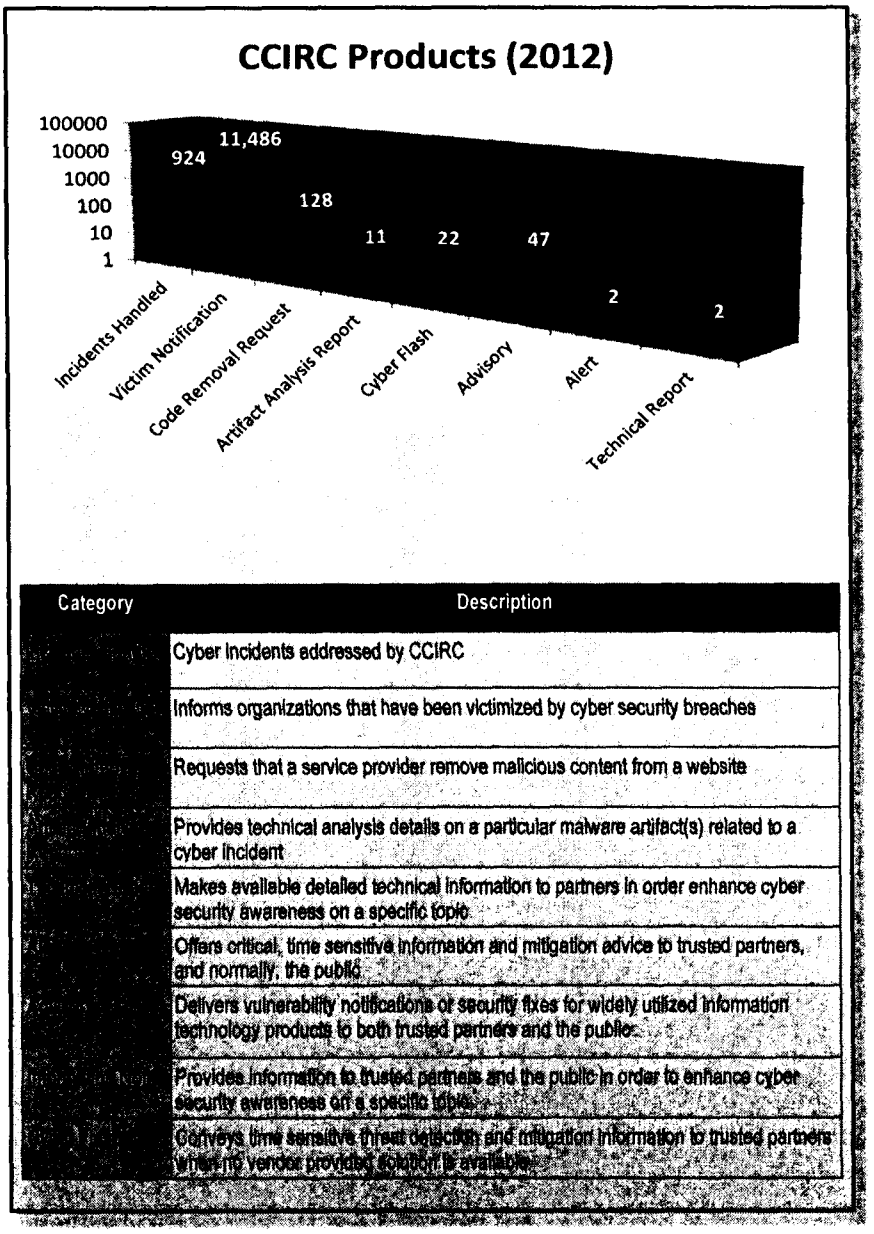
CCIRC Products and Services

Products

In 2012, CCIRC issued 47 Advisories, two Information Notes, two Technical Reports, two Alerts, 22 Cyber Flashes, and 11 artifact analysis reports. Publically available products can be found on the CCIRC website.

Advisories – CCIRC issued 47 Advisories to bring attention to significant upgrades and patches of commonly used computer products, such as those made by Microsoft, Adobe, and Oracle.

Alerts – CCIRC developed two Alerts related to Microsoft Internet Explorer security vulnerabilities.



Cyber flashes – CCIRC released 22 Cyber Flashes to its partners providing information and mitigation advice related to specific cyber incidents. These incidents included the APT spear phishing campaign targeting multiple critical infrastructure sectors detailed above; Shamoon/DistTrack malware targeting international companies in the energy and utilities sector; increased ZeroAccess botnet activity; and malware targeting point-of-sale systems.

Artifact Analysis Reports – CCIRC prepared 11 Artifact Analysis Reports (AAR) for partners. Launched in 2012, AARs are a CCIRC product that provides partners with timely and in-depth technical analysis during an incident affecting their systems and, in turn, mitigation advice for the associated cyber risks.

Technical Reports – CCIRC posted two Technical Reports to its website that provided background and mitigation information for denial-of-service attacks and ICS. Technical Reports provide an overview of prevalent cyber security risks and related mitigation advice which are not event or campaign specific, and as such are publicly available on CCIRC's website.

Information Notes – CCIRC disseminated two Information Notes (IN) which provided an overview of recent changes and upgrades in CCIRC's operational capacity, and its products and services.

In early 2013, CCIRC and US-CERT released a joint cyber awareness product (CCIRC IN13-001 and US-CERT Alert TA13-024A) to raise awareness of the fact that compromised web servers are increasingly being utilized by malicious actors to carry out cyber attacks, including DDoS attacks targeting critical infrastructure organizations. This joint Canada – U.S. cyber awareness product provides an assessment of the issue along with mitigation advice for website administrators.

In addition, CCIRC posted an Information Note (IN13-002) to its website regarding *Remaining Cyber Safe While Travelling: Security Recommendations* for partners in the private and public sectors. This Information Note includes a description of eight cyber security activities an organization should consider before, during, and after employee travel.

Contact Information

To be added to CCIRC's distribution list for any of the products detailed above, please contact CCIRC-CCRIC@ps-sp.gc.ca.

Services

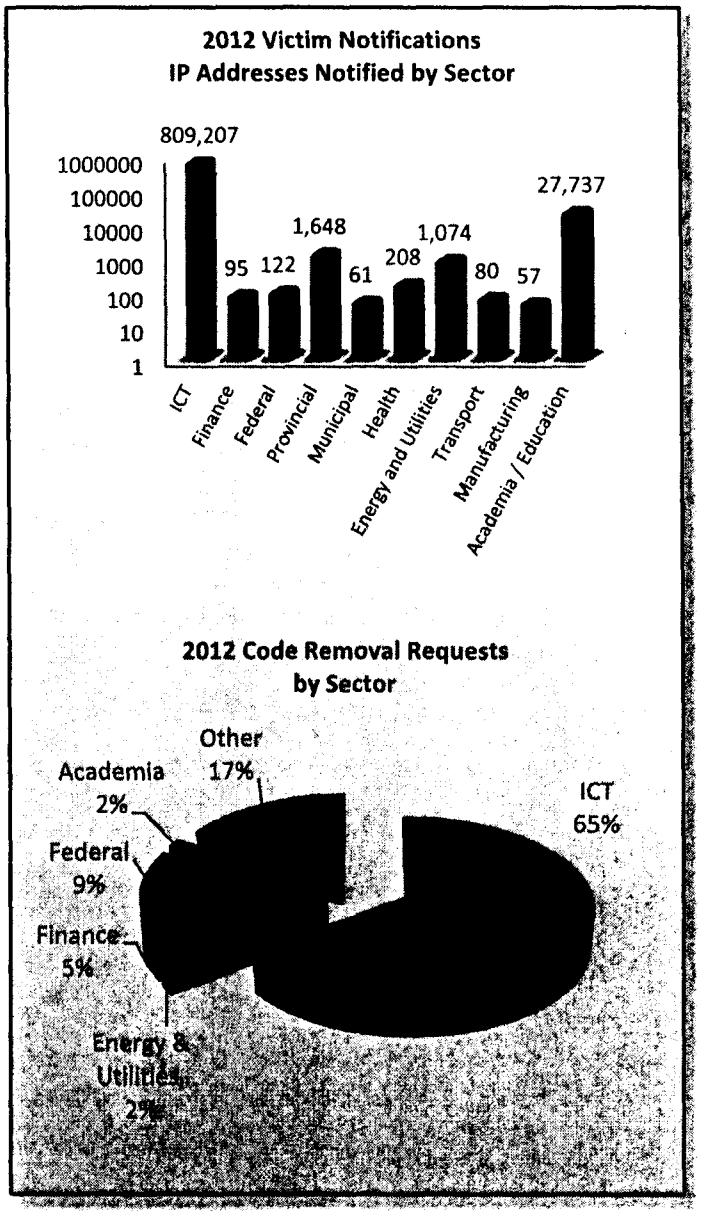
Victim notifications – In 2012, CCIRC sent out 11,486 victim notifications for 842,286 affected IP addresses. These notifications are a service CCIRC provides to organizations suspected to be affected by malware, and contain detection and mitigation advice.

The ICT and education sectors were the largest recipients of CCIRC's victim notifications in 2012, accounting for 99% of the affected computing devices. It should be noted that the high notification rate for ICT sector is likely due to the fact that most infections represent individual Canadians who are using an ICT organization as a service provider.

To deliver this service, CCIRC receives information about potentially infected computing devices from a number of trusted partners. This information is then compared with public and non-public lists to identify the victims and their associated business sectors.

The top three malware types for which CCIRC issued notifications in 2012 were Flashback, Conficker and Zeus (including its Citadel variant), each of which accounted for approximately one fifth of victim notifications.

Code removal requests – In 2012, CCIRC delivered 128 Code Removal Requests (CRR) to Internet service and hosting providers. A CRR is a CCIRC service that informs recipients that they are hosting malicious content, website forgeries, and/or personal information and requests that it be removed.



In the cases where it was not possible to determine the impacted sector in the graph above, the ICT sector was listed. This is because this sector includes the Internet service and hosting providers where malicious content, website forgeries, and personal information was held.

About the Canadian Cyber Incident Response Centre

Mandate

In support of Public Safety Canada's mission to build a safe and resilient Canada, the Canadian Cyber Incident Response Centre (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 security incident response 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.

Priorities and Progress Achieved in 2012

1. **Strengthened CCIRC's legal, policy and process foundations** – to ensure authority and management framework are in place to deliver on CCIRC's mandate.
    - Conducted a Privacy Impact Assessment that verified CCIRC's sensitive information handling procedures to be compliant with the *Privacy Act* (R.S.C., 1985);
    - Updated its mandate to provide greater clarity to partners;
    - Updated the majority of its Standard Operating Procedures; and
    - Developed and standardized incident reporting criteria and impact assessment guidelines.

2. **Deepened and expanded collaboration with internal and external partners** – to improve incident response across Canada, coordinate it when necessary, and ensure the Government of Canada and its partners have situational awareness of the cyber environment.
    - Developed new protocols and signed information sharing agreements to enhance information sharing with external partners and international counterparts;
    - Enhanced collaboration with partners, including DHS, the Royal Canadian Mounted Police's Critical Infrastructure Intelligence Team (CIIT), and the Government of Alberta's Alberta Security & Strategic Intelligence Support Team (ASSIST); and
    - Launched a secure CCIRC Community Portal for partners.

3. **Strengthened analytical capability** – to improve mitigation advice and incident response for partners.
    - Increased staffing to allow 15 hours per day, seven days per week operation as of November 5, 2012, thereby ensuring business hour coverage from coast to coast;
    - Acquired and integrated into its operations a world-class malware analysis laboratory from Industry Canada; and
    - Deployed two ICS test beds, which simulate a liquefied natural gas regasification facility and a coal-fired electric power generation facility, in order to enable malware analysis within an ICS environment.

Appendix

Annex A – Top 35 Recommended Mitigation Actions

The following is a list of recommended cyber threat mitigation strategies, listed in order of effectiveness and updated in October 2012, to which all organizations should adhere. Developed by the Australian Government's Defense Signals Directorate, this list has broad international agreement and is being widely distributed by CCIRC and Communications Security Establishment Canada.

Ranking	Mitigation Strategy
1	Undertake **application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs.
2	**Patch applications** such as Adobe PDF viewers and Flash Player, Microsoft Office and Java Runtime Environment. Patch or mitigate high risk vulnerabilities within two days.
3	**Patch operating system** vulnerabilities. Patch or mitigate high risk vulnerabilities within two days.
4	**Minimise the number of users with domain or local administrative privileges**. Such users should use a separate unprivileged account for email and web browsing.
5	**Disable local administrator accounts** to prevent network propagation using compromised credentials that are shared by several computers.
6	**Multi-factor authentication** especially implemented for remote access, when the user is about to perform a privileged action or access a sensitive information repository.
7	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication and user directory information.
8	**Application-based workstation firewall** configured to deny traffic by default, to protect against malicious or otherwise unauthorized **incoming** network traffic.
9	**Application-based workstation firewall** configured to deny traffic by default, that whitelists applications allowed to generate **outgoing** network traffic.
10	**Non-persistent virtualized trusted operating environment**, hosted within the internet gateway, for risky activities such as reading email and web browsing.
11	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking.
12	**Centralized and time-synchronized logging** of successful and failed **computer events**, with regular log analysis, storing logs for at least 18 months.
13	**Centralized and time-synchronized logging** of allowed and blocked **network activity**, with regular log analysis, storing logs for at least 18 months.
14	**Whitelisted email content filtering** allowing only business-related attachment types. Preferably convert/sanitize links, PDF and Microsoft Office attachments.
15	**Web content filtering** of incoming and outgoing traffic, using whitelisting, behavioural analysis, reputation ratings, heuristics and signatures.
16	**Web domain whitelisting for all domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.
17	**Web domain whitelisting for HTTPS/SSL domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.

Ranking	Mitigation Strategy
18	**Workstation application security configuration hardening** e.g. disable unrequired features in PDF viewers, Microsoft Office applications, and web browsers.
19	**Block spoofed emails** using Sender Policy Framework checking of incoming emails, and a 'hard fail' SPF record to help prevent spoofing of your organization's domain.
20	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid weak passphrases, passphrase re-use, exposing email addresses, and unapproved USB devices.
21	**Operating system exploit mitigation mechanisms** such as Data Execution Prevention and Address Space Layout Randomization.
22	**Computer configuration management** based on a hardened Standard Operating Environment with unrequired functionality disabled e.g. IPv6, autorun.
23	**Server application security configuration** hardening e.g. databases, web applications, customer relationship management and other data storage systems.
24	**Deny direct internet access** from workstations by using an IPv6-capable firewall to force traffic through a split DNS server, an email server or an authenticated web proxy.
25	**Antivirus software** with up-to-date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop antivirus software from different vendors.
26	**Workstation inspection of Microsoft Office files** for abnormalities e.g. using the Microsoft Office File Validation feature.
27	**Enforce a strong passphrase policy** covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words.
28	**Restrict access to Server Message Block (SMB) and NetBIOS services** running on workstations and on servers where possible.
29	**Removable and portable media control** as part of a data loss prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.
30	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.
31	**Disable LanMan password support and cached credentials** on workstations and servers, to make it harder for adversaries to crack password hashes.
32	**Block attempts to access web sites by their IP address** instead of by their domain name.
33	**Network-based Intrusion Detection/Prevention System** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
34	**Gateway blacklisting** to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.
35	**Selected network traffic capture** to perform post-incident analysis of successful intrusions, storing network traffic for at least the previous seven days.

Annex B – Vulnerability Mitigation

The prevalence of exploit kits that automate the installation of malware observed by CCIRC can be mitigated, in large part, by patching known vulnerabilities. The chart below lists the top vulnerabilities CCIRC observed being used for system exploitation in 2012. CCIRC recommends partners and operators of vital cyber systems focus on patching these 13 vulnerabilities.

Vendor	Vulnerability Reference	CCIRC Product
Microsoft	CVE-2009-3129	AV09-045
Microsoft	CVE-2010-3333	AV10-050
Microsoft	CVE-2012-0158	AV12-016
Microsoft	CVE-2012-4792	AV13-001
Microsoft	CVE-2012-4969	AV12-038
Adobe	CVE-2010-0188	AV10-007
Oracle	CVE-2011-3521	AV11-046
Oracle	CVE-2012-0507	AV12-007
Oracle	CVE-2012-1723	AV12-029
Oracle	CVE-2012-4681	AV12-037
Oracle	CVE-2013-0422	AV13-004
Oracle	CVE-2012-5076	CF12-018
OpenX	CVE-2012-4990	CF12-019

Annex C – Glossary

Term	Definition
Advanced persistent threat (APT)	Adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors. The APT actor pursues its objectives repeatedly over an extended period of time, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives.
Botnet	A botnet is a collection of compromised computers that can be used for malicious purposes such as sending spam or malware, or flooding a network with DoS attacks.
Crimeware	Malicious software that is covertly installed on computers and has the ability to 'steal' confidential information and send it back to cyber criminals. One form of crimeware is ransomware, which is software that denies access to a user's computer until they pay a ransom.
Cyber attack	The unintentional or unauthorized access to, use, manipulation, interruption or destruction, via electronic means, of electronic information or the electronic devices or computer systems and networks used to process, transmit or store information.
Cyber security	The body of technologies, processes, practices, and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or unwillingly participating in the DoS.
Event	An observable change to the normal behavior of a computer, IT system, environment, process, or workflow that may impact or may pose a threat to the system or data integrity, or safety and security. An event can be "upgraded" and become an incident if it becomes apparent that the change observed has a probable negative impact and requires mitigation or advice.
Hacktivism	Some groups of computer hackers are not motivated by financial gain and instead are driven by economic, political, or religious interests that generally go beyond their nation's borders. Their actions are called hacktivism, which is a merger of hacker and political activism. Hacktivists infiltrate networks and put their talents to work for their beliefs by organizing computer attacks, including piracy, hijacking servers, and replacing homepages with ideological messages.
Improper usage	Any activity that violates acceptable computing use policies.
Incident	An incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising the business operations and threatening the information security of system(s) of national significance within the Canadian public and private sectors.
Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.
Malicious code	*Successful* installation of malicious software (e.g. virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.

Term	Definition
Phishing / targeted emails	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. Criminally-fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
Scans/ probes/ attempted access	This incident category includes any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
Spear phishing	A category of phishing that consists of targeting specific individuals.
Unauthorized access	In this category of incident an individual gains logical or physical access without permission to a network, system, application, data, or other resource.

Annex D – Common Malware

This section summarizes the stages of a malware infection and provides an overview of the malware referenced in the *2012 Cyber Operational Report.*

It is recommended that partners and operators of vital cyber systems refer to CCIRC's Technical Report (TR11-001) *Malware Infection Recovery Guide.* Prepared by members of the London Action Plan, which includes the Government of Canada (Industry Canada), the Best Practices to Address Online and Mobile Threats also contains malware mitigation advice.

Malware Infection Stages

1. **Lure**. The potential victim is lured to click on a malicious link in a phishing email or on a website, which redirects them to exploit code.
2. **Exploitation**. A web browser, system, or application vulnerability is exploited to install malware onto the computing device.
3. **Call back.** The malware establishes contact with its owner and may, as a result, execute additional malicious code.
4. **Information theft or manipulation**. The malware's owner carries out the intended malicious action, such as stealing data or adding the infected computing device to a malicious network, or botnet.

Select Malware Types

Conficker

Type: Worm

Description: Conficker is a worm that targets the Microsoft Windows operating systems. It uses flaws in Windows software to spread itself. Computers infected with Conficker become part of a botnet and could be used for various malicious purposes such as DDoS attacks.

Additional information is available in CCIRC's Alert (AL09-003) *Conficker Worm.*

Domain Name System (DNS) Changer

Type: Trojan Horse

Description: DNS Changer causes a computer to use rogue DNS servers instead of a legitimate one which is generally provided by the ISP. This malware changes a computer's DNS server settings and attempts to access networking devices on the victim's small-office or home (SOHO) network that run a DHCP server (e.g. a "router" or "home gateway") using common default user names and passwords. If successful, the malware changes the associated DNS configuration. The latter technique may impact all computers on the home/small-office network even if they are not directly infected.

Additional information is available in CCIRC's Information Note (IN11-002) *DNS Changer Infrastructure and TDSS/ Alureon/ TidServ/ TDL4 Malware.*

Flame/sKyWIper

Type: Worm

Description: An advanced computer worm, Flame/sKyWIper can be used for data exfiltration, contains features allowing it to spread throughout the network, and propagates through removable media, malicious links, and email attachments. In addition, this malware has the capability to intercept network traffic, take screenshots and record audio, keystrokes and perform other monitoring activities.

Flashback

Type: Trojan Horse

Description: Flashback is a form of malware specifically targeting Apple's Mac computers. It is designed to grab passwords and other information from users through their Web browser and other applications and send this information back to a remote server. Flashback spreads by pretending to be an installer for Adobe's Flash plugin.

Gauss

Type: Worm

Description: Gauss is an information-theft toolkit that can intercept financial transactions, email, and social networking activity. Gauss shares some commonalities with Flame/sKyWIper.

Sality

Type: Polymorphic Virus

Description: Sality is a full featured virus that infects Windows executable files and exfiltrates data, delivers payloads, and uses the internet to send spam emails and download further malware. Sality is mainly distributed by infected files being transmitted by shared networks, shared drives, and physical media. As a polymorphic virus, Sality also has characteristics of a worm, a Trojan horse, and a rootkit.

Shamoon/DistTrack

Type: Information Theft Trojan horse

Description: Shamoon steals information and then renders infected systems unusable by overwriting the Master Boot Record (MBR), the partition tables, and most of the files on an infected system with random data. Once overwritten, the data is not recoverable.

ZeroAccess

Type: Rootkit

Description: ZeroAccess is a rootkit that has infected millions of machines worldwide and is continues to be used for various fraudulent moneymaking activities for its authors. It functions by concealing its presence on a computing device and adding it to a botnet. The primary distribution mechanisms of ZeroAccess include exploit kits such as Blackhole, drive-by downloads from seeded websites, malicious advertising (malvertising), and phishing emails.

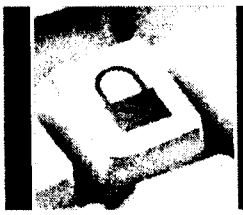
Zeus

Type: Information Theft Trojan Horse

Description: Zeus is a Trojan horse program created from the Zeus toolkit. The toolkit allows for the creation of the Zeus Trojan executable and the administration of a Zeus botnet. The Zeus Trojan primarily steals banking information but can also be used for other types of data. Zeus targets Microsoft Windows computing devices and is mainly distributed by exploit kits, phishing emails, drive-by downloads from seeded websites, and physical media such as USB memory sticks. Once a system is infected with the Zeus Trojan, it may participate in a botnet that is controlled by the owner.

Different variants of Zeus include: Zeus v1, Zeus v2, GameOver and Citadel, the latter of which includes additional features such as video capture.

Public Safety Canada | Sécurité publique Canada



CCIRC
Canadian Cyber Incident Response Centre

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

Partnering to Secure Vital Cyber Systems

Quarterly Operational Summary – January to March 2013

Public Safety Canada

This document provides a quarterly summary of the cyber incidents observed by the Canadian Cyber Incident Response Centre (CCIRC).

REPORTING CYBER INCIDENTS

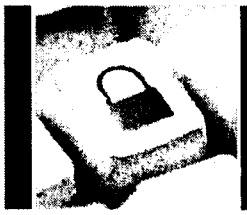
Private or public sector partners wishing to report incidents may send an email to cyber-incident@ps-sp.gc.ca using CCIRC's Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

FEEDBACK

Your feedback is appreciated and critical to making this product useful for you. Please email any feedback you have to the Operational Analysis and Support Section at CCIRC-CCRIC@ps-sp.gc.ca.

Canada

TABLE OF CONTENTS



CCIRC
Canadian Cyber Incident Response Centre

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

PURPOSE

This product discusses cyber incidents the Canadian Cyber Incident Response Centre (CCIRC) observed during the January to March 2013 reporting period. Its intent is to convey information to partners in the Canadian public and private sectors about products and services CCIRC provided, noteworthy incidents, and trends.

EXECUTIVE SUMMARY

What CCIRC Observed

- **Incidents** – 399 incidents, of which 80% involved malware and phishing attacks.
- **Malware analysis initiative** – ZeroAccess, Ransomware, Zeus, FakeAV, and Adware were the top five malware families connecting to Internet Protocol (IP) addresses in Canada.

What CCIRC Did

- **Recommended vulnerability mitigation** – The malware families listed above are mainly spread through exploited web vulnerabilities. This report includes a summary of mitigation information for the most common exploits CCIRC observed this quarter.
- **Victim notifications** – 2,536 victim notifications for 43,679 affected computing devices. The information and communication technology (ICT) sector and academic organizations were the largest recipients of these notifications.
- **Code removal requests** (CRR) – 73 CRRs sent to organizations that were hosting malicious content, website forgeries, or personal information. The ICT and finance sectors were the most affected by cyber incidents that led to CRRs.
- **Products** – two artifact analysis reports, one technical report, one alert, 15 advisories, two information notes, and five cyber flashes.

Trending Analysis

- **Increase in malicious code and phishing incidents** – Based on CCIRC's observations, the finance, energy and utilities, ICT, and government partner sectors were affected by this increase.
- **Web exploits and botnets** – The use of web exploits to spread malware and the popularity of botnets such as ZeroAccess were two key trends observed by CCIRC.

PRODUCTS

CCIRC issued two artifact analysis reports, one technical report, one alert, 15 advisories, two information notes, and five cyber flashes over this reporting period. Publicly available products can be found on the CCIRC website.

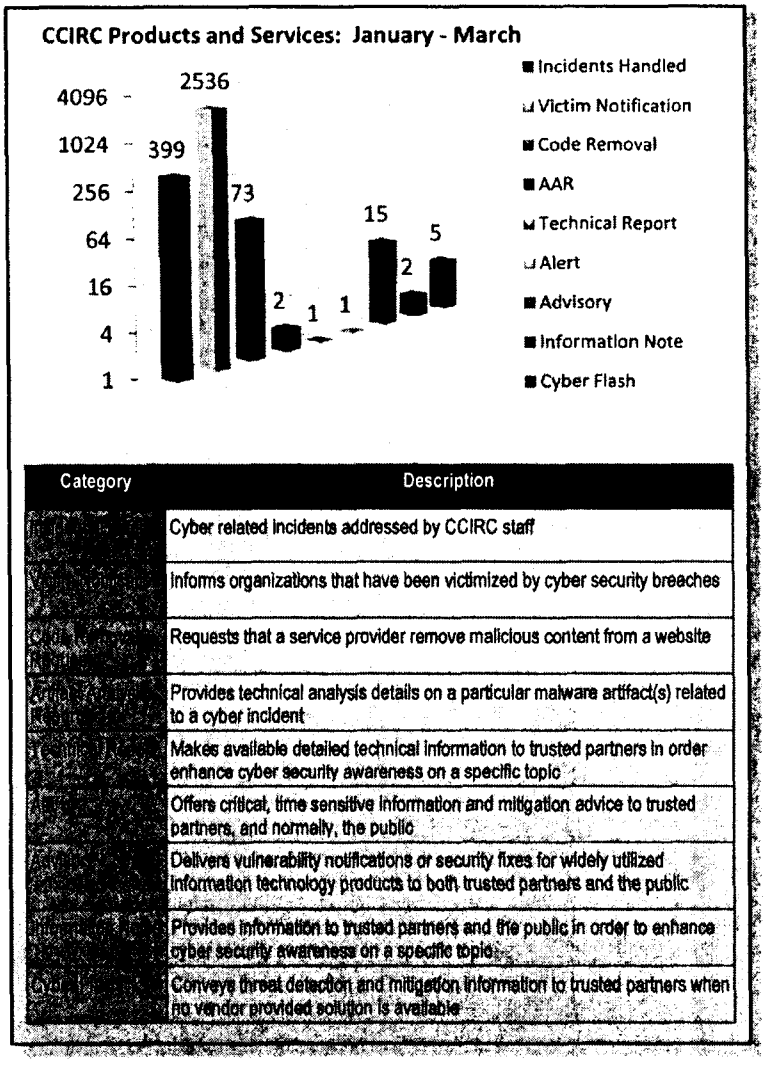
Artifact analysis reports (AAR) – CCIRC prepared two AARs for partners related to DNS Changer malware and advanced persistent threats. These reports contained artifact information, file analysis, mitigation advice, and indicators of compromise.

Technical report – CCIRC produced one technical report that provided an overview of Microsoft's Enhanced Mitigation Experience Toolkit. This toolkit helps prevent exploitation attempts targeting the Windows' systems.

Alert – CCIRC released one alert related to an Oracle Java zero-day vulnerability that allowed a remote attacker to run arbitrary code.

Advisories – CCIRC issued 15 advisories to bring attention to significant upgrades and patches of common computer products, such as those produced by Microsoft, Oracle, and Adobe.

Information note – CCIRC prepared two information notes to raise awareness of important cyber security practices related to content management systems and to provide travellers with information regarding the cyber based threats they face.



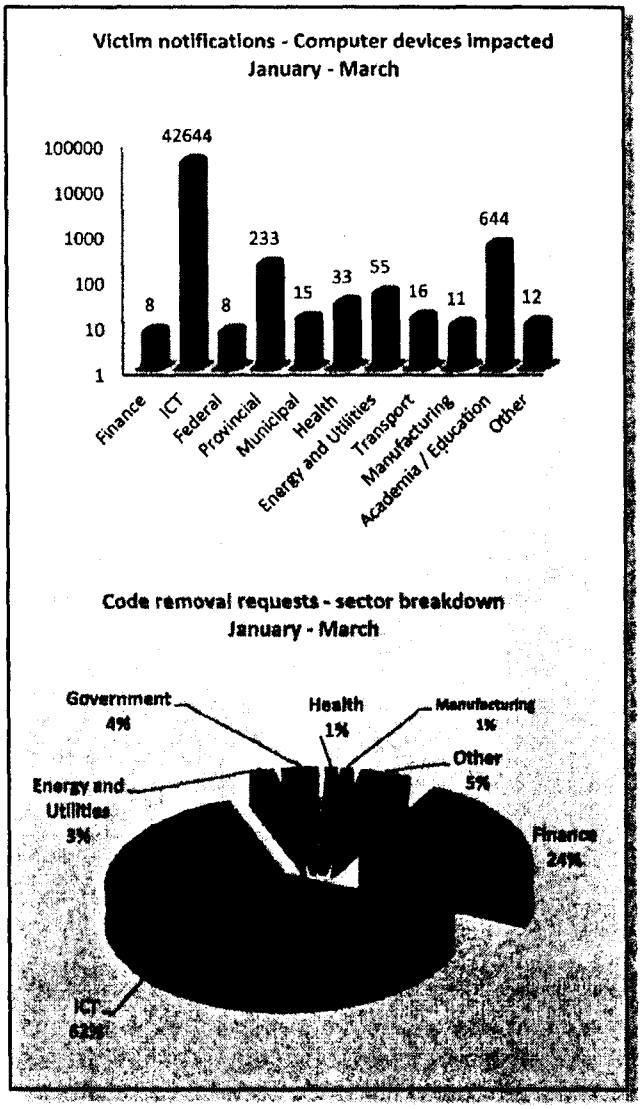
Category	Description
[illegible]	Cyber related incidents addressed by CCIRC staff
[illegible]	Informs organizations that have been victimized by cyber security breaches
[illegible]	Requests that a service provider remove malicious content from a website
[illegible]	Provides technical analysis details on a particular malware artifact(s) related to a cyber incident
[illegible]	Makes available detailed technical information to trusted partners in order enhance cyber security awareness on a specific topic
[illegible]	Offers critical, time sensitive information and mitigation advice to trusted partners, and normally, the public
[illegible]	Delivers vulnerability notifications or security fixes for widely utilized information technology products to both trusted partners and the public
[illegible]	Provides information to trusted partners and the public in order to enhance cyber security awareness on a specific topic
[illegible]	Conveys threat detection and mitigation information to trusted partners when no vendor provided solution is available

Cyber flashes (CF) – CCIRC released five CFs providing time sensitive information and mitigation advice related to: Oracle Java, Adobe Flash and Adobe Reader exploits and vulnerabilities, malicious activity against government and private sector entities, and major entertainment website compromises.

If you would like to be added to CCIRC's distribution list please contact CCIRC-CCRIC@ps-sp.gc.ca.

SERVICES

Victim notifications – CCIRC sent 2,536 victim notifications for 43,679 affected computing devices during this reporting period. These notifications are a service CCIRC provides to organizations affected by malware and contain detection and mitigation advice. This advice is specific to the type of malware affecting the organization. The ICT sector was the largest recipient of CCIRC's victim notifications this quarter, accounting for 42,644 computing devices.



To support this service, CCIRC receives information about potentially infected computing devices from a number of trusted partners. This information is then compared with public and non-public lists to identify the victims and their associated business sectors.

> *Comment: The high notification rate for the ICT sector is likely due to the fact that most infections represent individual Canadians who are using an ICT company as a service provider. Based on available data, actionable information, and malware traps (DNS sinkholes) Zeus, Conficker, and Flashback were the main types of malware CCIRC witnessed affecting its public and private sector partners this quarter – accounting for 78% of CCIRC's victim notifications.*

Code removal requests (CRR) – CCIRC delivered 73 CRRs to Internet service and hosting providers. A CRR is a CCIRC service that informs recipients that they are hosting malicious content, website forgeries, or personal information and requests that it be removed.

In some cases it was possible to determine the impacted sector as shown in the graph. For the incidents where CCIRC was unable to determine the impacted sector, the ICT sector was listed as this sector includes the Internet service and hosting providers where malicious content, website forgeries, and personal information was held.

CCIRC
Canadian Cyber Incident Response Centre

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

NOTEWORTHY INCIDENTS

Oracle Java zero-day vulnerability – CCIRC became aware of an Oracle Java vulnerability that allowed attackers to compromise users that visited specially crafted webpages. This vulnerability was incorporated into commonly used exploit kits as a means of automating the spread of malware. CCIRC issued a cyber flash **(CF13-001)** containing contextual information, pre-infection indicators, and mitigation advice and an alert to inform partners of the problem. CCIRC subsequently released an advisory informing its partners that Oracle had released a critical update to fix this vulnerability.

Adobe Flash Player exploit targeting critical infrastructure – CCIRC observed a spear phishing email campaign that was targeting critical infrastructure organizations. This campaign used an aerospace conference and a generic human resource theme to entice recipients to open a Microsoft Word attachment containing malicious Flash content. CCIRC issued a cyber flash **(CF13-002)** containing contextual information, indicators of compromise, and mitigation advice. CCIRC subsequently released an advisory informing its partners that Adobe had released a security bulletin to address this exploit.

Malicious activity against government and private sector entities – During this reporting period, cyber actors engaged in malicious activity against government and private sector entities. The apparent objective of this activity was the theft of intellectual property, trade secrets, and other sensitive business information. CCIRC issued a cyber flash **(CF13-003)** containing contextual information, indicator descriptions, and mitigation advice.

TOP FIVE MITIGATION ACTIONS

Implementing the following recommended actions will help prevent the majority of reported cyber incidents. CCIRC strongly recommends that all organizations use them.

1. **Undertake application whitelisting of permitted/ trusted programs to help prevent malicious or unapproved programs from running.**
2. **Patch application vulnerabilities as soon as possible (e.g. PDF viewer, Flash Player, Microsoft Office and Java). Use the latest version of applications.**
3. **Patch operating system vulnerabilities as soon as possible. Use the latest operating system version.**
4. **Minimise the number of users with administrative privileges. Users should use a separate non-administrative account for email and web browsing.**
5. **Disable local administrator accounts to prevent network propagation using compromised credentials that are shared by several computers.**

See Annex C for a complete list of 35 mitigation actions for which there is broad international consensus.

Adobe Reader zero-day vulnerabilities – CCIRC became aware of critical vulnerabilities in Adobe Reader affecting Windows, Apple, and Linux systems. These vulnerabilities allowed an attacker to seize control of an affected system. This vulnerability was actively exploited by a targeted spear phishing campaign that attempted to trick victims into opening a malicious PDF file. CCIRC issued a cyber flash **(CF13-004)** containing contextual information, indicators of compromise, and mitigation advice and also released an advisory informing its partners that Adobe had released a security update to address this vulnerability.

Distributed denial-of-service attacks (DDoS) targeting United States (U.S.) financial institutions – Since September 2012, CCIRC has been aware of DDoS attacks against financial institutions in the United States. These attacks aim to disrupt the availability of computing resources from legitimate users and the source of these attacks appear to be compromised servers that are scattered around the world, and are controlled by the attacker(s). CCIRC is aware of approximately 500 IP addresses and servers that are located in Canada and connected to these attacks.

CCIRC continues to collaborate closely with Canadian financial institutions' security teams and has sent victim notifications to Canadian operators of these affected servers. CCIRC, in collaboration with its U.S. counterpart, developed a public awareness product to reach out to server operators who have configured their servers in such a way that they may be compromised. CCIRC also encouraged its public and private sector partners to consult its mitigation guidelines for denial-of-service attacks.

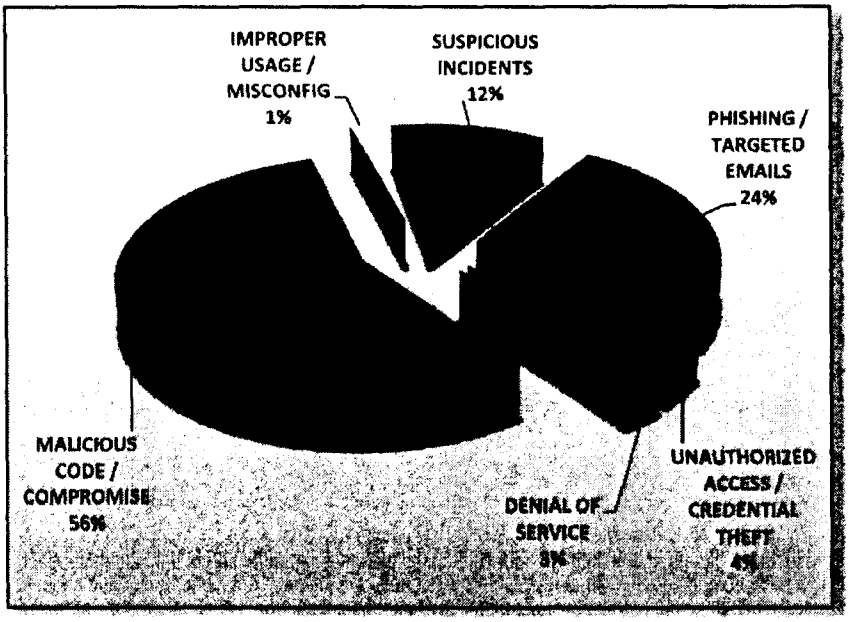
Major entertainment websites redirecting users to malware – CCIRC observed that several popular U.S. entertainment websites were compromised with malicious code that redirected website visitors to the RedKit exploit kit. This kit then attempted to exploit a vulnerability on visitors' browsers to install various forms of malware. CCIRC observed that Citadel, a variant of the Zeus Trojan horse, was one of the most commonly used malwares. Citadel uses key logging and screen captures to steal victims' data, such as banking credentials, and has reportedly been used for data exfiltration from critical infrastructure organizations in the past. CCIRC issued a cyber flash **(CF13-005)** containing contextual information, time sensitive indicators of compromise, and mitigation advice.

TREND ANALYSIS

Canadian public and private sector partners with the greatest take-up of CCIRC's products and services have been the financial, ICT, energy and utilities, and government sectors. These enhanced partnerships have provided CCIRC with sector specific data, and therefore, these sectors are the initial focus of analysis. Going forward, this summary will add other sectors as partnerships mature. Definitions of incident categories are provided in Annex B.

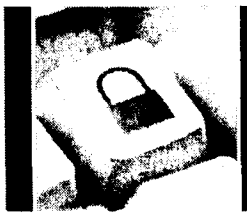
There are two important caveats regarding the statistics used in this analysis. First, certain incidents can affect organizations in multiple sectors. To represent this as accurately as possible, these incidents are accounted for in each affected sector rather than in only one. Second, as certain incidents may fall into more than one category, the number of incidents reported may be different than the total of each category and some of the statistics in this report may reflect this discrepancy.

INCIDENTS HANDLED



CCIRC handled 399 incidents during this reporting period, a 40% increase from the previous quarter. Malware attacks (e.g. viruses, key loggers, and Trojan horses) and phishing attacks (i.e. attempts to acquire personal or sensitive information by impersonating a trustworthy source) were the most common cyber threats observed by CCIRC – totalling 80% of the incidents handled.

Unauthorized access / credential theft, denial of service, improper usage / misconfiguration, and suspicious incidents totalled the other 20% of observed incidents.



Canadian Cyber Incident Response Centre

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

TRENDS OBSERVED BY CCIRC

Oct-Dec	285	40%	↑	8	88%	↑	12	-8%	↓	178	25%	↑	12	-50%	↓	2	F	31	52%	↑	42	131%	↑
Jan-Mar	399			15			11			223			6			0		47			97		
Oct-Dec	93	53%	↑	1	700% [E]	↑	4	25%	↑	65	28%	↑	9	-44%	↓	1	F	4	500%	↑	9	89%	↑
Jan-Mar	142			8			5			83			5			0		24			17		
Oct-Dec	98	56%	↑	1	500% [E]	↑	3	F		76	42%	↑	6	-83%	↓	0	F	5	80%	↑	7	271%	↑
Jan-Mar	153			6			3			108			1			0		9			26		
Oct-Dec	33	112%	↑	0	F		1	F		19	195%	↑	1	F		0	F	3	100%	↑	9	-44%	↓
Jan-Mar	70			3			0			56			0			0		6			5		
Oct-Dec	35	180%	↑	0	F		3	33% [E]	↓	15	227%	↑	0	F		0	F	3	167%	↑	14	157%	↑
Jan-Mar	98			3			2			49			0			0		8			36		

**Some incidents may impact multiple categories and sectors, and therefore be counted more than once. As such, the total incidents in the above chart may be higher than actual totals. For example, CCIRC dealt with 223 malicious code incidents this quarter but when accounting for multiple sectors affected by the same incident the sum total is higher than 223.*

*** E = Use with caution*

****F = Zero / too unreliable*

↑ ***Malicious code incidents*** – This quarter CCIRC observed that its partner sectors were affected by increased malware incidents. The ICT and government sectors were the largest targets of malware attacks, accounting for 191 observed incidents – a 42% and 28 % respective increase from last quarter.

Comment: A noteworthy portion of this rise can be attributed to exploit kits, botnets such as ZeroAccess, and software vulnerabilities. CCIRC has witnessed an increasingly widespread use of exploit kits, which automatically scan for and exploit known vulnerabilities in order to introduce malware. CCIRC also observed vulnerabilities targeting commonly used applications from vendors such as Microsoft, Adobe, and Oracle. Many of these new vulnerabilities were rapidly integrated into existing exploit kits. Page 12 has a list of the top vulnerabilities CCIRC has observed being used for system exploitation over the last quarter. CCIRC recommends its public and private sector partners both focus on patching these vulnerabilities and consulting CCIRC's Malware Infection Recovery Guide.

⬆ ***Investigation*** – This quarter, CCIRC investigated 47 suspicious incidents – a 52% increase from last quarter.

Comment: The increase in investigation of suspicious incidents this quarter can largely be attributed to efforts taken to enhance CCIRC's capacity and capabilities. Automated administrative processes have allowed CCIRC to reallocate more time to cyber incident investigation.

⬆ ***Phishing*** – This quarter, CCIRC processed 97 phishing incidents – a 131% increase from last quarter.

Comment: The increase in phishing incidents this quarter can be largely attributed to CCIRC's recent addition of new information sources, partners sending more phishing samples to CCIRC, and the expansion of CCIRC's client distribution list. Another reason for the observed increase can be attributed to the fact that this quarter covered Canada's tax season and CCIRC normally sees an increase in financial phishing during this period.

⬆ ***Unauthorized Access*** – This quarter CCIRC observed that its partner sectors were affected by increased unauthorized access incidents. The ICT and government sectors were the largest targets of unauthorized access attempts, accounting for 14 observed cases – an increase from last quarter.

Comment: The increase in unauthorized access incidents this quarter can be largely attributed to a surge in notable website defacements. CCIRC is more actively following on-line defacement archives in order to better notify affected public and private sector partners.

INCIDENT REPORTS RECEIVED

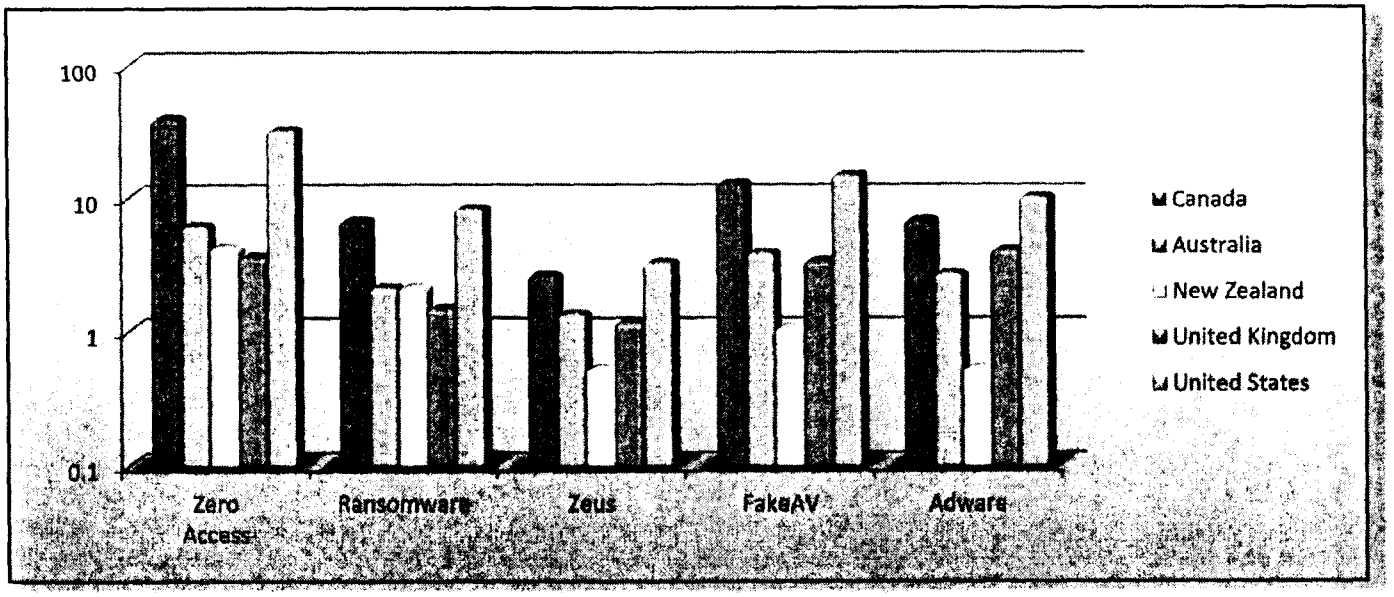
CCIRC received 32 cyber incident reports from public and private sector partners directly affected by a cyber incident, which represents a 22% decrease from the last reporting period. As cyber security is a shared responsibility and can be enhanced through information sharing, CCIRC encourages Canadian operators of vital cyber systems, which includes the critical infrastructure community, to report cyber incidents to CCIRC at CCIRC-CCRIC@ps-sp.gc.ca. Going forward, CCIRC will be focused on enhancing its number of trusted partnerships.

MALWARE ANALYSIS INITIATIVE

This quarter, CCIRC received 10,318,823 malware samples and studied 1,735,665 of them within its isolated analysis facilities. Of these, 330,364 malware samples were found to be attempting to connect to various Internet hosts.

The top five malware families connecting to Internet Protocol (IP) addresses in Canada were ZeroAccess, Ransomware, Zeus, FakeAV, and Adware. Together, these malware families accounted for nearly half of the IP addresses used by malware within the Five Eyes (Australia, Canada, New Zealand, United Kingdom, United States). This data showed that on a per capita basis, a greater proportion of IP addresses participating in malware infrastructure were in Canada and the U.S. It also showed that Canada seems to be more affected by ZeroAccess malware.

TOP FIVE MALWARE AFFECTING IP ADDRESSES (PER MILLION INTERNET USERS)



Methodology

- CCIRC receives samples from various sources, some of which are aggregating other sources. All data is anonymized and mechanisms being used to perform the sampling are often considered trade secret. Assessing whether malware is being proportionally captured across the globe is a challenge and the data behind this graph should be interpreted with care.
- This quarter CCIRC improved its processes to asses which malware threats are prevalent within Canada.
- This is still a trial process and all data should be treated as such.

ZeroAccess – *Trojan horse rootkit*: ZeroAccess' main goal is to assume full control of an infected machine, add this machine to a ZeroAccess botnet, and then use this botnet for various fraudulent moneymaking activities. ZeroAccess is mainly distributed by exploit kits such as Blackhole, drive-by downloads from seeded websites, malicious advertising, and phishing emails. Additional information and mitigation advice can be found in CCIRC's ZeroAccess Botnet Activity Cyber Flash (**CF12-016**).

Ransomware – Ransomware is a type of malware that prevents a user from accessing their computer or data. This malware then attempts to extort money (i.e. the ransom) from the impacted user in exchange for regaining access.

Zeus – *Trojan horse password stealer*: Zeus is a Trojan program that primarily steals banking information. Once a machine is infected, Zeus monitors Internet activity and uploads stolen data to a command and control server. Zeus targets Microsoft Windows and is mainly distributed by exploit kits, phishing emails, drive-by downloads, and physical media such as USB memory sticks.

FakeAV – *Trojan*: FakeAV is a type of malware that attempts to convince users to purchase false antivirus software in order to remove intentionally misrepresented malware or security risks from a computer.

Adware – Adware is a form of, sometimes legitimate, software that displays advertisements on a user's computer. When the software is unwillingly installed, it is considered a nuisance / malicious.

RECOMMENDED VULNERABILITY MITIGATION

Below is a list of the top vulnerabilities CCIRC observed being used for system exploitation over the last quarter. CCIRC recommends owners and operators of cyber systems focus on patching these:

Vendor	Vulnerability Reference	CCIRC Product
Microsoft	CVE-2013-1288	AV13-014
Microsoft	CVE-2012-1889	AV12-028
Microsoft	CVE-2012-0158	AV12-016
Microsoft	CVE-2012-4792	AV13-001 Update
Microsoft	CVE-2012-4969	AV12-038
Oracle	CVE-2012-5076	AV12-042
Oracle	CVE-2012-4681	AV12-037
Oracle	CVE-2012-1723	AV12-029
Oracle	CVE-2013-0422	AV13-004 AL13-001
Oracle	CVE-2013-1493	AV13-013
Oracle	CVE-2013-0431	AV13-011
Adobe	CVE-2013-0634	AV13-007
Adobe	CVE-2013-0640	AV13-010
Adobe	CVE-2013-0641	AV13-010
Adobe	CVE-2010-0188	AV10-007

***Also, please see Annex C for a complete list of 35 mitigation actions for which there is broad international consensus.**

Conficker – *Worm*: Conficker is a worm that targets Microsoft Windows. Computers infected with Conficker become part of a botnet and could be used for various malicious purposes such as DDoS attacks. Conficker mainly spreads itself by using flaws in Microsoft Windows' software.

Flashback – *Trojan horse virus*: Flashback is a form of malware that specifically targeted Apple's Mac computers. It was designed to monitor online searching and browsing behaviour and send this information back to a remote server. Flashback mainly spread by drive-by downloads utilizing a Java vulnerability. At this time, the Java vulnerability has been fixed. However, a few users who have not updated their operating systems still remain vulnerable to Flashback.

PUBLISHED THREAT REPORTS

CCIRC encourages its partners to stay updated on the latest in cyber security. This section provides a brief outline of a few open source reports published during the first quarter of 2013.

Websense 2013 Threat Report – Websense reports that numerous cyber threats have bypassed traditional controls, and that the insider threat is a 'rising blind spot for security solutions'.

F-Secure Threat Report H2 2012 – F-Secure states that botnets, web exploits, and banking Trojans were the three most prevalent security trends observed in the last half of 2012.

FireEye Advanced Threat Report: 2H 2012 – FireEye reports that spear phishing was widely used for initiating advanced attacks in the last half of 2012.

McAfee 2013 Threats Predictions – McAfee predicts that malicious actors will continue to refine crimeware, that the use of ransomware "kits" will continue to increase, and that hacktivist groups' effectiveness will continue to decline.

Kaspersky's Top Threats for 2013 – Kaspersky forecasts that major cyber threats in 2013 will include cyber espionage, hacktivism, and nation-state sponsored cyber attacks.

Mandiant Intelligence Center Report – Mandiant allegedly exposed a state-sponsored espionage group they describe as "one of the most persistent of China's cyber threat actors." It is reported that this group stole hundreds of terabytes of data.

Trend Micro Global Botnet Map – Trend Micro offers a real-time map that identifies the location of botnet command and control servers, as well as the computers that they control. This information aims to help increase protection against botnet attacks.

Sophos - Malware B-Z: Inside the Threat from Blackhole to ZeroAccess – Sophos observed widespread increased use of automated exploit kits in 2012. This report provides an overview of the prevalent ZeroAccess family of rootkits and one of the most common malware delivery mechanisms, the Blackhole exploit kit.

Symantec - The World of Financial Trojans – Symantec suggests that many financial institutions are ineffectively addressing the risks posed by the modern banking Trojan. This report examines eight of the most popular financial Trojans that have recently targeted institutions across the globe.

- It is important to note that as these links are provided for your convenience, the Government of Canada is not responsible for the accuracy, currency or the reliability of the content nor does it endorse the links.

ANNEX A – ABOUT CCIRC

Mandate

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

As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention 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.

Core functions

To deliver on its mandate, CCIRC:

- Builds and maintains trusted relationships and information sharing mechanisms with partners and clients;
- Disseminates a variety of cyber information products based on data from domestic and international partners and sources;
- Conducts daily cyber operations such as code removal requests related to malicious sites, the notification of compromised systems, and the repatriation of stolen data; and
- Maintains the protocols and mechanisms for coordinating the national cyber incident response in collaboration with law enforcement and intelligence.

Background

Created in 2005 and housed within Public Safety Canada's National Cyber Security Directorate, CCIRC is Canada's national computer emergency readiness team. CCIRC works to reduce Canada's cyber risk by enhancing the cyber security of public and private sector partners and ensuring a coordinated national response to significant cyber events.

ANNEX B – COMMON TERMS

Name	Definitions
Activity	These are "back-of-house" procedures that occur on a daily basis, and that cannot be classified as an event or an incident. In general, they include administrative tasks, or support functions to events or incidents.
Advanced Persistent Threat (APT)	Adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors. The APT actor pursues its objectives repeatedly over an extended period of time, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives.
Botnet	A botnet is a collection of compromised computers that can be used for malicious purposes such as sending spam or viruses, or flooding a network with denial of service attacks.
Crimeware	Malicious software that is covertly installed on computers and has the ability to 'steal' confidential information and send it back to cyber criminals. One form of crimeware is ransomware, which is software that denies access to a person's files until they pay a ransom.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
DNS Sinkhole	A Domain Names Server (DNS) that provides incorrect information to stop the use of the Domain Names that it represents. Commonly used against botnets, a DNS sinkhole denies a computing device from successfully making a connection to the malicious host or domain which may have the intent of executing malicious code.
Event	An event is an observable change to the normal behavior of a computer, IT system, environment, process, or workflow that may impact or may pose a threat to the system or data integrity, or safety and security. An event can be "upgraded" and become an incident if it becomes apparent that the change observed has a probable negative impact and requires mitigation or advice.
Exploit kit	Toolkit that automates the exploitation of vulnerable devices through operating system, browser, and program vulnerabilities. One key characteristic of exploit kits are the ease with which they can be used by those without significant cyber knowledge.
Hacktivism	Some groups of computer hackers are not motivated by financial gain and instead are driven by economic, political, or religious interests that generally go beyond their nation's borders. Their actions are called hacktivism, which is a merger of hacker and political activism. Hacktivists infiltrate networks and put their talents to work for their beliefs by organizing computer attacks, including piracy, hijacking servers, and replacing homepages with ideological messages.
Improper Usage	Any activity that violates acceptable computing use policies.
Incident	An incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising the business operations and threatening the information security of system(s) of national significance within the Canadian public and private sectors.
Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.
Malicious Code	Successful installation of malicious software (e.g. virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
Malware sample	Samples of malicious software reported by victims, or automatically gathered using various technologies such as antivirus programs and network monitoring tools. These samples can be acquired either through open source and commercial feeds, or by establishing strategic partnerships.

Phishing / Targeted Emails	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. Criminally-fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
Rootkit	A collection of tools used to mask the intrusion of, and to obtain elevated permissions to, a computing device or network.
Scans/Probes /Attempted Access	This category includes any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or DoS.
Trojan Horse	A non-replicating program that appears to be benign but actually has a hidden malicious purpose. Some Trojan horses replace existing files with malicious versions, while others add another application to a computing device without overwriting existing files. Trojan horses can be difficult to detect because they often appear to be providing a beneficial purpose.
Unauthorized Access	Category of incident where an individual gains logical or physical access without permission to a network, system, application, data, or other resource.
Virus	A virus is designed to make copies of itself and distribute these copies to other files, programs, or computing devices. Viruses insert themselves into host programs and spread when the infected program is executed (e.g. opening a file, running a program, or clicking on a file attachment).
Worm	Worms are self-replicating programs that are completely self-contained. They do not require a host program to infect a victim. Worms are also self-spreading, but unlike viruses, they can create fully functional copies and execute themselves without user intervention. Worms waste system and network resources and may damage systems by performing malicious acts such as installing backdoors and performing DoS attacks.

ANNEX C – TOP 35 RECOMMENDED MITIGATION ACTIONS

The following is a list of recommended cyber threat mitigation strategies, listed in order of effectiveness and updated in October 2012, to which all organizations should adhere. This list has broad international agreement and is being widely distributed following an initial public release by the Australian Government's Defense Signals Directorate.

Ranking	Mitigation Strategy
1	Undertake application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs.
2	Patch applications such as Adobe PDF viewers and Flash Player, Microsoft Office and Java Runtime Environment. Patch or mitigate high risk vulnerabilities within two days.
3	Patch operating system vulnerabilities. Patch or mitigate high risk vulnerabilities within two days.
4	Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing.
5	Disable local administrator accounts to prevent network propagation using compromised credentials that are shared by several computers.
6	Multi-factor authentication especially implemented for remote access, when the user is about to perform a privileged action or access a sensitive information repository.
7	Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information.
8	Application-based workstation firewall configured to deny traffic by default, to protect against malicious or otherwise unauthorized incoming network traffic.
9	Application-based workstation firewall configured to deny traffic by default, that whitelists applications allowed to generate outgoing network traffic.
10	Non-persistent virtualized trusted operating environment, hosted within the internet gateway, for risky activities such as reading email and web browsing.
11	Host-based Intrusion Detection/Prevention System to identify anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking.
12	Centralized and time-synchronized logging of successful and failed computer events, with regular log analysis, storing logs for at least 18 months.
13	Centralized and time-synchronized logging of allowed and blocked network activity, with regular log analysis, storing logs for at least 18 months.
14	Whitelisted email content filtering allowing only business-related attachment types. Preferably convert/sanitize links, PDF and Microsoft Office attachments.
15	Web content filtering of incoming and outgoing traffic, using whitelisting, behavioural analysis, reputation ratings, heuristics and signatures.
16	Web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.
17	Web domain whitelisting for HTTPS/SSL domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.
18	Workstation application security configuration hardening e.g. disable unrequired features in PDF viewers, Microsoft Office applications, and web browsers.
19	Block spoofed emails using Sender Policy Framework checking of incoming emails, and a 'hard fail' SPF record to help prevent spoofing of your organization's domain.
20	User education e.g. Internet threats and spear phishing socially engineered emails. Avoid weak passphrases, passphrase re-use, exposing email addresses, unapproved USB devices.

21 Operating system exploit mitigation mechanisms such as Data Execution Prevention and Address Space Layout Randomization.

22 Computer configuration management based on a hardened Standard Operating Environment with unrequired functionality disabled e.g. IPv6, autorun.

23 Server application security configuration hardening e.g. databases, web applications, customer relationship management and other data storage systems.

24 Deny direct Internet access from workstations by using an IPv6-capable firewall to force traffic through a split DNS server, an email server or an authenticated web proxy.

25 Antivirus software with up-to-date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop antivirus software from different vendors.

26 Workstation inspection of Microsoft Office files for abnormalities e.g. using the Microsoft Office File Validation feature.

27 Enforce a strong passphrase policy covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words.

28 Restrict access to Server Message Block (SMB) and NetBIOS services running on workstations and on servers where possible.

29 Removable and portable media control as part of a data loss prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.

30 TLS encryption between email servers to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.

31 Disable LanMan password support and cached credentials on workstations and servers, to make it harder for adversaries to crack password hashes.

32 Block attempts to access web sites by their IP address instead of by their domain name.

33 Network-based Intrusion Detection/Prevention System using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.

34 Gateway blacklisting to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.

35 Selected network traffic capture to perform post-incident analysis of successful intrusions, storing network traffic for at least the previous seven days.

Public Safety Canada | Sécurité publique Canada
Deputy Minister | Sous-ministre
Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: MAI MAY 3 1 2013

File No.: 395446
RDIMS No.: 832988

MEMORANDUM FOR THE MINISTER

THE CANADIAN CYBER INCIDENT RESPONSE CENTRE'S OPERATIONAL REPORTS

(Information only)

ISSUE

Your office has requested that the Canadian Cyber Incident Response Centre's (CCIRC) 2012 Annual Cyber Operational Summary and the latest Quarterly Operational Summary be shared with your colleagues on the Cabinet Committee on National Security, including the Prime Minister.

These reports are part of a suite of professional products to provide decision makers with relevant cyber information including noteworthy incidents and trends, as well as services provided by CCIRC. These products are shared with provincial, territorial, and municipal governments as well as approximately 140 partners in the private sector on a regular basis.

CONCLUSION

Please find attached a proposed cover letter for your signature (**TAB 1**) and copies of CCIRC's 2012 Annual Cyber Operational Summary and the Quarterly Operational Summary for the first three months of 2013 (**TAB 2**).

Should you require additional information, please do not hesitate to contact me or Lynda Clairmont, Senior Assistant Deputy Minister, National Security, at 613-990-4976.

François Guimont

Enclosures: (2)

Prepared by: Nate Klassen

Canada

The Right Honourable Stephen Harper, P.C., M.P.
Prime Minister of Canada
Office of the Prime Minister
80 Wellington Street
Ottawa, Ontario K1A 0A2

Dear Prime Minister:

Please find attached, for your information, two reports from the Canadian Cyber Incident Response Centre (CCIRC): the annual 2012 Cyber Operational Report, as well as the most recent Quarterly Operational Summary, covering the period from January to March 2013.

As Canada's computer security incident response team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents affecting non-federal government systems. CCIRC provides authoritative advice and support to the vital cyber systems that underpin Canada's national security, public safety, and economic prosperity.

The attached reports are part of a new suite of professional products for CCIRC's clients that provide decision makers with relevant cyber information including noteworthy incidents and trends, as well as services provided by CCIRC. These are released regularly to provincial, territorial, and municipal governments as well as a growing list of partners in the private sector.

These reports provide a good picture of how we are providing real, hands-on support to critical infrastructure across Canada. Given the growing importance of cyber security and upcoming discussions among Ministers on the issue, I trust this background will be of interest.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P

Enclosures: (2)

The Honourable John Baird, P.C., M.P.
Minister of Foreign Affairs
House of Commons
Ottawa, Ontario K1A 0A6

Dear Colleague:

Please find attached, for your information, two reports from the Canadian Cyber Incident Response Centre (CCIRC): the annual 2012 Cyber Operational Report, as well as the most recent Quarterly Operational Summary, covering the period from January to March 2013.

As Canada's computer security incident response team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents affecting non-federal government systems. CCIRC provides authoritative advice and support to the vital cyber systems that underpin Canada's national security, public safety, and economic prosperity.

The attached reports are part of a new suite of professional products for CCIRC's clients that provide decision makers with relevant cyber information including noteworthy incidents and trends, as well as services provided by CCIRC. These are released regularly to provincial, territorial, and municipal governments as well as a growing list of partners in the private sector.

These reports provide a good picture of how we are providing real, hands-on support to critical infrastructure across Canada. Given the growing importance of cyber security and upcoming discussions among Ministers on the issue, I trust this background will be of interest.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P

Enclosures: (2)

The Honourable Julian Fantino, P.C., M.P.
Minister of International Cooperation
House of Commons
Ottawa, Ontario K1A 0A6

Dear Colleague:

Please find attached, for your information, two reports from the Canadian Cyber Incident Response Centre (CCIRC): the annual 2012 Cyber Operational Report, as well as the most recent Quarterly Operational Summary, covering the period from January to March 2013.

As Canada's computer security incident response team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents affecting non-federal government systems. CCIRC provides authoritative advice and support to the vital cyber systems that underpin Canada's national security, public safety, and economic prosperity.

The attached reports are part of a new suite of professional products for CCIRC's clients that provide decision makers with relevant cyber information including noteworthy incidents and trends, as well as services provided by CCIRC. These are released regularly to provincial, territorial, and municipal governments as well as a growing list of partners in the private sector.

These reports provide a good picture of how we are providing real, hands-on support to critical infrastructure across Canada. Given the growing importance of cyber security and upcoming discussions among Ministers on the issue, I trust this background will be of interest.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P

Enclosures: (2)

The Honourable Jason Kenney, P.C., M.P.
Minister of Citizenship, Immigration and Multiculturalism
House of Commons
Ottawa, Ontario K1A 0A6

Dear Colleague:

Please find attached, for your information, two reports from the Canadian Cyber Incident Response Centre (CCIRC): the annual 2012 Cyber Operational Report, as well as the most recent Quarterly Operational Summary, covering the period from January to March 2013.

As Canada's computer security incident response team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents affecting non-federal government systems. CCIRC provides authoritative advice and support to the vital cyber systems that underpin Canada's national security, public safety, and economic prosperity.

The attached reports are part of a new suite of professional products for CCIRC's clients that provide decision makers with relevant cyber information including noteworthy incidents and trends, as well as services provided by CCIRC. These are released regularly to provincial, territorial, and municipal governments as well as a growing list of partners in the private sector.

These reports provide a good picture of how we are providing real, hands-on support to critical infrastructure across Canada. Given the growing importance of cyber security and upcoming discussions among Ministers on the issue, I trust this background will be of interest.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P

Enclosures: (2)

The Honourable Denis Lebel, P.C., M.P.
Minister of Transport, Infrastructure and Communities,
Minister of the Economic Development Agency of Canada
for the Regions of Quebec and Minister of Intergovernmental Affairs
House of Commons
Ottawa, Ontario K1A 0A6

Dear Colleague:

Please find attached, for your information, two reports from the Canadian Cyber Incident Response Centre (CCIRC): the annual 2012 Cyber Operational Report, as well as the most recent Quarterly Operational Summary, covering the period from January to March 2013.

As Canada's computer security incident response team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents affecting non-federal government systems. CCIRC provides authoritative advice and support to the vital cyber systems that underpin Canada's national security, public safety, and economic prosperity.

The attached reports are part of a new suite of professional products for CCIRC's clients that provide decision makers with relevant cyber information including noteworthy incidents and trends, as well as services provided by CCIRC. These are released regularly to provincial, territorial, and municipal governments as well as a growing list of partners in the private sector.

These reports provide a good picture of how we are providing real, hands-on support to critical infrastructure across Canada. Given the growing importance of cyber security and upcoming discussions among Ministers on the issue, I trust this background will be of interest.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P

Enclosures: (2)

The Honourable Peter MacKay, P.C., M.P.
Minister of National Defence
House of Commons
Ottawa, Ontario K1A 0A6

Dear Colleague:

Please find attached, for your information, two reports from the Canadian Cyber Incident Response Centre (CCIRC): the annual 2012 Cyber Operational Report, as well as the most recent Quarterly Operational Summary, covering the period from January to March 2013.

As Canada's computer security incident response team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents affecting non-federal government systems. CCIRC provides authoritative advice and support to the vital cyber systems that underpin Canada's national security, public safety, and economic prosperity.

The attached reports are part of a new suite of professional products for CCIRC's clients that provide decision makers with relevant cyber information including noteworthy incidents and trends, as well as services provided by CCIRC. These are released regularly to provincial, territorial, and municipal governments as well as a growing list of partners in the private sector.

These reports provide a good picture of how we are providing real, hands-on support to critical infrastructure across Canada. Given the growing importance of cyber security and upcoming discussions among Ministers on the issue, I trust this background will be of interest.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P

Enclosures: (2)

The Honourable Robert Nicholson, P.C., Q.C., M.P.
Minister of Justice and Attorney General of Canada
House of Commons
Ottawa, Ontario K1A 0A6

Dear Colleague:

Please find attached, for your information, two reports from the Canadian Cyber Incident Response Centre (CCIRC): the annual 2012 Cyber Operational Report, as well as the most recent Quarterly Operational Summary, covering the period from January to March 2013.

As Canada's computer security incident response team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents affecting non-federal government systems. CCIRC provides authoritative advice and support to the vital cyber systems that underpin Canada's national security, public safety, and economic prosperity.

The attached reports are part of a new suite of professional products for CCIRC's clients that provide decision makers with relevant cyber information including noteworthy incidents and trends, as well as services provided by CCIRC. These are released regularly to provincial, territorial, and municipal governments as well as a growing list of partners in the private sector.

These reports provide a good picture of how we are providing real, hands-on support to critical infrastructure across Canada. Given the growing importance of cyber security and upcoming discussions among Ministers on the issue, I trust this background will be of interest.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P

Enclosures: (2)

UNCLASSIFIED

DATE:

File No.: 395446
RDIMS No.: 832988

MEMORANDUM FOR THE MINISTER

THE CANADIAN CYBER INCIDENT RESPONSE CENTRE'S OPERATIONAL REPORTS

(Information only)

ISSUE

Your office has requested that the Canadian Cyber Incident Response Centre's (CCIRC) 2012 Annual Cyber Operational Summary and the latest Quarterly Operational Summary be shared with your colleagues on the Cabinet Committee on National Security, including the Prime Minister.

These reports are part of a suite of professional products to provide decision makers with relevant cyber information including noteworthy incidents and trends, as well as services provided by CCIRC. These products are shared with provincial, territorial, and municipal governments as well as approximately 140 partners in the private sector on a regular basis.

CONCLUSION

Please find attached a proposed cover letter for your signature (**TAB 1**) and copies of CCIRC's 2012 Annual Cyber Operational Summary and the Quarterly Operational Summary for the first three months of 2013 (**TAB 2**).

Should you require additional information, please do not hesitate to contact me or Lynda Clairmont, Senior Assistant Deputy Minister, National Security, at 613-990-4976.

François Guimont

Enclosures: (2)

Prepared by: Nate Klassen