Communications Security Establishment
Centre de la sécurité des télécommunications

CYBERJOURNAL

EDITION 6 – 2014 Volume 2

IN THIS EDITION

KEEPING OUR INFORMATION SECURE

Government of Canada (GC) departments rely on information technology (IT) systems to support their business activities. These interconnected systems are often subject to serious threats which can have adverse effects on departmental business activities by compromising the confidentiality, integrity or availability of the systems.

Since cyber threats are becoming increasingly sophisticated and targeted, insufficient IT security can lead to an increase in successful cyber-security exploits. These incidents can have a significant and direct impact on organizations. Properly assessing the security risks specific to your organization can help minimize your weak points. CSE can provide leading-edge guidance and strategic advice to help secure your networks.

In this edition of Cyber Journal, we discuss the security risks involved with some current technologies such as Instant Messaging (IM) and Voice over Internet Protocol (VoIP), both of which are fast becoming popular methods of communication and collaboration at work. We also broach the subject of keeping the information assets contained on our classified networks secure.

The security of the GC's IT systems is CSE's business!

Originally signed by

Toni Moffa
Deputy Chief, IT Security

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

INSTANT MESSAGING SECURITY RISKS

Instant Messaging tools such as Google Talk, BlackBerry Messenger, and Pidgin, provide a quick and easy way to communicate, collaborate, and share information. Since IM is quickly becoming a popular communication method in GC departments, it is important to understand the risks associated with using IM tools, and the available mitigation techniques.

Like e-mail, IM clients have similar risks associated with their usage such as vulnerabilities to worms, Trojan horses, hijacking, impersonation, denial of service attacks, and social engineering. However, there are also unique risks to using IM clients. Some of these risks include:

- ✗ Bypassing firewall restricted ports;
- ✗ Bypassing anti-virus gateways;
- ✗ Unencrypted communications; and
- ✗ No Authentication.

GC departments planning to use IM tools should perform a threat and risk assessment as outlined in: IT Security Risk Management: A Lifecycle Approach (ITSG-33), in order to implement a balanced set of security controls.

Methods for mitigating the risks associated with IM tools that can be implemented include:

- ✓ Patching operating systems and applications;
- ✓ Establishing and enforcing a departmental IM policy;
- ✓ Configuring firewalls to block unapproved IM clients;
- ✓ Using protective software (e.g., anti-virus);
- ✓ Isolating the IM system; and
- ✓ Using a private naming convention.

For more helpful tips on keeping your network secure, visit our IT Publications website to download CSE Top 35 Mitigation Measures (ITSB-89A), or contact us at itsclientservices@cse-cst.gc.ca.

SPOTTING MALICIOUS E-MAILS

Malicious e-mails are often used by cyber intruders to introduce malware through a network's security perimeter in order to gain access. These e-mails typically target individual recipients or group mailboxes to solicit information or execute malware.

If a threat actor targets a network administrator, they can gain access to all the privileges of that user. To increase the probability that recipients will open malicious e-mails, threat actors use spear-phishing techniques to target specific individuals and introduce malware.

The following methods are the most popular means of inducing a recipient into opening a malicious message and introducing malware:

- Pretending to be someone you know;
- Innocent looking links or documents attached; and
- Unknown e-mail addresses.

Implementation of the Top 4 mitigation measures as outlined in Cyber Case Study: Why The Top 4 Measures Are Essential (ITSB-97) will significantly help mitigate against cyber threats through policy and technical measures. Patching operating systems and applications, whitelisting applications and minimizing administrator privileges are strategies that work cohesively to prevent the execution and spread of malware within a network.

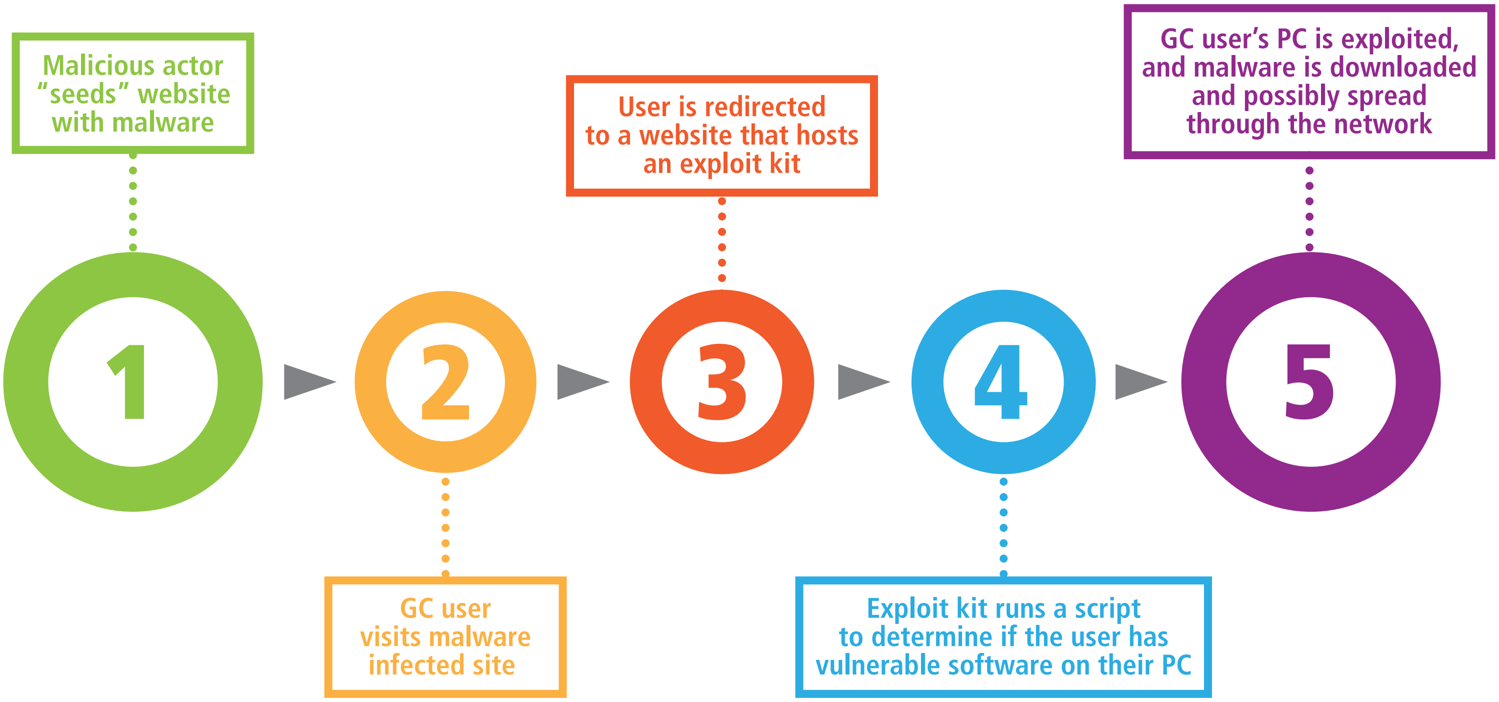
Departments can further minimize the effects of malicious e-mails by using:

- ✓ Anti-virus software;
- ✓ Hyperlink scanning tools;
- ✓ Network segmentation & segregation;
- ✓ A Signed Message Policy (SMP);
- ✓ A virtualized e-mail client;
- ✓ Server access control; and
- ✓ Transport Layer Security (TLS) e-mail encryption.

GC CIRT POINTER: THE DANGER OF EXPLOIT KITS

Exploit kits are currently one of the most effective and pervasive threats to GC networks. An exploit kit is a web application that allows malicious actors to compromise other computers over a network by exploiting known vulnerabilities.

Browsers, and any programs that can be accessed by a browser, are the main targets of exploit kits. The more popular exploit kits target vulnerabilities in various browsers such as Internet Explorer, Firefox, Google Chrome, and Safari. They also target vulnerabilities in browser plugins such as Adobe products, and Java applications running on the Microsoft Windows platform.



1 Malicious actor "seeds" website with malware

2 GC user visits malware infected site

3 User is redirected to a website that hosts an exploit kit

4 Exploit kit runs a script to determine if the user has vulnerable software on their PC

5 GC user's PC is exploited, and malware is downloaded and possibly spread through the network

Once a computer is exploited, a door is left open for the exploit kit to download any type of malicious file such as spyware, Trojans or state-sponsored implants without the consent or knowledge of the user. This exploit can result in theft of login credentials of a protected system, theft of banking credentials, identity theft or bitcoin mining. Moreover, because exploit kits are not bounded by geographical limits, (i.e., they can be remotely controlled), their sources are difficult to trace.

In order to prevent exploit-kit compromises from escalating throughout the whole network, GC departments are encouraged to implement CSE's Top 4 Mitigation Measures as well as the more "defense-in-depth strategies" listed in CSE's Top 35 Mitigation Measures (ITSB-89A).

If you are concerned that your network may have been compromised by or is a possible target of a malicious exploit kit, please contact the Shared Services Canada Computer Incident Response Team at: sscgccirt.spcericgc@ssc-spc.gc.ca for detection, mitigation and prevention options.

CYBERJOURNAL

EDITION 6 – 2014 Volume 2

SECURING YOUR GC SECRET NETWORK

GC networks are frequently targeted by a wide variety of threat actors wishing to gain access to GC information. If your department has a SECRET-level system, there are a couple security measures you can implement to protect it from threat actors.

1 In accordance with the above directive, SECRET networks should be physically and logically isolated from Internet accessible systems, as well as being appropriately zoned according to Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22) and Network Security Zoning – Design Considerations for Placement of Services with Zones (ITSG-38); and

2 Cross-domain transfers between your SECRET network and other networks must always be carried out using an approved Cross-Domain Solution. Encryption alone does not make USB flash drives or other portable storage devices safe for transferring media between networks of different security levels. For more information on Cross-Domain Solutions contact ITS Client Services.

SHARING INFORMATION ACROSS DIFFERENT SECURITY DOMAINS

Driven by the operational requirements to access and share information more efficiently between partners and within their own infrastructure, GC departments need to have the ability to transfer data between networks at different security levels. Cross-Domain Solution (CDS) technology can meet these requirements with automation, timeliness, efficiency and enhanced security.

When attempting data transfers across domains with different security policies, there are inherent risks and threats. Depending on the policies and practices in place, these threats can have impacts on security:

- Leakage of corporate data;
- Installation of unauthorized software; and
- Exposure of classified information.

Since CDS can be a potential exploitation point, deployments can attract more sophisticated threat actors. Consequently, greater attention to the selection and implementation of appropriate security controls is required in conjunction with an approved CDS. It is strongly recommended to adhere to a robust design and development framework such as: IT Security Risk Management: A Lifecycle Approach (ITSG-33) when deploying a CDS.

CSE's role on matters related to cybersecurity in the GC includes acting as the GC CDS technical authority, which includes providing technical advice and guidance on all aspects of CDS.

CSE is working closely with Shared Services Canada (SSC) to ensure the needs of all departments within the GC are met on these and other topics:

- **Securing your GC networks;**
- **Sharing information across different security domains; and**
- **VoIP systems.**

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

VOIP FOR GC DEPARTMENTS

Voice over Internet Protocol (VoIP) can be a cost-effective alternative to traditional telephone systems for GC departments. The merging of voice and data networks offers new possibilities, but also introduces new network security risks. Maintaining the availability, integrity, and confidentiality of voice communication is a challenge when VoIP is implemented on a combined network with a corporate intranet or deployed over the Internet.

Every network environment has different security requirements, and the creation of a departmental Threat and Risk Assessment (TRA) will outline where the networks are most vulnerable. Based on this assessment, a multi-layer "defense-in-depth" solution is required to setup and secure VoIP infrastructure.

A multi-layer approach involves having technical, operational and managerial controls in place that are tailored to the unique situation and needs of the departmental environment. This solution can be implemented in a variety of ways with different elements such as:

- ✓ Physical separation of network segments;
- ✓ Virtual separation;
- ✓ Port security; and
- ✓ Firewalls.

As well as following IT Security Risk Management: A Lifecycle Approach (ITSG-33) recommendations, the following guidelines should be used as references when installing non-classified VoIP systems in classified facilities in Canada:

- Guidelines for VoIP Computer Telephony (CNSSI 5000);
- National Instruction for Approved Telephone Equipment (CNSSI 5006); and
- TSG Guidelines for Computerized Telephone Systems.

These publications provide security controls to minimize the risk of classified audio or video being emitted to unauthorized entities outside of the classified facility. The guidance provided in these publications should be considered in any situation where the security classification level of the VoIP system is lower than that of the physical security zone in which it is deployed. For example, a SECRET-level conversation held in the vicinity of an unclassified VoIP phone, could lead to the compromise of classified information.

CSE can provide guidance on the many options that are available for maintaining the security of VoIP. To learn more, contact us at itsclientservices@cse-cst.gc.ca.

SMARTCOMPUTING TIP

Pass-the-Hash (PtH) is a lateral movement and privilege escalation technique that exploits a vulnerability in all current versions of Microsoft Windows.

To learn more about mitigation measures and to protect your systems against PtH, download: Microsoft Windows Pass-the-Hash Vulnerability and Mitigations (ITSA-66)

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

TBS CORNER: WEB 2.0 AND THE GC IT SECURITY COMMUNITY

Web 2.0 tools provide a method to quickly disseminate information of value across communities of practice, and most importantly, for users to engage in interactive two-way communication and dynamic collaboration. Within the IT security community, Web 2.0 provides a way to share unclassified material amongst members.

For several years, the IT security community within the GC has made use of various Web 2.0 collaboration tools, such as GCforums, GCpedia and GCconnex. In particular, the Security Awareness Working Group has been successfully using GCpedia – the internal GC Wiki – to share their material and build a of community of practice for Security Training and Awareness.

With more than 30,000 members across the GC, GCconnex, an internal professional networking platform, is experiencing rapid growth. A "Swiss army knife" in terms of its social networking functionality, GCconnex gives users the ability to create open or closed groups, share unclassified documents, and vote on ideas.

The GC Enterprise Security Architecture (GC ESA) working group has built a presence on GCconnex and GCpedia for IT security practitioners. These newly devised groups enable the building and maintenance of working relationships in an open environment for the purposes of networking, cooperation and supporting the creation of focused collaboration networks.

The GC ESA group can help reduce duplication of effort among practitioners in various departments and agencies by providing a forum to share best practices. In addition, the site will be used to share GC ESA tools and templates, including draft documentation, in order to engage the IT security community.

GCconnex

GCPEDIA
PEOPLE & KNOWLEDGE
GENS & SAVOIR

QUESTIONS?

CSE's business is ensuring that the GC's critical information systems are secure!

If your GC organization has any IT security questions or concerns, please contact our Client Services team at:

613-991-7654, or
itsclientservices@cse-cst.gc.ca

APPLICATION-BASED FIREWALLS

Application-based firewalls are used to protect the integrity and confidentiality of application-based information. They are software programs that operate up to the Application Layer of the OSI Model and protect the integrity of the system by filtering the requests for application-based information.

CSE recommends the use of application-based firewalls on workstations to filter and exclude unauthorized communications. The efficacy of these firewalls can be improved through the use of Application Blacklisting, wherein a 'blacklist' of unauthorized executables is used to exclude communications with specific—possibly malicious—programs.

While application blacklisting is good practice, it is not the only choice. Application Whitelisting can also be used to improve the effectiveness of an application-based firewall through the use of a 'whitelist'. Only executables on the 'whitelist' are allowed to send and receive communication within the application's environment.

The use of an application-based firewall can improve the department's security profile by adding another layer of control within the system's security perimeter. In order to perpetrate a successful exploit, a malicious intruder would not only have to subvert the network's standard security defense but then also overcome the security represented by the application-based firewall.

For more information about application-based firewalls and protecting system boundaries, visit our IT Publications webpage and download Top 35 Mitigation Measures (ITSB-89A) and IT Risk Management: A Lifecycle Approach (ITSG-33) Annex 3.

ITS LEARNING CENTRE NEWS

The ITS Learning Centre (ITSLC) continues to foster a closer relationship with the Canada School of Public Service (CSPS). As part of this evolving partnership, the ITSLC is now offering the following courses through CSPS:

HARMONIZED THREAT & RISK ASSESSMENT (HTRA) (A341)

The revised instructor-led course is structured to provide HTRA methodology through a combination of classroom presentations, discussions, exercises, and examples relevant to the GC IT environment. This course allows participants to apply the HTRA methodology to their specific departmental security situation.

IT SECURITY RISK MANAGEMENT: A LIFECYCLE APPROACH (ITSG-33) E-LEARNING COURSE (I216)

In addition to its classroom-based course (104), the ITSLC has developed an abbreviated online course (I216). This new e-learning course provides a high-level appreciation of the key concepts and processes outlined in ITSG-33 while focusing on IT-related security risks to the GC.

BASIC TACLANE E-LEARNING COURSE (B280)

Basic TACLANE (280) has been converted into an e-learning course available online through CSPS (B280). This course provides participants with an overview of the TACLANE family of products, as well as basic IP network and keying concepts.

COMING SOON!

LOOKING FOR COMSEC INFORMATION?

COMSEC Client Services recognizes the importance of providing pertinent COMSEC information to all of its clients, as well as providing efficient and reliable solutions to meet their changing communications needs.

There are two online locations to find COMSEC information:

1. The IT Security Publications web-page on the CSE web-site contains the most recent COMSEC Control Directives, Guidelines, Alerts and Bulletins.
2. The COMSEC User Portal (CUP) provides more detailed equipment information such as, Approvals for Use, Equipment User Manuals, and forms. In order to access the CUP, you must be appointed as a member of departmental COMSEC staff. The CUP is located at https://comsecportal.cse-cst.gc.ca/.

ABOUT THIS NEWSLETTER

Cyber Journal has been prepared for GC IT practitioners and stakeholders and is published on a periodic basis. This publication reflects the CSE IT Security commitment to share information, advice and guidance with the broader GC community to help departments and agencies better protect themselves from cyber threats. The aim is to highlight key security issues and stimulate discussion about security within your Department. In addition, the newsletter profiles key products and services offered by CSE with information on how you can leverage them to help your GC organization. Security awareness throughout an organization is an essential element to improving the GC's security posture. As such, we encourage you to share this information within your organization.

SUBSCRIBE

To be notified of future releases, contact: itsclientservices@cse-cst.gc.ca.

CONTACT US

For general advice and security guidance support, contact:

✉ **itsclientservices@cse-cst.gc.ca**

☎ **General Inquiries: (613) 991-7654**

To contact the Cyber Threat Evaluation Centre:

✉ **ctec@cse-cst.gc.ca**

For planning, support or any issues regarding COMSEC devices, contact COMSEC Client Services:

✉ **comsecclientservices@cse-cst.gc.ca**

☎ **General Inquiries: (613) 991-8495**

COMSEC custodians can contact the Crypto Material Assistance Centre (CMAC):

✉ **cmac-camc@cse-cst.gc.ca**

☎ **General Inquiries: (613) 991-8600**

For education and training services, contact the IT Security Learning Centre:

✉ **its-education@cse-cst.gc.ca**