Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

UPDATE

JUNE 2014

The Cyber Security Picture 2013

Summary

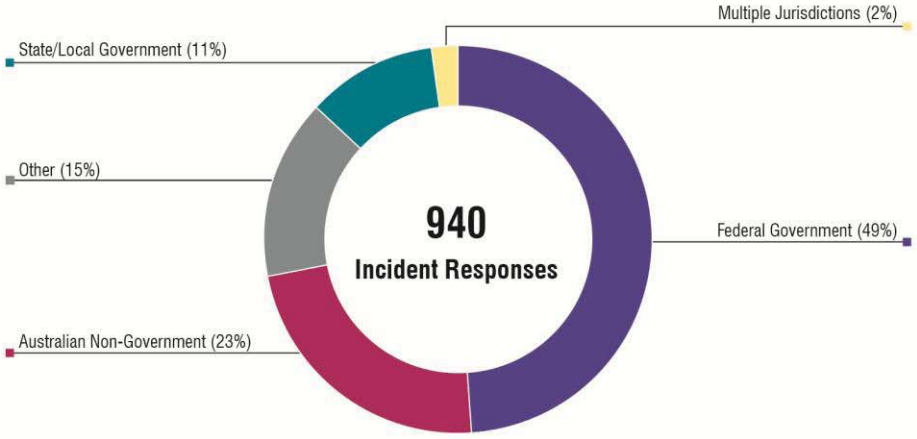
1. This report summarises cyber intrusion activity identified by or reported to the Cyber Security Operations Centre (CSOC) during 2013. It provides a broad overview of cyber threats to Australian government networks, as observed by the CSOC.

2. The *Strategies to Mitigate Targeted Cyber Intrusions* remain your best defence against the cyber threat. Implementing the Top 4 strategies as a package is at the core of this protection, as they mitigate at least 85% of cyber intrusions responded to by the CSOC. The Top 4 strategies prevent execution of malicious software, and minimise software vulnerabilities and the ability of a cyber adversary to propagate across a network. The remaining 31 strategies form an excellent basis from which to assess further network security initiatives based on a risk assessment. Your risk assessment processes should take into account the specific risks faced by your agency, the information you are protecting, and your current network security posture.

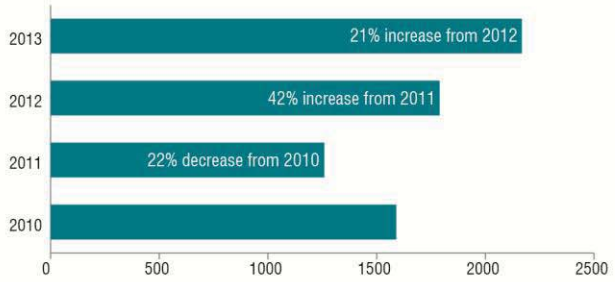
3. While socially engineered emails remain the most prevalent threat to Australian government networks, the CSOC observed the emergence of several new techniques used in these emails during 2013, such as the use of cloud storage providers, Java files, and the repurposing of genuine emails. The increasing skill and resourcefulness of cyber adversaries highlights the importance of being continually vigilant and up-to-date in your network security. The *Strategies to Mitigate Targeted Cyber Intrusions* have been updated in 2014 to reflect the evolution of the threat environment.

4. Although the initial cost of implementing the *Strategies to Mitigate Targeted Cyber Intrusions* can seem high for some agencies, they actually represent an important investment in your organisation, reducing long term costs and risk. If you experience a network compromise, not only will you be faced with the cost of implementing these strategies to prevent further compromise, but you will also incur both higher direct and indirect costs associated with remediating the compromise. These costs include, but are not limited to: investigating the compromise, tactical remediation, reputational costs, opportunity costs from the loss of information, and lost productivity. See ASD's *The Cost of Compromise* publication for more information about costs associated with compromise.

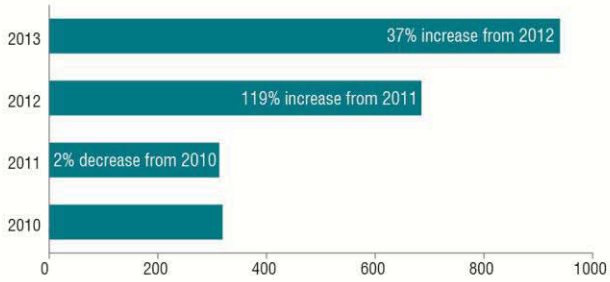
Key CSOC Statistics 2013



Cyber security incidents observed by the CSOC



Cyber security incident responses



Top 5 identified attack or intrusion methods

Socially engineered emails
Stolen credentials
Website defacement
Drive-by download
Denial of service

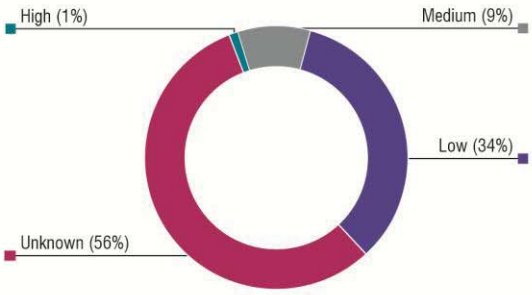
Top 5 attachment types used

- Microsoft Word (inc RTF)
- Zip
- JAR
- PDF
- RAR

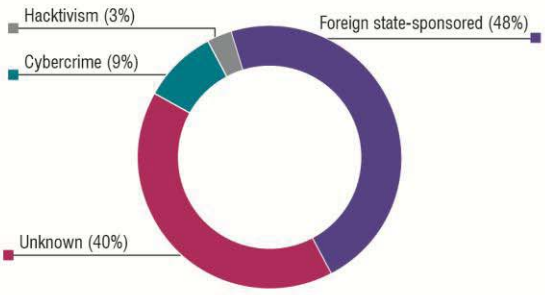
Common subject themes in socially engineered emails

- G20
- ASEAN
- Taxation
- Employment opportunities
- Current affairs

Victim impact of cyber security incidents



Threat adversary



Something old, something new

The same spear phishing threat…

5. Targeted socially engineered emails remain the most prevalent method used to target Australian government networks. Where an intrusion method was identified, these emails comprised 53% of cyber security incidents responded to by the CSOC, in 2013. While the percentage decreased from 63% in 2012 and 77% in 2011, a corresponding increase in other techniques demonstrates the persistence and innovative methods of cyber adversaries to compromise Australian government information.

…but new techniques

6. While targeted socially engineered emails are a traditional threat vector, cyber adversaries have diversified aspects of their tradecraft in order to increase the likelihood of successful delivery and user interaction, such as through the use of:

a. cloud storage providers, including Dropbox;

b. Java (JAR) files; and

c. repurposing genuine emails.

7. Dropbox is a free online file storage service which allows users to share files and collaborate with other users, accessing and synchronising all types of files across all the devices they use. An email with a legitimate subject and a Dropbox link is more likely to bypass email content filtering and gateway antivirus scanning. Files shared through the use of Dropbox are downloaded over an encrypted channel, and consequently, unless an appropriate vendor product has been installed, the effectiveness of traditional network monitoring to detect malware significantly decreases.

In a targeted intrusion attempt reported to the CSOC in May 2013, a socially engineered email was sent to several Australian government departments. The email contained a link to a **Dropbox** storing a zip file that concealed two executable (.exe) files. Upon opening the zip file, the user would then open what would appear to be a benign Adobe Portable Document Format (PDF) file, while malicious code from the .exe file ran in the background. If the malware were to execute, it would attempt to communicate with a cyber adversary website to gain remote access to the victim network.

8. The CSOC recommends that you carefully risk-assess your use of cloud storage services, review the mitigations these services have in place and assess their effectiveness, and implement appropriate strategies to mitigate the risks.

9. In 2013, the CSOC noted that socially engineered emails sent to Australian government departments containing malicious Java (.jar or JAR) attachments accounted for 10% of attachments used in socially engineered emails, where an intrusion method was identified. A JAR file is an archive file format that distributes software on the Java platform - successful execution of JAR attachments may allow a cyber adversary to gain remote access to the victim network.

During 2013, the CSOC observed repeated attempts to compromise Australian government networks via Java attachments. In the typical scenario, a user inadvertently downloaded a JAR file after clicking on a malicious link. The file contained malware that would allow a cyber adversary to gain remote access to the user's workstation, and then continue to propagate across the network from that point. Agencies that had successfully implemented the Top 4 strategies prevented serious intrusions from occurring. However, if the malware had been able to execute, it would have been possible for a cyber adversary to masquerade as the compromised user, send a socially engineered email enticing more users to click on the link, and then extensively compromise a network.

10. With its ability to run regardless of the user's workstation architecture, the Java platform remains a preferred program to perform business functions. Although each new version of Java undergoes heavy scrutiny by the IT community for new security vulnerabilities, many Australian government agencies have poor patching practices, leaving them exposed to vulnerabilities that are exploited by cyber adversaries.

11. The *Strategies to Mitigate Targeted Cyber Intrusions* have been updated in 2014 to reflect the growing emergence of Java as a threat to Australian government networks. In addition to implementing the Top 4 strategies to protect your network from your user's browsing activities, the following strategies are also recommended to combat the Java threat:

a. Strategy 5 – **User application configuration hardening**, disabling: running of Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.

b. Strategy 7 – **Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).

c. Strategy 17 – **Email content filtering**, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.

d. Strategy 18 – **Web content filtering** of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.

e. Strategy 21 – **Workstation and server configuration management** based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.

12. In addition to these strategies, ASD also recommends that you consider these additional technical controls for mitigating malicious Java exploits:

a. Allowing Java applications to run only from trusted sources, such as the corporate intranet or Australian government (gov.au) internet domains.

b. Configuring separate browsers for internal and external use.

c. Investigate the use of Oracle's *Deployment Rule Set* which ensures less trusted applications are run with only the latest version of Java, while allowing legacy applications to run on other versions.

13. Cyber adversaries are persistent and aggressive in their efforts to compromise Australian government networks, and are constantly updating their tradecraft to achieve success. In 2013, the CSOC also saw evidence of legitimate emails and attachments being repurposed, modified to include malicious code, and then re-used to target Australian government users in socially engineered emails.

The CSOC observed the increasing **use of legitimate email addresses to conduct malicious activities**. For example, a day after receiving a legitimate email, several Australian government employees received the same email but with a different attachment, containing malware. In most cases, these emails were ineffective as they were either blocked from reaching the end user, or the malware was blocked from executing due to the implementation of application whitelisting. ASD recommends that agencies also consider implementing Strategy 5 – User Application Configuration Hardening, to further protect their networks against this type of intrusion activity.

Drive-by download and watering-hole techniques

14. Open-source reporting has alluded to the growing popularity of watering-hole techniques in 2013. Taking full advantage of a user's trust in a website, the watering-hole technique provides an effective method for exploitation.

Intrusions using **watering-hole techniques** involve cyber adversaries compromising and placing malware on a legitimate website, in an attempt to compromise the computers of visitors to the website. After learning their victim's behaviour and habits, the cyber adversary chooses a website that their targeted victim has a valid business reason to visit, thereby creating a **targeted drive-by download**.

15. In 2013, the amount of activity observed by the CSOC attributed to drive-by download activity increased. However, the nature of this activity was incidental and opportunistic rather than deliberate targeting – it is very difficult to identify watering-holes that have been specifically created to target particular users. Consequently, the CSOC has little evidence of premeditated targeting of Australian government victims using this technique.

16. While user education is an important defence-in-depth approach, it will not prevent a user from visiting a legitimate website that has been temporarily compromised to deliver malicious content as part of a watering-hole or drive-by download. Visiting such a website might compromise the user's workstation without any obvious indications of compromise to the user.

17. There are two aspects to mitigating this type of activity:

a. Ensure that your websites and web applications cannot be compromised and used as watering-holes. ASD has released the guidance document *Protecting Web Applications and Users*, which can assist.

b. In addition to implementing the Top 4 *Strategies to Mitigate Targeted Cyber Intrusions* to protect your networks from your user's browsing activities, you should also deploy:

i. Strategy 5 – **User application configuration hardening**, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.
ii. Strategy 6 – **Automated dynamic analysis** of email and web content run in a sandbox to detect suspicious behaviour, including network traffic, new or modified files, or other configuration changes.
iii. Strategy 7 – **Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).
iv. Strategy 17 – **Email content filtering**, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF, and Microsoft Office attachments.

A final word

18. Your network is not necessarily the only network that holds your agency's information – do not forget about contractors and other service providers, who may be the weaker and therefore more attractive target for a cyber adversary that wants your information. Also consider that you likely hold the information of others, often with contractual provisions around confidentiality or secrecy. While your own information may potentially not be of interest to a cyber adversary, information you hold for third parties may be, and cyber adversaries often target the weakest link.

Further Information

19. The *Australian Government Information Security Manual* (ISM) assists in the protection of official government information that is processed, stored or communicated by Australian government systems, and is available at:

http://www.asd.gov.au/infosec/ism/index.htm

20. ASD's *Strategies to Mitigate Targeted Cyber Intrusions* and its companion ASD products, which complement the advice in the ISM, are available on ASD's website:

http://www.asd.gov.au/top35mitigationstrategies.htm

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.