(UPDATED) AUGUST 2012

Personal computing and the implications for agency networks

1. This document is for government agencies that allow the use of non-agency controlled devices to conduct government business either through consumer-oriented services such as webmail, or via remote access to agency networks.

2. Government officials can unwittingly endanger Australian government information when they access government systems and/or information using non-agency controlled devices infected with malicious software (malware). This increases the potential for the unauthorised disclosure of government and corporate information, theft of personal identity information and fraud.

3. This document explains the risks posed by, and possible mitigations for, malware which is able to steal Australian government login credentials and remotely view and even access official information and systems.

Intended audience

4. This document is intended for information security practitioners, to inform security risk management decisions and user education programs regarding the use of personal computing devices when conducting government business.

Risks for agency networks

5. New technologies are providing opportunities for government agencies to conduct their business with more efficiency and mobility. Accordingly, users are increasingly using remote access solutions and accessing government networks and information from non-agency controlled devices.

6. However, using a non-agency controlled device for both personal and business purposes can make it more susceptible to internet based threats. In particular, during personal web browsing, users are more likely to open unidentified links or visit unfamiliar sites, which can lead to infection with malware.

7. This not only has personal consequences for the user – such as identity theft and fraud – but also poses a threat to the government networks and information they access. Malware may find an entry route into the associated agency networks as well as access to information stored or communicated on the non-agency controlled device.

8. Malware also has the ability to perform keystroke logging, capture screen shots, and even remotely control and use infected computers. This can enable the theft of usernames, passwords and other personal information, including user credentials for government networks accessed from infected devices. This activity can be difficult for an agency to detect as an adversary using stolen login credentials can imitate a legitimate user, and therefore circumvent agency access controls.

9. Malicious activity of this nature is most commonly used for direct financial gain. Approximately 65% of malicious activity observed by the Cyber Security Operations Centre (CSOC) has an economic driver, targeting information about Australia's business dealings, its intellectual property, its scientific data and the government's intentions, as well as personal data for identity theft.

10. The unauthorised disclosure of official information into the public domain could result in embarrassment and loss of confidence in government services, or even adversely affect Australia's national security and economic well-being.

Case Study: The SpyEye Threat

What is SpyEye?

SpyEye, a piece of malware sold in underground internet forums, is designed to steal business and personal information from a victim's computer. SpyEye infects computers in a number of ways, commonly through the exploitation of websites, spear-phishing or spam campaigns and peer-to-peer file sharing sites.

In 2010, SpyEye superseded Zeus as the malware of choice amongst cyber criminals stealing bank and credit card details online. Cyber criminals using SpyEye have a global reach. It is estimated cyber criminals have access to a global network of 2.2 million computers infected with SpyEye.

What are the implications for government?

Australian government login credentials are being stolen by SpyEye after users access government networks from their personal computing devices. The CSOC estimates that roughly 1000 government credentials are stolen each month by SpyEye, and that there are up to 50,000 Australian devices infected with SpyEye at any given time. These numbers are based on sampling of the current cyber threat environment, and are potentially much higher.

This represents a significant threat to government, as it increases the possibility of unauthorised access to government networks, services and official information.

Mitigation strategies

11. When agencies allow users to access government information remotely they risk exposure to malicious activity, as these users may not maintain the same level of security awareness when using personal devices. Therefore, agencies should educate users on the risks of using non-agency controlled devices to conduct government business.

12. User education should be tailored to the job role of the user. However, in general, users should be made aware of the common techniques used to spread malware and be educated to avoid:

a. clicking on links in emails

b. opening email attachments from suspicious or unfamiliar sources

c. selecting weak passphrases

d. re-using the same passphrase across multiple applications

e. unnecessarily exposing their email address and other personal details

f. where possible, using the same device for work-related and personal activities (e.g. downloading and playing computer games).

13. Users should also be advised of the benefits of implementing strategies from DSD's *Strategies to Mitigate Targeted Cyber Intrusions*. Agencies may need to include implementation guidance as part of their user education program. Recommended strategies include:

a. **patching applications and operating systems.** Users should always use the latest version of operating systems and applications, especially PDF viewer, Flash Player, Microsoft Office, Java, web browser and web browser plugins such as Active X

b. **implementing an application based workstation firewall.** This should be configured to deny traffic by default that protects against malicious or otherwise unauthorised incoming network traffic and to whitelist which applications are allowed to generate outgoing network traffic

c. **choosing antivirus software with up to date signatures, reputation ratings and other heuristic detection capabilities**

d. **avoiding logging into the administrative account of the personal device unless performing administrative tasks.**

14. Agencies should not allow the use of privileged access to agency networks remotely, including logging in as an unprivileged system user and then escalating privileges.

15. Further mitigations for agencies to consider implementing may include:

a. monitoring the use of remote access solutions for anomalous activity

b. at log-in, presenting the user with details of their last login attempt

c. using multi-factor authentication

d. network segmentation and filtering – minimise the services provided by remote access to only those required. This applies to which services are made available and also to the number of users which may access them

e. endpoint compliance checking

f. using, where feasible, an agency-approved and managed Trusted Operating Environment.

Further information

16. Further security controls, including for remote or privileged access, can be found in the *Australian Government Information Security Manual* at:
http://www.dsd.gov.au/infosec/ism/index.htm

17. A complete list of *DSD's Strategies to Mitigate Targeted Cyber Intrusions*, as well as more detailed information on the Top 4 strategies, can be found at:
http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

18. Complementary guidance published by DSD for information security practitioners includes:

Multi-factor Authentication (January 2012)

Using Remote Desktop Clients (December 2011)

19. DSD has also published a range of advice for Australian government users:

Drive-by Downloads (December 2011)

Detecting Socially Engineered Emails (November 2011)

Travelling Overseas with a Laptop (April 2011)

Travelling Overseas with a Blackberry (November 2010)

20. These products are available through the OnSecure web portal, DSD public website or upon request for distribution within your agency.

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

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.