

Information Technology Security Guide
Lead Agency Publication G2-006



Spyware Prevention Guidelines

Technical Security Branch
Technical Operations
Royal Canadian Mounted Police
Issued: March 2008

Disclaimer of Responsibility

This publication has been prepared by the RCMP for the use of departments or agencies in the Government of Canada. The publication is informal and limited in scope. It is not an assessment or evaluation and does not represent an endorsement of any sort by the RCMP. The material in it reflects the RCMP's best judgment in light of the information available to it at the time of preparation. Any use a third party makes of this publication, or any reliance on or decisions made based on it, are the responsibility of such third parties. The RCMP accepts no responsibility for damages, if any, by any third party as a result of decisions or actions based on this publication.

Copyright 2008 Government of Canada, Royal Canadian Mounted Police (RCMP)
1200 Vanier Parkway, Ottawa, Ontario, Canada, K1A 0R2

This publication may be reproduced verbatim, in its entirety, without charge, for educational and personal purposes only. However, written permission from the RCMP is required for use of the material in edited or excerpted form, or for any commercial purpose.

TABLE OF CONTENTS

1	Introduction	1
1.1	Purpose.....	1
2	Spyware Infections.....	1
2.1	Web browsing	1
2.2	Downloading free software	2
2.3	File sharing programs	2
2.4	Email.....	2
3	Spyware Symptoms	2
4	Defence Mechanisms	2
4.1	Anti-Spyware Software	3
4.2	Anti-Virus Software	3
4.3	Surf Safely	3
4.4	Patch Management.....	3
5	Security Awareness	4
6	Conclusion	4
7	Glossary	5

1 Introduction

Government department information systems are often targets of various types of threats, such as malicious code, spam and more recently, spyware. With government departments offering more web-based services, spyware is a growing threat. Such a threat can be difficult to detect, as it gathers information, gains unauthorized access or installs spyware silently or covertly.

By definition, spyware is any software that collects personal information about a person or organization, usually without their knowledge or consent. This information is then sent to an unauthorized third party. The information collected by spyware can include usernames, passwords, web surfing habits, inventory of applications installed on a computer, registry settings, version of operating system, etc., which is then sent to third-party on the Internet. These spyware programs are often built-in to 'free' downloadable programs from the Internet. Typically, the reason these programs are free is a result of marketing/advertising companies compensate the program developer of the program to embed spyware within it. The concept of freeware certainly can create a trade-off between functionality and cost versus privacy and security. Without the proper defences of information systems, spyware can enter organizations through browser downloads, shareware, emails and spam.

As described in the Government Security Policy, information systems must be secured against evolving threats, which includes spyware. Spyware poses a real threat to the confidentiality, integrity and availability of computers systems and data. The risks and consequences of spyware against a government organization can be severe given the nature of its business operations, domestic and foreign commitments, combined with public accountability and scrutiny.

Spyware threats originate from un-trusted websites or emails and the task of securing information systems should not be taken lightly.

1.1 Purpose

The purpose of this document is to provide guidelines for the effective implementation of safeguards and countermeasures that can be used to reduce the risk spyware threats. These guidelines are intended to complement existing standards such as the *Government of Canada Operational Security Standard: Management of Information Technology Security (MITS)*.

2 Spyware Infections

There are numerous ways a computer system can become infected with spyware. Some of the most common risk areas follow.

2.1 Web browsing

While surfing the Internet, spyware can infect your machine. For example, pop up ads is a means whereby the pop up window may disguise as a Windows error message. When the user clicks on a button that will supposedly fix the error, spyware is installed. The goal of these pop up ads is to deceive you into clicking on a button.

Other forms of spyware are designed so that you do not need to click on any buttons or install any software. Simply visiting an infected or malicious website (e.g. adult content) can install spyware. These malicious web sites exploit vulnerabilities in web browser's built-in components, such as ActiveX or JavaScript.

2.2 Downloading free software

Some companies offer free programs that are bundled with spyware. When the free program is installed, you are also installing the spyware component. These companies will often disclose their intent in the software's end user license agreement (EULA). These EULAs are often lengthy and full of legal jargon which results in users failing to completely read before agreeing to the terms and conditions.

The advice for users is to read the EULAs carefully and understand what this program may do to your system before clicking on "I accept" or "Yes".

2.3 File sharing programs

File sharing programs are notorious for bundling with spyware with the main application code. These programs are used by millions of people to download music, movies, software, etc. and the end result is the unauthorized installation of spyware being secretly installed without your knowledge.

2.4 Email

Email is another delivery mechanism of spyware. Email messages with an embedded link/webpage or attachments (i.e. software programs bundled with spyware) can potentially install spyware on your computer. It is also advisable to set your email client to view email messages in text rather than html.

3 Spyware Symptoms

In addition to privacy infringement and information disclosure (i.e. username, password, etc.), the more common effects of spyware include:

- Poor performance; your computer is considerably slower and takes more time to complete tasks or crashes more than usual. This is the number one tell-tale sign that a computer is infected with spyware.
- Change in default home page settings.
- Unexpected tool bars mysteriously appear the browser.
- Search page settings, pop-up and pop-under ads, etc.
- You see pop-up ads, even though you are not on the Internet.
- Available bandwidth is decreased resulting in loss of productivity.
- Being redirected to websites other than the one you typed in the browser.

4 Defence Mechanisms

The most effective defence against spyware is the implementation of a multi-layered approach or defence-in-depth strategy. There is no single technology (hardware or software based) that can provide the perfect solution to the spyware threat. It is the responsibility of each department to achieve an acceptable balance between convenience and security, while minimizing the level of residual risk.

The combinations of the following safeguards are used to greatly reduce the potential spyware threat to information or computer systems.

4.1 Anti-Spyware Software

The most important defence mechanism against spyware is the use of anti-spyware software. There are numerous anti-spyware software packages available on the market today. Most of these commercial products function similarly and operate very much like anti-virus software. Anti-spyware software scans hard drives, the registry, active processes for spyware. Other options include removing, quarantining, restoring removed objects, updating definition files (manually or auto-update). In some cases, you can configure the software to scan removable drives (i.e. USB flash drive). The auto-update feature should be enabled to download the latest definitions. If an auto-update is not built-in to the software, it is advisable to check at least weekly for the latest definitions.

4.2 Anti-Virus Software

Another very important countermeasure is the use of anti-virus software. Anti-virus software is used to scan or analyze memory, boot sectors, system and compressed files, in real time and on command, for the purpose of identifying, isolating and eradicating the presence of malicious code and taking action against it.

Anti-virus software should be installed on all computers that will have access to the network in order to be effective. The process of updating the latest virus definitions is very important for the anti-virus software to be effective in detecting newer viruses and variants. A good practice is to run a full scan on all storage devices, after every update.

Real-time or on-access scanning is essential in preventing detectable threats from infecting the computer system.

4.3 Surf Safely

The best defence against spyware and other unwanted software is to use caution and common sense when downloading software. If there is a need to download content from an Internet website consider the following helpful tips:

- Be aware of the risks; educate yourself.
- Download programs only from websites you trust.
- Read the End User License Agreement carefully before installing any software.
- Be cautious of free file sharing programs, as they are known to install spyware.
- Utilize the security features built-in to your web browser. For example, in Internet Explorer, set the 'Internet Zone' security setting to at least Medium Level. Other settings can be activated to prompt the user before JavaScript applets or ActiveX controls are run or installed.

4.4 Patch Management

Patch management is another very important defence mechanism in preventing malicious threats from infecting computer systems. To have an effective patch management process, organizations need to keep abreast of the latest vulnerabilities as they are publicized, quickly evaluate the risk to help determine if further action is required, and take immediate corrective action as necessary.

Most major software vendors often publish a summary of their own threat risk analysis, assign a severity level to the vulnerabilities, and outline the corrective action that is required if any. Third party information sources (i.e. PSEPC, SANS, etc.) should also be considered as valuable reference as they may provide a more in-depth analysis of the threat and a more objective assessment of the potential risk.

In the past, the mean time between the announcement of a vulnerability and development of an exploit was significant compared to what can be expected at the present time. Today, this mean time has decreased significantly and zero-day exploits continue to increase. Therefore, the risk of a devastating attack resulting from the exploit of a particular vulnerability is greater soon after the vulnerability has been disclosed. To ensure the greatest return on a patch management solution, all critical software patches should be analysed and applied by the organization as soon as possible after they are made available by the vendor.

5 Security Awareness

Security awareness training helps to provide the end-user education regarding the many aspects of security and safe computing practices. Security awareness efforts are designed to change behaviour or reinforce good security practices.

With the spyware threat only a few years old, organizations should begin by increasing user awareness that spyware exists and familiarizing them with the ways that spyware propagates and the potential danger that it poses to an organization. The next step is educating them in the signs and symptoms of a spyware infestation.

Spyware represents a significant threat to computing and networking, ranking high with spam, worms and virus attacks as potential security risks. Organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment without ensuring that all people involved in using and managing information technology know their roles, understand the organization's IT security policy, procedures and practices.

Users should also have an understanding of the counter measures their government department is taking to prevent and protect against spyware. They must also be made aware of their responsibilities in preventing spyware attacks. Policies concerning the requirements and proper use of anti-virus / anti-malware software, desktop firewalls, intrusion detection/prevention systems should be accessible to all employees and/or contractors using departmental information systems. However, having a policy in place is only as effective as the department's willingness to monitor compliance and implement sanctions against policy violation.

There is a wealth of information available on reputable websites (i.e. SANS, Microsoft, eWeek, etc.) in relation to the spyware threat. Similar to other forms of malicious code, spyware and adware threats are evolving quickly as creators of spyware and adware continue to discover new methods to infect users.

At the time of this publication, the following web sites are useful resources for guidance on spyware:

<http://www.spywareinfo.com>

<http://www.pcpitstop.com/spycheck/default.asp>

<http://www.spywareguide.com/index.php>

6 Conclusion

The spyware threat continues to evolve and the methods used to infect systems are becoming more sophisticated. IT security coordinators, system/LAN administrators should be constantly vigilant on all

spyware threats, keeping users informed on these and all other types of threats. As described in the Government Security Policy, the proper safeguards must be installed to preserve the confidentiality, integrity, and availability of information systems.

Similar to the virus threat, the most effective defence against spyware is to have a multi-layered (defence-in-depth) approach, such as installing and regular updating of anti-virus and anti-spyware software,. In addition, Intrusion Detection Systems (IDS), firewalls, security-hardened browser security, and an effective patch management solution all contribute to decreasing the spyware threat.

Regular security awareness sessions benefit both the employee and the organization. The purpose of security awareness sessions is simply to focus attention on security and allow individuals to recognize and respond to current IT security concerns (i.e. spyware, viruses, spam, etc.).

Although it is not possible to eliminate all spyware threats, with increased knowledge and the implementation of the appropriate defences, these threats can be significantly reduced. There are numerous websites that are excellent sources of information (type of spyware, removal, quarantining, anti-spyware software, etc.) on the spyware threat. With more and more services offered through the Internet, system users must practice good security.

7 Glossary

Access control: The process of limiting access to information system resources only to authorized users, programs, processes, or other systems.

ActiveX: ActiveX is a model for writing programs. ActiveX technology is used to make interactive web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the web page.

Adware: A form of **spyware** that collects information about the user in order to display advertisements in the **web browser** based on the information it collects from the user's browsing patterns.

Browser hijackers: Browser hijackers are malicious programs that change browser settings, usually altering designated default start and search pages. But some, also produce pop-up ads for pornography, add dozens of bookmarks -- some for extremely hard-core pornography websites -- to Internet Explorer's Favorites folder, and can redirect users to porn websites when they mistype URLs.

Cookies: A small text file that is stored on the user's browser by the Web server. Cookies may include information such as registration identification, password, user preferences, whether a user has visited the site, etc.

Defence-in-depth: A security approach used to ensure that every system on the network is as secure as possible. You put up as many defences (i.e. firewall, anti-virus and anti-spyware software, etc.) as possible.

JavaScript: A scripting language developed by Netscape that enable Web authors to design interactive sites.

Key loggers: A program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker.

Malicious Code: Software designed or distributed with malicious intent. The term is used to broadly encompass various types of threats such as Trojans, worms and viruses.

Spyware: Computer software that gathers information about a computer user without the user's knowledge or informed consent, and then transmits this information to an external entity -- usually one that expects to be able to profit from it in some way.

Trojan or Trojan horse: Malicious software disguised as legitimate or desirable application. Usually, this type of threat does not self-replicate, but is instead distributed deliberately.

Virus: A computer virus is “a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself.

Worm: A worm uses the network to spread from computer to computer. It resembles a virus in that it self-replicates, but it does not necessarily require human intervention in order to propagate.