Guideline for Prevention of Spyware and other Potentially Unwanted Software

Introduction

Most users are aware of the impact of virus/worm and therefore they have taken measures to protect their computers, e.g. using Anti-Virus program. However, spyware and other potentially unwanted software are commonly overlooked. They are programs which sit quietly on the system and steals information. They are much less visible than virus and worm. So, the actual number of this kind of infection must be much greater than the figures reported.

According to the statistics of incident reports received by Hong Kong Computer Emergency Response Team (HKCERT) in 2005, there are 880 reports on spyware infection, which is more than that on virus/worm (see Fig. 1). It shows that spyware has become another pre-eminent security threats to computer systems.

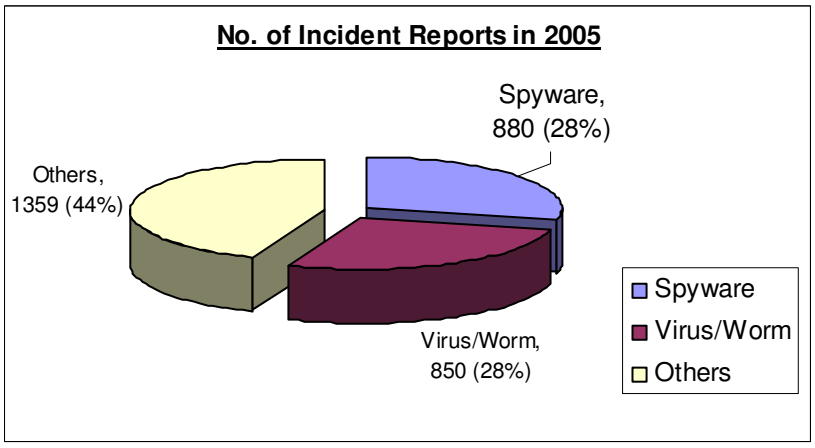

Fig. 1: Number of Incident Reports in 2005 by HKCERT

What are Spyware and other Potentially Unwanted Software?

Spyware and other potentially unwanted software (spyware and PUS) are unwanted computer programs which can be installed on the computer without your knowledge or consent, with a threat of information leakage. They are different from virus or worm which targets on massive attacks and performs visible destructive actions to hosts and networks. Spyware and PUS are sometimes just secretly hidden in your computer and may not be easily detected by system protection software such as Anti-Virus programs.

The main function of spyware and PUS is to collect information in a computer or an opening network and send it back to a third party through network channel or the Internet. The information could be a file in your hard disk or personal data such as login name and password you typed in an e-banking website.

Types of Spyware and PUS and Their Threats

The term "spyware and PUS" actually represents a subset of **malicious programs** (sometimes called **malware**). It usually describes two types of program: Adware and Information Theft Agent.

Adware

Adware is a software package which automatically displays advertising materials on your screen once it is installed in your computer. It delivers advertisements to you from time-to-time and may collect information about your web surfing habits. Some kinds of Adware (also called Browser Hijackers) may even change your browser settings such as default home page of Internet Explorer and default search engine. Therefore, the browser may be automatically redirected to web pages that you are not supposed to visit. Furthermore, the background programs adhered to Adware may consume lots of your system resources and network bandwidth. As a result, the productivity may be reduced when working with the infected computer.

Information Theft Agent

An information theft agent is a malicious program that is installed on your computer without your knowledge and transfers information from your personal computer to a third party through network (e.g. the Internet). It could bring one or more of the following threats:

1. *Information Leakage*
   An information theft agent may look for 'useful' information in the infected computer system. It could be any files or programs such as business plan, source code, financial records, email addresses in your address book and other copyrighted materials. The selected information could be secretly sent to an external party through internal network or the Internet.

2. *Key Logging & Screen Grabber*
   It could be another kind of information leakage. The key logging function inside an information theft agent can log all keystrokes that you interacts with the computer. The captured information, for example, the login name and password you have inputted in an e-banking website, can be sent to a third party without your notice. Although dynamic keypad is implemented in some online transaction websites, some targeted agents could grab the screen of the web page and record the locations of keypad pressed.

3. *Man-in-the-middle Attack*
   Man-in-the-middle attack is an attack that could allow an attacker to read, insert and modify messages between two communicating parties. Both sender and receiver may not notice that the traffic in the communication channel has been observed or intercepted by a third party program (sometimes called a proxy agent). The attacker could also replay a data transmission process with tampered data which could lead to loss of data integrity.

Where do spyware and PUS come from?

Spyware and PUS can get into your computer by various means. The following shows some possible ways that they could infect your computer.

- *Bundled with Untrusted Freeware or Shareware*
  Freeware and shareware (e.g. games, screen savers and P2P clients) can be downloaded easily from the Internet or can be found in free distributed CD-ROMs which are obtained conveniently in computer shopping malls. Most people do not pay much attention on the programs to be installed and do not read the End User License Agreement (EULA) carefully during installation. This gives a chance for bundled malicious programs (including spyware and PUS, virus and worm) to go into your computer "legitimately" and perform harmful actions afterwards.

- *False Anti-Spyware Tools*

  Some programs claim to have capabilities to detect and remove spyware and PUS. In fact, they themselves are spyware and PUS. They may keep asking you to pay for their functionalities after installation. There is no proper way to uninstall those programs. One of the notorious examples is SpyAxe.

  To know the possible false Anti-Spyware tools, please visit:
  http://www.spywarewarrior.com/rogue_anti-spyware.htm#products

- *Installing Harmful Browser Helper Objects or ActiveX Components*

  A Browser Helper Object (BHO) is a plugin for Microsoft Internet Explorer to provide added functionalities. It is loaded when each new browser instance is opened. Yahoo and Google Toolbars are examples of BHOs; ActiveX components allow programs running across network such as the Internet. ActiveX technology provides feasibilities for Microsoft computer systems to operate with each others, for instance, opening a Word or PDF document in a Microsoft Internet Explorer, and accessing information inside a user's hard drives from a remote location.

  Both of them are initially designed for good purposes, however, some malicious parties take advantages of the features and develop spyware and PUS to get benefits from users who have installed it.

- *Faulty Options in Pop-up Windows*

  Some websites use pop-up windows to show advertisements on services or products. The pop-up windows invite users to subscribe or purchase the items. They usually provide "Yes" or "No" buttons for users to select. However, in most cases, clicking either one of the buttons may have the same effect of allowing spyware and PUS to be installed into your computer.

- *Viruses and Worms via Shared Network*

  Viruses and worms can propagate quickly within your home or corporate network. Therefore, they can be used to carry spyware and PUS or as an agent to download spyware and PUS. If your computer does not have enough protection against virus and worm, the chance of being compromised will be greatly increased. A well-known example for this kind of attack is TrojanDownloader and its variants.

- *Running Harmful Files in Email Attachments or from an Instant Messenger*

  Spyware and PUS can be attached with email sent from hackers who impersonate

the identities of your friends or colleagues in the company. You may easily trust the senders, open the email attachments and execute the spyware and PUS. Fortunately, the maturity in email filtering service implemented in most email servers has reduced the probability of this type of attack.

On the other hand, Instant Messengers like ICQ, MSN, Yahoo Messenger become more and more popular but their security is not strong enough at this stage. It leads to a threat that the computer system be contaminated with malicious programs through the use of these tools.

Note:

Once spyware and PUS are installed on your computer, they will try to ensure its operation whenever the system is online. It can be achieved by loading themselves as startup programs or integrating themselves with other startup services or applications. Therefore, knowing where the spyware and PUS from can reduce the chance of their infection.

Symptoms in Infected Computers

The infected computer may have one or more of the following symptoms.

1. The default home page of browser is changed. It cannot be reset or the same page is shown again after re-configuration.
2. New toolbars, menus or buttons are added to the browser.
3. Suspicious web links or folders are added in “My Favorites”.
4. Advertising pop-up windows or strange dialog boxes are shown up occasionally.
5. The browser takes you to a site other than the one you typed into the address bar. For example, it redirects you to a search engine with plenty of marketing information.
6. Unknown program(s) is/are listed in “Add/Remove Programs” in Control Panel or icon(s) is/are found in the task bar, e.g. a date calendar or a weather information.
7. System runs significantly slower than usual. The system takes longer to boot up.
8. Network traffic increases significantly from and to the infected computers, even the system is being idle.

Preventive Measures / Best Practices

1. *Install Anti-Spyware Program*

   There are many Anti-Spyware programs available in the Internet. Some are free and some have to be paid. The following lists three free common tools which are recommended by security professionals.

Name / Download Link	Platform
Windows Defender (Beta 2) http://www.microsoft.com/	Windows 2000(SP4)/XP(SP2)/2003(SP1)
Ad-aware SE Personal Edition http://www.lavasoft.de/	Windows 98/Me/NT/2000/XP
Spybot Search & Destroy http://spybot.safer-networking.de/	Windows 98/Me/NT/2000/XP

   For other trustworthy Anti-Spyware products, please visit:
   http://www.spywarewarrior.com/rogue_anti-spyware.htm#trustworthy

   As new type of spyware and PUS is discovered from time-to-time, it is advised to update the signature file regularly (often this can be done automatically by the Anti-Spyware program), ensure the real-time protection is on and perform scanning at least once a week.

2. *Install Anti-Virus Program*

   As some kinds of spyware and PUS infect computers through virus, it is recommended to install an Anti-Virus program in your computer and keep the virus definition file up-to-date.

   You may find a list of Anti-Virus programs (evaluation version) at HKCERT website:
   http://www.hkcert.org/english/relinks/usefultoolcontent.htm
   Furthermore, HKCERT has a virus prevention guideline at the following location:
   http://www.hkcert.org/english/sguide_faq/sguide/secguide02.html

3. *Keep Your Operating System and Software Up-to-date*

   Perform update for operating system and software whenever relevant patches are available. It mitigates the risk of your computer from being compromised through exploits of known vulnerabilities.

For Microsoft Windows update, please visit:

http://windowsupdate.microsoft.com/

4. *Use Personal Firewall*

A personal firewall acts as a door guard of your computer. It filters out malicious traffics that try to reach your computer over the Internet. For Microsoft Windows XP (SP2) users, a Windows Firewall is already turned on by default.

ZoneAlarm is another Firewall program that supports other versions of Windows:

http://www.zonelabs.com/store/content/home.jsp

5. *Ensure Adequate Security Level for Your Browser*

Make sure that the browser setting is set to at least "Medium" (or "Default Level") for the Internet Zone to avoid downloading unnecessary or malicious programs automatically (see Fig. 2). Furthermore, it is advisable to block pop-up windows which can stop displaying numerous windows with advertisements at the same time (see Fig. 3).

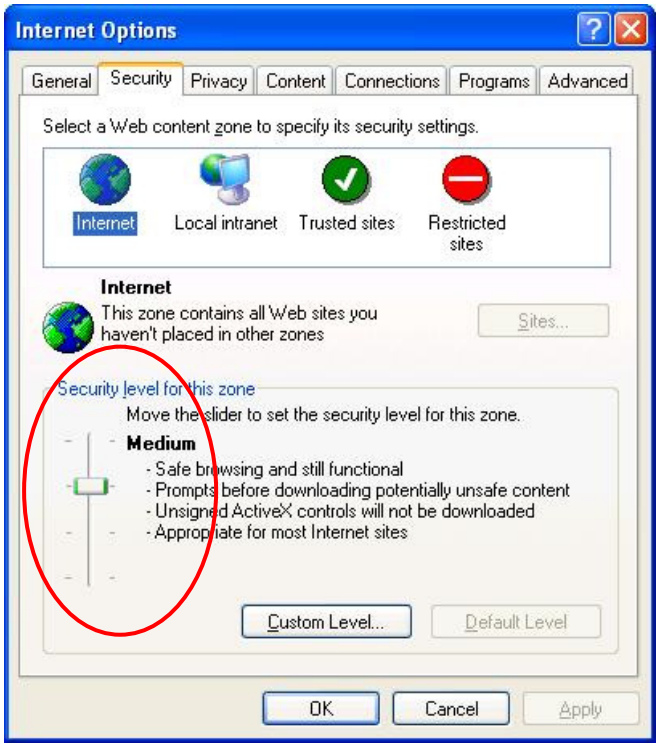

Fig. 2: Setting Internet Security Level in Microsoft Internet Explorer

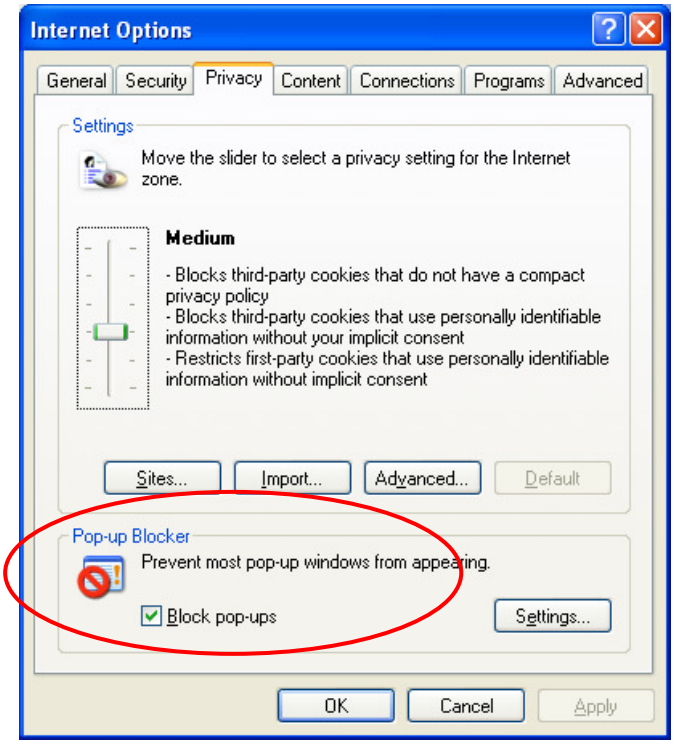

Fig. 3: Setting Pop-up Blocker in Microsoft Internet Explorer

(Note: For other browsers' settings, please refer to the corresponding vendors' user manuals.)

6. *Surf the Internet in a Safety Manner*

(i) Close advertising pop-up windows by clicking the "X" at the top right corner or pressing "Alt" and "F4" keys on your keyboard simultaneously. Do not click the links or buttons (even the button looked like "X" or labeled "NO") inside the window as they may fool you to install unwanted programs.

(ii) Pay attention to security warnings, especially when downloading files or installing ActiveX components, especially those marked "unsigned". (see Fig. 4)

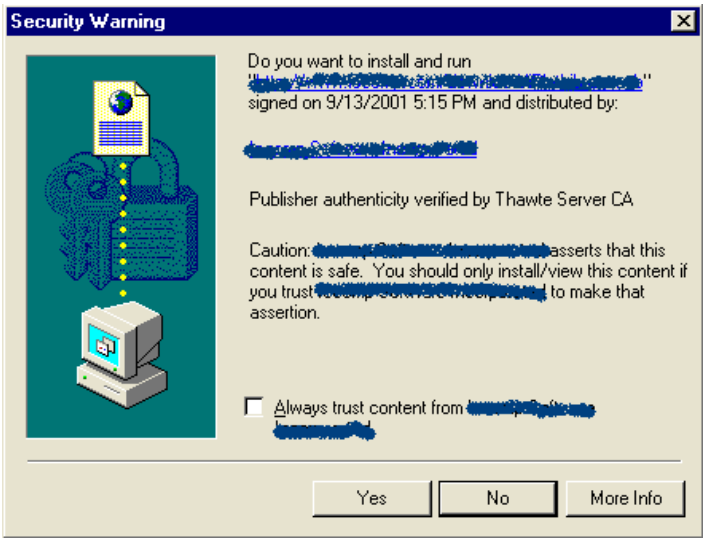

Fig. 4: Security Warning Window

(iii) Read the End User License Agreement (EULA) carefully before downloading or installing any software, especially freeware and shareware. If the EULA is hard to find or difficult to understand, you should think twice about installing the software.

7. *Beware of Executing Files in Email Attachments or from an Instant Messenger*

It is too easy to impersonate an identity on the Internet. Do not easily open files even they are sent from "your friends". If the files are really needed to be opened, it is recommended to scan them using Anti-Virus and Anti-Spyware program before executing them.

References (Technical Papers)

1. *Spyware (US-CERT)*
   http://www.us-cert.gov/reading_room/spywarehome_0905.pdf
2. *The Spyware Epidemic: Dealing With "Legal" Malicious Code (Aladdin Knowledge Systems)*
   http://www.ajoomal.com/descargas/aladdin/esafe/esafe_spyware_wp.pdf
3. *Spyware: an annoying and dangerous problem you can eradicate (Secure Computing)*
   http://www.securecomputing.com/pdf/SpywareSC-TP.pdf
4. *Stopping Spyware at the Internet Gateway: Lessons from Real-World Spyware Attacks (CP Secure)*
   http://www.ccl.co.uk/downloads/Stopping-Spyware-At-The-Internet-Gateway.pdf

References (Websites)

1. *Microsoft Security at Home: Spyware*
   http://www.microsoft.com/athome/security/spyware/
2. *Anti-Spyware Coalition*
   http://www.antispywarecoalition.org/
3. *Stopbadware.org*
   http://www.stopbadware.org/
4. *Spywaretesting.org*
   http://www.spywaretesting.org/metadot/index.pl
5. *Preventing Spyware From GetNetWise*
   http://www.truste.org/articles/preventing_spyware.php
6. *Anti-Spyware Guide*
   http://www.firewallguide.com/spyware.htm
7. *Rogue/Suspect Anti-Spyware Products & Web Sites*
   http://www.spywarewarrior.com/rogue_anti-spyware.htm
8. *Spyware (From Wikipedia, the free encyclopedia)*
   http://en.wikipedia.org/wiki/Spyware