Spyware, Your Hidden Threat

Abstract
Spyware performs activities on your computer without your knowledge or consent. Spyware software uses technology to secretly gather information about a person or organization and gathers and relays information about the user to advertisers or other interested parties. Spyware can:

- Bombard you with advertisements
- Change your computer settings
- Collect personal information and invade your privacy by transmitting confidential information to others
- Slow down or crash your computer system

Spyware may be installed on a computer:

- As the result of the computer user installing a new program
- Visiting a web site and clicking on a link
- From a software virus
- Clicking on an e-mail link
- Downloading files
- Via music and video files

Network Security Audits
Network security audits help organizations identify, manage, and reduce their spyware related risks. They are ideal for ensuring compliance (HIPAA, Sarbanes Oxley, GLB), emerging and fast growing firms, IPO ready organizations, and organizations concerned about security.

Spyware Basics
Programs that are installed with the computer user's knowledge are technically not spyware, assuming the user fully understands what data is being collected and with whom it is being shared. However, spyware is often installed without the user's knowledge or consent. Frequently spyware is installed as the result of downloading a file or as the result of clicking a link or an option in a deceptive pop-up window.

Cookies are a well known means of storing information about an Internet user. Cookies are generally stored on a computer's hard drive and may contain information about the user. Cookies by themselves are generally not spyware. However, if a web site stores information about the user in a cookie without the user's knowledge, the cookie can be considered a form of spyware.

Many organizations have spyware on their computers. Without knowledge of the computer user, the spyware is sitting there, using the computer memory and processor, quietly informing advertisers about the user's Internet surfing habits and

favorite programs. Some forms of spyware may actually change the user's computer configuration and may be almost impossible to remove. Spyware not only invades privacy, it also causes stability issues with the computer's operating system. Spyware can slow computer systems and bring them to a crawl. The most common forms of spyware include:

- Browser hijackers - Browser hijacking is a common way for spyware programs to get visitors to a web site. If a computer user's browser home page keeps changing to an advertisers' web page, the user probably has spyware.
- Search hijackers - Search requests are performed by an unknown search engine that returns results from unauthorized services. Many of the listed sites are run by friends of the spyware community.
- Pop-up windows - The user may see pop-up windows appearing in their browser. Although these windows might advertise mundane products, the user might also be flooded with porn sites that put their employer at risk.
- Key loggers - These utilities track the keystrokes made on your machine. Unfortunately these key logging hardware and software devices may capture Ids, passwords, and credit card information, everything needed for identify theft.

How Do You Know You Have Spyware?

Music sharing web sites (MP3), peer to peer web sites and P2P software, and porn web sites tend to have spyware that can infect computer systems. It is not always easy to know when you have spyware. Some symptoms include:

- Your computer system runs slower than normal.
- Your browser home page has been changed from its default setting. When you manually change the home page, the home page is changed back to some obscure web site.
- When you are surfing the Internet, unknown web sites pop up in your browser.
- When you enter a search term into your Internet search engine, a new and unfamiliar site handles the search.
- New sites are automatically added to your list of Favorites without your knowledge or consent.
- Efforts to manually fix the above are to no avail.
- You get pop-up advertisements that address you by your name.

Spyware Removal

In the future, operating systems and anti-virus programs will be designed to recognize and prevent spyware from attaching itself to your computer systems. Until then, removing spyware from an infected machine can be difficult and should not be attempted without professional guidance.

Spyware scanner software can be used to detect and remove common spyware. Since new spyware is developed on a daily basis, the spyware detection and removal software must be updated regularly. Spyware, anti-virus, and other tools are listed under the Resources section of this paper.

Some spyware and adware programs provide an uninstall program. Check Add/Remove programs to see if an uninstall utility exists for the offending program.

Tips And Techniques

Spyware can be hard to remove and purchasing spyware removal software isn't the only solution. Altius IT recommends the following tips and techniques to protect your information systems from Spyware:

Avoid and protect against spyware

Follow these steps to avoid and protect your systems from spyware:

- Auto updates - Turn on automatic updates to your operating and application software packages. Some spyware programs take advantage of known security flaws. Keeping your systems up-to-date prevents problems.
- Firewall - Use a firewall to monitor and restrict incoming and outgoing Internet activity.
- Browser security settings - Set your Internet security settings to Medium or higher. See 'Additional Protection' below.
- Browser Plug-ins - Say no when installing plug-ins to your Internet browser. What may seem like a harmless application may be spyware.
- Media files - Some Windows Media files may initiate pop-up ads and install adware. Change Windows Media player settings to limit your vulnerability in this area.
- Active X - Set your browser to prompt or disable downloading Active X controls.
- Pop-up blocker - Use a pop-up blocker or configure your browser to block pop-up ads.
- Cookie blocker - Use cookie blocker software and/or configure your browser to block all cookies. Select Tools, Internet Options, Privacy, Setting: Block all cookies.
- Avoid bad areas of the Internet. This includes porn sites, free downloads of copyrighted music, music programs, hacked software, etc.
- E-mails. Avoid phishing scams. Instead of clicking on links, open a browser and manually type in a website's URL address. Manually typing in the URL address will protect you from cross site scripting where a phishing e-mail contains an attack script that places malicious code onto the page of a legitimate website.
- Surfing habits - Close pop-up windows by clicking the red 'X' in the corner, not by clicking OK or Cancel.

- Software installation - Read the software license agreement and don't install any software if you aren't comfortable with the terms and conditions.
- Downloading programs - Only download programs from sites you trust. Check with people you trust or research the software application on the Internet.

Remove spyware

Download the Spyware removal software before you get spyware. Some spyware products prohibit the installation and running of spyware removal software. Install the software before you have problems. Remove suspicious applications. Go to the Add and Remove Programs utility to remove unneeded applications. If you aren't sure what a particular application does, check on the Internet or consult with a computer professional. Use multiple spyware removal packages. One package may not do it all. Check the Resources section of this paper for Altius IT's recommended spyware removal applications and utilities. Temporarily disable the Windows System Restore Process. Windows maintains a backup of important files. In the event something becomes corrupted or damaged, the operating system replaces the file with one from the backup. Some spyware applications are placed in the System Restore area. This allows the spyware to be reinstalled by the System Restore Process if you attempt to remove the spyware. Follow these steps:

- Disable: right click on My Computer, Properties, System Restore, check Turn Off System Restore on all drives
- Spyware removal: run spyware removal software or manually remove the software
- System Restore: re-enable System Restore by following the steps listed above

If necessary, run the spyware removal software in Windows Safe Mode. Some forms of spyware start up when your computer is initially turned on. Spware removal software can be more effective if it is run in Safe Mode. To restart Windows in Safe Mode:

- Restart your computer
- Press F8 as the computer starts up (this may vary depending upon the version of Windows)
- Select Safe Mode
- Run the spyware removal software
- Restart your system

Not all anti-spyware software is alike. Check for the following anti-spyware software characteristics:

- Features - does the anti-spyware software include tools to enhance the removal process? Does the software offer descriptions of detected software? Can the software be updated automatically? Can it be scheduled automatically? Are there undo capabilities?

- Effectiveness - does the anti-spyware software provide real time protection (prevention) or only removal (corrective action)? Is the product effective at finding and removing spyware?
- Ease of use - is the software easy to install and run? Can you quickly and easily find the necessary features? How quickly does it run?
- Customization - can you target selected portions of the hard drive to reduce run time? Can you opt-out of certain features?
- Support - is there live telephone support or are you limited to e-mail support? How quickly does support respond to your questions?

Additional Protection
Not all spyware is spyware. What may seem to be spyware may actually be a virus. Run your anti-virus software on a regular basis. Spyware software presents new and constant threats. Like anti-virus software, spyware removal software needs to be run and updated on a regular basis. Check to see if your spyware removal software has an auto-update feature. If so, turn it on.

Scanning and removing spyware doesn't protect you from future spyware. Spyware prevention programs are an effective way of preventing spyware and adware from infecting your PC. Enhance your security protection by increasing your browser's security settings.

Some spyware is automatically loaded when Windows starts. Computer professionals have the experience to edit your system configuration. By unchecking selected boxes, many of the Spyware programs can be prevented from running.

Some spyware components are browser plug-ins knows as Browser Helper Objects (BHO). BHO's reside in the Temporary Internet Files area. Review and possibly delete BHO's that are spyware. If a browser is open, you may need to Restart the computer then click Start, Control Panel, and Internet Options to get to the same menus without opening Internet Explorer. These steps should be performed by seasoned professionals.

Be careful when installing new software and/or downloading files. Before you install software, read the End User License Agreement to know your risks. Consult a computer professional when dealing with spyware. Computer professionals have the experience needed to protect your privacy and your data.

Keystroke Loggers
Keystroke loggers record your keystrokes as you type on your keyboard. Hardware and software keystroke recording devices capture confidential information with the purpose to transmitting the data to interested parties. Keystroke logging hardware attaches to your keyboard. To retrieve data from a hardware logging device, the person collecting your data must regain physical access to your machine. Hardware

loggers work by storing information in the actual device, and generally do not have the ability to broadcast or send information over a network. Common hardware keystroke logging hardware products include Key Katcher and Key Ghost.

Key Katcher and KeyGhost will most likely not be discovered by anti-spyware, anti-virus, or desktop security software. To detect keystroke logger hardware, the back of the machine must be examined to detect it's presence.

Keystroke logging software records your keystrokes on your computer system. Keystroke logging software can remain completely undetected and starts when the computer is powered on. The keystroke logging software may even record outgoing communications including e-mail messages, documents, Ids and passwords, and credit card numbers. The following is a list of common keystroke logging software programs.

- Amecisco Invisible Keylogger Stealth
- Boss Everywhere
- Ghost Keylogger
- I-See-U
- KeyKey Monitor
- Phantom2
- Spector
- StarrCommander Pro

Altius IT recommends an IT professional be contacted for the safe removal of keystroke logging software. Anti-keylogger and SkyCop are programs that detects keystroke logging software.

Use of Public Computers

Traveling executives and other employees may use public computers at Internet cafes, airports, copy centers, hotel business services centers, public libraries, and other locations. Unfortunately, these computer systems may contain spyware and other keystroke logging software. These software programs may record the user's keystrokes and e-mail the collected information to an unauthorized individual.

Altius IT recommends the following:

- Avoid public computers. If you must use public computers, do not enter confidential information such as credit card or bank account information.
- Check the computer hardware. An unauthorized individual may have loaded unauthorized software by downloading an application from the Internet or installing it from a flash drive.
- Erase your tracks. Browsers keep a record of web sites that you've visited. Before leaving the computer, erase your history (temporary files, cookies, etc.). This won't prevent someone from tracking your activity, but it will make it harder for them.

- Temporary password. Set up a temporary password for your employees who use public computers. Change the password when they return back to the office.

Definitions

- Malware (malicious software) - Specifically designed program to disrupt or damage your systems.
- Trojan Horse - a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.
- Virus - A program or piece of code loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. They may damage your systems by deleting files, corrupting documents, and using the computer's memory and processor.
- Worm - a special type of virus that can replace itself and use memory. Unlike other types of viruses, it cannot attach itself to programs.

Resources

Altius IT recommends a computer professional be consulted when using any of these tools and utilities:

- Ad-aware
- Anti-Key Logger
- Anti-Spam SpamNet
- Anti-virus McAfee or Symantec
- Hijack This
- Microsoft Anti-spyware (Windows Live OneCare)
- Pest Patrol
- Zone Alarm

Summary

Each organization has a unique environment that makes it difficult to protect against new and emerging threats. Network security audits help organizations meet compliance requirements by identifying, managing, and reducing their risks.

Publication Information

Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.