Title:
Spyware: Protect Your Privacy

Word Count:
1875

Summary:
What is Spyware? I have lost count of the number of times that we have been called out to repair a personal computer and found that the system was damaged by "Spyware". Spyware is Internet jargon for Advertising Supported software

Keywords:
spyware, malware, network security, networking security, computer service, computer security, computer spyware, computer malware, computer trouble, virus help, spyware help, computer help,

Article Body:
What is Spyware?

I have lost count of the number of times that we have been called out to repair a personal computer and found that the system was damaged by "Spyware". Spyware is Internet jargon for Advertising Supported software (Adware).

Advertising Spyware is software that is installed alongside other software or via ActiveX controls on the internet, often without the user's knowledge, or without full disclosure that it will be used for gathering personal information and/or showing the user ads. Advertising Spyware logs information about the user, possibly including passwords, email addresses, web browsing history, online buying habits, the computer's hardware and software configuration, the name, age, sex, etc of the user.

In addition to privacy and security concerns, resource-hogging Adware and Spyware can cause system and browser instability and slowness.

Here are a couple of scenarios indicating a Spyware "infection".

- Scenario 1:

Your search engine is New: Google. You visit the Google website and do your search. All of a sudden you have advertisements popping up all over your screen. Annoying right? The Google web site does not use pop-ups! It is against their

company philosophy (another reason why I love Google). So where are the pop-ups coming from? There is software (Spyware) on your PC monitoring your key strokes and hard drive contents and sending the information to a third party on the Internet which then presents advertising pop-ups to you based on your search interests or the web sites you have been visiting.

This scenario illustrates how Spyware can be extremely annoying. But worse, consider the security and privacy issues that are highlighted by this type monitoring. How secure are your passwords that you use locally or online? Is this information being sent back to a server along with other personal or business information scanned from your hard drive? Maybe, maybe not. It is not worth taking a chance. We will discuss how to identify and prevent Spyware from "infecting" your system a little later.

- Scenario 2:

You start your computer in the morning. The PC was never the fastest on the block to boot up and be ready to work but it was never as slow as it is now. Now the computer's hard drive's light stays on continuously and you can hear the hard drive thrashing away in your computer. This abnormal disk activity is a clue that there may be Spyware scanning your hard drive and sending the results to a third party which in turn is using it to aim advertising at you based on your interests.

The second scenario illustrates not only the privacy and security issues mentioned in scenario one, but also the resources that the Spyware appropriates for it's own use. The most noticeable resource degradation is that of the PC itself. Valuable RAM, CPU cycles, and hard disk reads are being used by the Spyware for it's own use. On a slower PC this resource use is very noticeable creating an unusable and unstable PC for periods of time. User productivity is sure to suffer because of this. Network and Internet bandwidth is also being used by the Spyware which results in slower access for legitimate network communications and can result in reduced productivity and higher costs of network ownership.

How to Identify a Spyware "Infestation"

There are some clues that indicate spyware could be installed on a computer.
You are bombarded with pop-up ads every time you use the web browser.
The PC is showing sluggishness and increased disk activity is noticed.
The PC becomes increasingly unstable and more prone to crashes and blue screens.
Icons appear in the taskbar tray that weren't there before.
Network activity is observed when the computer is not being used.

An increase in the amount and frequency of email spam is observed.

There are many freeware titles available that install Spyware on your system. One of the most identifiable types of Spyware is from a company called Gator Advertising(http://www.gator.com/). Their Spyware is installed alongside free programs such as Precision Time, Date Manager, and Offer Companion. You may have seen one or more of these programs after they magically appear in your Taskbar Tray (where your computer clock is displayed). See figure 2-1 and 2-2. Ever wondered how they got there? You're about to find out.
Date Manager tray icon

Precision Time tray icon

How Spyware is Installed

Some Internet websites utilize additional software to enable special features available on the site. One of the most common sites using this technology is the Microsoft Windows Update site. Before installing updates, you are required to accept the installation of a small piece of software called an ActiveX control. Shockwave enhanced sites also require the acceptance of additional software. It is okay to accept this software. Provided that your Web Browser security settings are enabled you will be shown a screen asking permission to install the software. See figure 2-3 and 2-4

Now this is where it gets confusing. Have a look at the figure 2-5 and 2-6 below. Not much difference from the Shockwave and Windows Update Security Warnings shown above. These usually popup when you are first entering a website which gives the impression that they are required in order to view the site. Not so. That's where they get you. Most users will assume they need to install the software, they click <Yes> and the Spyware payload is downloaded to their PC. Other forms of spyware infection are a result of saying OK to offers like the ones shown in Figure 2-7 and figure 2-8.

How to Prevent Spyware "Infection"

The chance of keeping a PC free of Spyware infection is greatly increased by following a few simple rules.

Ensure that your internet browser settings are set to at least default levels. Internet Explorer security settings are accessible by going to the Internet Explorer Tools menu and choosing Internet Options. Go to the Security tab to view or modify the settings.
Read all security warnings before hitting the Yes button. If you are unsure, choose No. If it turns out the webpage to be viewed requires the download, hit the Refresh button on the web browser or use the F5 key to refresh the screen.
Avoid using peer-to-peer file sharing services such as Kazaa. They are notorious for packaging Spyware with their programs.
Check your start menu, desktop, and Add/Remove Programs module for unknown installed applications.
Regularly clean out the internet browsers temporary files and cookie cache. This can be performed from Internet Explorers Internet Options on the General tab.
Whenever possible, close advertising pop-ups using the Close "X" in the top right corner of the window. If there appears to be no way of closing the window without clicking a button within the window, don't. Press the Alt and F4 key at the same time. This will close the window in focus.
Use a firewall product that monitors and prevents unauthorized applications and data from both entering and leaving the PC.
Use Spyware cleaning software such as New: AdAware from New: Lavasoft. Scan for Spyware regularly.
In a corporate environment it is good practice to disable a users ability to install software on the PC.
Educate yourself and other users about what Spyware is and how it can be prevented.
Have your computer examined by a qualified computer technician who can access vulnerabilities and suggest ways of increasing your computer's security.

In Conclusion

There are millions of useful websites on the Internet that survive exclusively due to their use of various forms of advertising. Internet advertising has evolved to the point where it is possible to aim advertising to a very precise target audience. This capability has brought with it a hornet's nest of privacy and security issues.

A lot of the targeted advertising is possible because of Spyware software. Spyware is a tool that provides advertisers with data about a target computer and user. It is often installed accidentally or without the users knowledge. Spyware logs information about the user, possibly including passwords, email addresses, web browsing history, online buying habits, the computer's hardware and software configuration, the name, age, sex, etc of the user, and sends this

information to a third party on the Internet, usually an advertiser.

Advertising pop-ups, system instability, sluggishness, and increased hard drive and network activity are all symptoms of a Spyware "infestation".

To prevent Spyware "infestations" there are some simple rules that a user should follow. They include such things as ensuring that Internet settings are set to at least default settings. The use of a good firewall, which monitors activity both in and out of your computer, can assist in identifying and preventing Spyware. Avoid installing peer-to-peer file sharing software and offers to install software that may pop-up on your screen. Educate yourself about Spyware and how it can be prevented.

For a thorough examination of your system and its vulnerabilities contact a qualified computer technician. They will be able to identify areas of concern and suggest ways to increase your computers security.

Glossary

ActiveX Control - A control using ActiveX technologies. An ActiveX control can be automatically downloaded and executed by a Web browser. ActiveX is not a programming language, but rather a set of rules for how applications should share information. ActiveX controls have full access to the Windows operating system. With this power comes a certain risk that the applet may damage software or data on your machine. To control this risk, Microsoft developed a registration system so that browsers can identify and authenticate an ActiveX control before downloading it.

Cookie - A message given to a Web browser by a Web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. When you enter a Web site using cookies, you may be asked to fill out a form providing such information as your name and interests. This information is packaged into a cookie and sent to your Web browser which stores it for later use. The next time you go to the same Web site, your browser will send the cookie to the Web server. The server can use this information to present you with custom Web pages. So, for example, instead of seeing just a generic welcome page you might see a welcome page with your name on it.

Shockwave - A technology developed by Macromedia, Inc. that enables Web pages to include multimedia objects.

Spyware - Also called adware , spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

For the Full Figured article: click here - Spyware: Protect Your Privacy from ONE IT computer consulting, computer service, networking and network security