

Running head: SPY? WHERE?: UNDERSTANDING SPYWARE

Spy? Where?: Understanding Spyware

Benny C. Rayner

East Carolina University

Abstract

Where is the spy that is lurking on my computer? Spyware is an insidious and crafty computer program. Even though spyware hasn't been around as long as viruses, it is beginning to make its mark with computer security breaches. Spyware can collect personal data from a users' computer. If not taken care of spyware can cause delayed processing of many of your applications. Spyware has begun to cause more problems than viruses. There are many forms of spyware ranging from mild to severe. Since spyware is causing so much grief, laws are being made to prevent companies from taking advantage of people with their spyware. People can fight back for their computer by installing anti-spyware software.

Spy? Where? : Understanding Spyware

Spyware is a pest no matter which way you think about it. Whether it's causing you to have numerous pop-ups or it is consuming all of your system resources; spyware is a menace to be reckoned with. I was a resident computer consultant for East Carolina University for four years, and during that time the majority of the problems encountered pertained to spyware. Some people knowingly install spyware on their computer system because they want particular software and consider it a fair trade-off (Delio, 2005). Regardless if you put spyware on your computer knowingly or unknowingly spyware should be taken seriously.

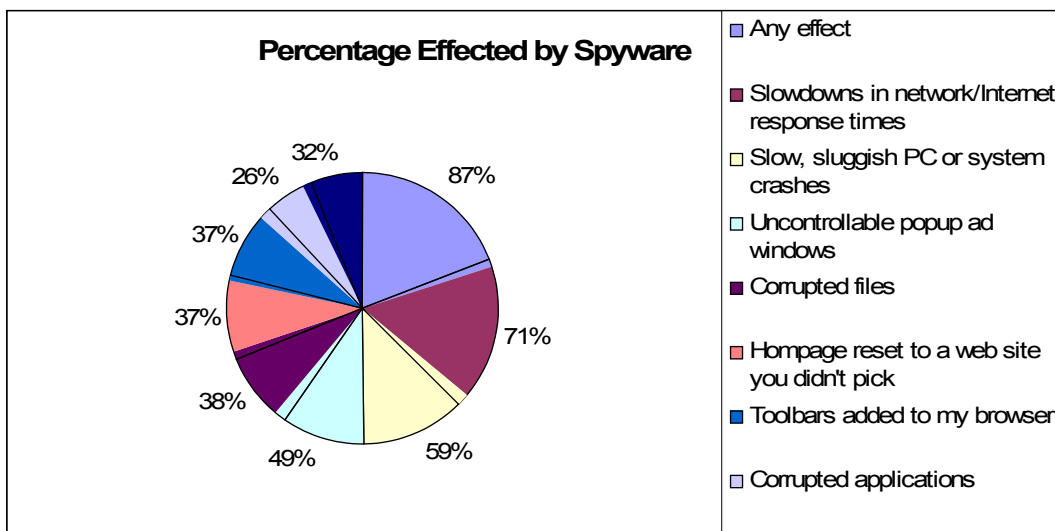
In the past viruses were computer users' main concerns for security breaches. Spyware was around; however, it was not as widely known and was not considered being as much of a problem as viruses. Present day, spyware is beginning to lead the race of computer security concerns. A survey done from a California security company Trend Micro revealed that more than 87% of corporate end users are now familiar with the spyware and 40% has had their personal experience with spyware (Zetter, 2005).

Spyware has come to have many meanings according to Paul McFedries. It is generally defined as any program that secretly monitors a user's computer activities, particularly the typing of passwords, PINs, and credit card numbers (McFedries, 2005). Spyware also harvest sensitive data from the user's computer and then sends that information to an individual or company by the user's Internet connection. This process has become known as back channeling.

Any system exposed to the Internet, using a web browser or e-mail, can become a spyware victim. Symptoms might or might not occur, depending on which form of spyware encountered. Nevertheless, there are some simple symptoms that a user should keep an eye on.

Symptoms of spyware can be subtle and can sometimes be very evident. Chart 1 illustrates the percentage of people whom has been affected by some form of spyware. A symptom that a computer user may notice could be an overall delayed processing of applications, which over time may crash the computer system. According to Microsoft, spyware causes 50% Windows failures (Ames, 2005). For example, a program that normally takes a matter of seconds to process now takes many minutes to process. Most of the time spyware will install other application software, discussed later, which will start up whenever Microsoft Windows run and in turn can cause other software failure. Since all of the spyware programs are starting up, it will have an affect on the processing speed of the computer.

Chart 1: Effects of Spyware



Another evident symptom of spyware is advertisement pop-ups. Computer users should be suspicious of excessive spamming and pop-up advertising. If your browser jumps to new Web sites you didn't specifically request, or adds new browser settings and links, spyware could possible be the blame. If you open your browser window and you are barricaded with pop-ups, more than likely you have adware, which is a form of spyware. Most legitimate pop-ups open over your browser window when you visit a web site. If the website is legitimate, for example

MSNBC or CNN, then the advertiser is usually legitimate and well-known (Pastore, 2005). If the ads you see seem to target you based on the websites that you recently visited or things that you searched for, more than likely this is a cause of adware or spyware.

The primary source of spyware is file-sharing software. Many who download file-sharing software find their computers burdened by piggyback programs, discussed later, that install themselves without the user's consent (Petrick, 2003). Though the software may say that it is 100% spyware free, normally that means that it is 100% spyware. Let's take Kazaa for example. From the Kazaa website (see figure 1) it states that it has no spyware. After installing Kazaa and running Microsoft Antispyware, eight components of spyware were found (see figure 2).



Figure 1: From Kazaa website

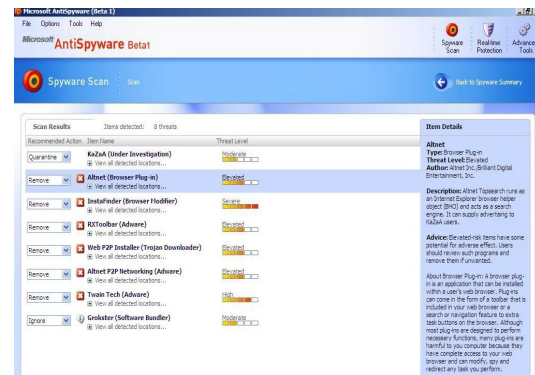


Figure 2: Spyware found after Kazaa installation

Spyware has different levels of destruction ranging from mild to...”hot ‘n spicy.” A mild level of spyware would be an internet cookie within a website that allows a user to reenter the website without entering in their username and password. “This is a form of spyware!? Oh my goodness”! No need to get alarmed over this minor spyware. These are normally harmless and can easily be cleaned by clearing your cookies within your internet browser. Simple cookie identification enables the site to recognize the user when the user returns to the website.

Commercial sites use cookies more readily than government or education sites, though any web page can include them. The Federal Trade Commission (FTC) 2000 survey of commercial websites found that 78% of the top 100 web sites permitted third parties to employ cookies and more than 97% of the sampled sites collected e-mail addresses or other “personal identifying information (Schultz, 2001).” Cookies also allow a site to store information about a user. For example, an Internet shopping site uses a cookie to keep up with how many items are in your shopping cart. Normally a user has recognition that the data that they are allowing the website to have is ok for the site to have so the information is at low risk for the user know that the site is going to store this information. Cookies are not normally referred to as spyware, but some consider it as such because of the user identification and associated data storage that occurs at some sites (Ames, 2004).

The next level of spyware is called associated cookies. These cookies work by identifying a single user each time he connects to any member site. These cookies then track activity and store data gathered from the user’s interaction with each member site. Advertising companies form agreements with the member sites, which allow these advertisers to place references on the site. These references cause the user’s browser to travel to the referenced spyware site and attempt to acquire the reference. Once there, the spyware site looks for a recognizable cookie on the user’s system. Finding none, it sends one with a unique ID called a globally unique identifier (GUID) that identifies the user any time he visits a member site (Ames, 2004). If a user types in their name, account, password, or any other personal data, the spyware data server can store that transaction in its master database. The primary goal of the spyware server is to gain enough information for targeted advertising. The server can also gather credit

card information. A person would think that associated cookies were bad enough. Unfortunately it gets worse.

The last level and by far the worse and most harmful is the infamous application-based spyware. Application-based spyware can cause severe security breaches. The main problem of application-based spyware is that the user has no control over it. The spyware itself is in control of the computer system. It can start itself when it wants to start and it can stop itself when it wants to stop. It can cause other programs not to start and make browsing the Internet almost impossible. These applications can query the system for any desired data and can transmit anything and everything from the users' computer system to an outside source. Associated cookies, discussed previously, transmit user data also, but application-based spyware does not have to wait for the user to share the data with a member site. Application-based spyware can open a receiving channel to accept upgrades for the spyware, install new applications, and generate advertising, all without any permission of the user.

Application-based spyware is installed many ways. Three of the most common methods for sneaking application-based spyware onto a system are piggybacking on desired applications, installing a utility program, and executing Java or ActiveX.

Piggybacking on a desired application is spyware that attach onto a desired program that a computer user download. The spyware loads when the application loads, and the activities of the spyware remain hidden to the user. Once activated, the spyware application configures itself to run without knowledge or intention.

The second common way spyware gains control of a system is to offer utility services within the spyware itself. These programs offer services such as storing and retrieving

passwords, accounts, addresses, and phone numbers. In addition to performing these tasks, these utility services install software that can operate with complete freedom in your system.

Using a Java or ActiveX Web site application is the third method of transferring application-based spyware to a user's system. Once activated, the Java applet or ActiveX code can download and invoke the spyware. The result is the same as in the previous two methods, but these occur completely without a user's knowledge. This type of spyware gain is the most offensive form of installation and is normally how hackers break into a private company's computer system.

Spyware and viruses both run malicious code and can also, if left on the computer system long enough, crash the computer. One may wonder from what is difference between viruses and spyware. In identifying the difference between spyware and viruses one has to look at five questions.

Who creates spyware and viruses? When viruses are created they are normally created by one person sitting alone in a basement or apartment trying to prove something to themselves or someone else. Spyware is normally created by a team of people. Surprisingly enough they are sometimes done by companies that think that they are doing nothing wrong.

Why are spyware and viruses created? Viruses are normally created for bragging rights. Sometime the virus is created by the person to boost their ego. Maybe the person wanted to see if they could exploit the vulnerabilities of particular software. Spyware is normally created for profit. They get into it primarily to sell information about data that they have collected from users. They're mainly driven by the financial reward. Advertising agencies are the main companies that profit from spyware.

Table 1: Viruses vs. Spyware

	Viruses	Spyware
Who creates it?	one person	A team of people
Why is it created?	Bragging rights ; exploit software	Profit
What constitutes it?	identifiable	Debatable
How is it spread?	Primarily e-mail	Web browser
Legal sanction?	settled	Chaotic

What is the amount of knowledge that people have for viruses and spyware? People normally understand what a virus is. There is a broad consensus of what a virus does. When it comes to what constitutes spyware, one person may say that this is spyware and another may say it is only a feature of the web browser.

How are both of these spread? Viruses are mainly spread through e-mail attachments. You may get an e-mail from an unknown source that has an attachment. Once the attachment is open the virus infiltrates the computer. Spyware is mainly spread through your web browser involving the use of cookies and other browser components.

What is the legal situation with both? Viruses have been around long enough and there have been many incidents of it. It is illegal to create and use it against a person or company. The legal aspect of spyware is chaotic, however, beginning to be settled. In certain cases people have been prosecuted for the use of spyware and other cases you can not find a statute to prosecute the person for the crime. House of Commerce Committee chairman Joe Barton stated “To my mind, invading a personal computer is no different than breaking and entering a person’s home. Those who do it are crooks, if not strictly burglars...I want the FTC to go after them with a vengeance (Grebb, 2005).” The US Federal Trade Commission (FTC) recently sued an Internet marketing organization for infecting consumers’ PCs with spyware (Stern, 2005). Seismic Entertainment Productions developed a design that seized control of PCs nationwide.

Seismic Entertainment then infected them with spyware and other malicious software, bombarded them with pop-up advertising, exposed the PCs to security risk, and caused them to malfunction, slow down, and at times, crash. Seismic then offered the victim an “anti-spyware” program to fix the computers and stop the pop-ups and other problems.

Many Internet service providers (ISP) such as Comcast, Verizon, and America Online are providing security measures to ward off spyware (Calem, 2005). Besides ISPs filtering your e-mail for embedded viruses and spyware, they are also offering free or low-cost security software that users can download directly to their computer.

Comcast offers PestPatrol which is an application that detects spyware, adware, keyloggers, browser hijackers, and remote access trojans. The program offers free automatic pest updates, on-demand and scheduled scanning, and active protection, which monitors your computer in real-time to immediately destroy any suspicious activity. This is offered as part of the Comcast Toolbar.

Verizon offers free computer security tools through its portal partners, MSN and Yahoo!, as well as premium subscription service called Verizon Internet Security Suite (Calem, 2005). The service is run within a web browser, constantly monitors your computer, and includes anti-spyware, anti-virus, and an ad blocker.

Recently America Online launched AOL Spyware Protection (ASP) 2.0. The program is free for public use and has multilevel spyware protection. These levels include minute-to-minute, every 15 minutes, daily, and weekly spyware protection.

If the ISP that you are with does not offer any type of spyware protection, fortunately there are programs that you can download for free to rid your computer of 90% of all spyware (Tittel, 2005). Spybot Search & Destroy, SpywareBlaster, Lavasoft Ad-Aware SE Personal

Edition, and Microsoft Windows AntiSpyware are commonly used spyware removal tools. If you are debating on which one to try, I would use them all for what one anti-spyware does get remove, another anti-spyware program will.

Spybot Search & Destroy is a free spyware checker that is very fast and reliable. If you don't mind being interrupted on occasions, it has a feature called Tea Timer that will alert you about any suspicious activity. It will warn you immediately if a program is trying to change anything in your registry. Activating Tea Timer can help you identify and isolate the source of your problems.

SpywareBlaster is not a scanner, but a roadblock to keep a huge range of spyware from getting into your system. It can be thought of as an advanced version of Tea Timer with Spybot Search & Destroy. You only need to run it once to get the blocking effect. SpywareBlaster would best work beside of a browser such as Mozilla Firefox. This powerful browser locks out many spyware breaches with its default configuration and can be made even more robust by settings for it from SpywareBlaster.

Lavasoft Ad-Aware SE Personal Edition is free for personal use, however, requires a fee for commercial use. It's thorough, but slower than Spybot Search & Destroy. You would probably want to leave this running overnight if you've either never used it before or haven't used it in awhile. Ad-Aware seems to go deeper into the registry and file structures, so it sometimes catches things the other checkers miss.

Out of all the anti-spyware programs mentioned, the most powerful one would have to be Microsoft Windows Antispyware. This program digs deep into the registry finding keys that Ad-Aware couldn't find. The program constantly monitors your computer system letting you know of any suspicious activity, similar to Spybot. Microsoft AntiSpyware was originally GIANT

AntiSpyware which require a fee to use. Microsoft, by the end of 2004, was in need of an antispyware application to battle spyware in its own platform acquired GIANT software.

Before using any of the anti-spyware software always check the program of updates. If you constantly use the program without updating the spyware definitions, you will be fighting a losing battle. Spyware are like viruses. Everyday seem to bring about a new form of spyware and if your anti-spyware program is not up-to-date then the new spyware will have a safe haven on your computer system.

Watch out for similar names to the listed anti-spyware programs. Several products try to fool people into thinking they are using an anti-spyware program, which in turn are spyware themselves (Harrison, 2004). When looking for anti-spyware or anti-adware software, you should always check (Calem, 2005):

- Whether the program continuously scans for malicious code or requires the user to do a manual scan.
- Whether it detects malicious code only when the malicious code is running or while the malicious code is dormant.
- Whether the program gives users the option to keep desirable adware, such as a peer-to-peer file sharing program.
- Consumers also should check whether the software vendor offers free customer support.

In conclusion, as stated before spyware is a force to be reckoned with. Many people think that they are safe from spyware and think that their computer system is spyware free while in actuality they have some shape or form of some type of spyware and/or adware. The only safe way to know that you are free from spyware is to download a “legitimate” spyware program and run a full system scan, preferably in safe mode. Safe mode would be best to scan for spyware for sometimes spyware can hide from the anti-spyware software when done in the regular windows environment. Maybe one day we will not have to worry about spyware, which is highly

unlikely. In the mean time, watch what you download and the websites that you go to for spyware is lurking in ever crevice.

References

- Ames, W. (Sept.-Oct. 2004). Understanding spyware: Risk and Response, *6* (5), 25-29.
- Calem, R. E. (2005, October 15). *Stalking your identity; Latest wave of spyware steals personal information*, p. 01.
- Delio, M. (2004, December 6). Retrieved November 19, 2005, from Spyware on My Machine? So What? Web site: <http://www.wired.com/news/technology/0,1282,65906,00.html>
- Grebb, M. (2005, March 10). Retrieved November 21, 2005, from Revised Spyware Bill Moves Ahead Web site: <http://www.wired.com/news/politics/0,1283,66848,00.html>
- Harrison, W. (Nov.-Dec. 2004). User Confidence--and the Software Developer, *21* (6), 5-8.
- McFedries, P. (2005). Technically Speaking: The Spyware Nightmare, *42* (8), 72.
- McLaughlin, J. (April-June 2001). I Spy With My Little Eye. *WebNet Journal*, *3* (2), 54.
- Pastore, M. (n.d.). Retrieved November 14, 2005, from Symptoms of Spyware and Other Pests Web site: <http://www.intranetjournal.com/spyware/index.html>
- Petrick, J. (2003). Beware of 'spyware'; It's a hidden risk of file-sharing programs, 05.
- Schultz, N. W. (April-June 2001). On Cookies & Academic Privacy. *WebNet Journal*, *3* (2), 38.
- Singel, R. (2005, July 12). Retrieved November 21, 2005, from Giving New Meaning to 'Spyware' Web site: <http://www.wired.com/news/privacy/0,1848,68167,00.html>
- Stern, R. H. (Jan.-Feb. 2005). FTC cracks down on spware and PC hijacking, but not true lies, *25* (1), 6-7.
- Tittel, E. (2005, May 25). Retrieved November 20, 2005, from Spyware vs. viruses: Two different fights Web site: http://searchsmb.techtarget.com/columnItem/0,294698,sid44_gci1085980,00.html
- Zetter, K. (2005, October 17). Retrieved November 14, 2005, from Spyware: What You Need to Know Web site: <http://www.wired.com/news/print/0,1294,68275,00.html>