



NewNet 66 Network Security

Spyware... Understanding the Threat

What is Spyware?

Spyware is an evolved term. In the mid 90s, it was used to refer to high-tech espionage gadgets. By the late 90s, it became a computer security term, when the concern about companies tracking individual computer usage first erupted into a serious issue. By early 2000, it had become an all-encompassing term; it was used broadly to refer to software that delivers ads, programs that silently install, applications that are tough to get rid of, or remote access tools that lock a person out of his or her own computer. Since then, the term has continually gained notoriety.

So really, what is it?

Spyware can be understood on two levels. First, it is a general term, ranging from applications that may upon installation carry harmful programs, to downright malicious programs like Trojans and dialers.

Second, it is conceptually defined as an application that affects a user's privacy, performs surveillance, or poses significant harm without appropriate consent in proportion to that harm.

Is Spyware profitable? (You bet it is!)

To gain a clear understanding of how companies make money using spyware read the article located at the link below. While this article was written in November of 2003, it's accuracy regarding the monetary value of Spyware is still valid today.

<http://msnbc.msn.com/id/3541497>

IT surveys from many companies around the globe have determined that Spyware falls into three categories. Percentages may vary but the magnitude of the threats are still the same.

Severe Threats - 15% of spyware threats send private information gathered from the end user currently logged on to the infected system: logging the user's keystrokes, logged-on user name, hash of the administrator passwords, email addresses, contacts, instant messengers login and usage, and more.

Moderate Threats - 25% of spyware sends information gathered from the victim's operating system, including the computer (host) name, domain name, logs of all processes running in memory, installed programs, security applications, client's internal IP address, OS version, the existence and versions of service packs and security updates, TCP ports the spyware is listening to, computer Security Identifier (SID), default browser's homepage, browser plug-ins, etc.

Minor Threats - 60% of spyware transmits gathered commercial-value information about the end user's browsing habits. This includes keywords used in search engines, browsing habits and ratings of frequently visited websites, shopping reports etc.



The Signs of Computer Spyware

Recognizing the signs of spyware infection on your computer is an important step in securing your interests.

These signs include:

1. Significant increase in network activity
2. Significant decrease in PC performance
3. Strange, dialog boxes, asking suspicious questions
4. New modem dialup connections
5. System instability
6. Excessive pop-up windows
7. Website re-direction
8. New toolbars, menus or buttons
9. Persistent homepage address changes
10. Default search engine change
11. New taskbar icons
12. New items in Favorites
13. Excessive hyperlinks added to webpages

What does Spyware do when it infects your machine?

Spyware can do any number of things once it is installed on your computer.

At a minimum, most spyware runs as an application in the background as soon as you start your computer up, hogging RAM and processor power. It can generate endless pop-up ads that make your Web browser so slow it becomes unusable. It can reset your browser's home page to display an ad every time you open it. Some spyware redirects your Web searches, controlling the results you see and making your search engine practically useless. It can also modify the DLLs (dynamically linked libraries) your computer uses to connect to the Internet, causing connectivity failures that are hard to diagnose.

Certain types of spyware can modify your Internet settings so that if you connect through dial-up service, your modems dials out to expensive, pay telephone numbers. Like a bad guest, some spyware changes your machine's firewall settings, inviting in more unwanted pieces of software. There are even some forms that are smart enough to know when you try to remove them in the Windows registry and intercept your attempts to do so.

Below are some examples of how spyware gets into a computer.

So how did it get into my computer?

Spyware usually gets onto your machine because of something you do, like clicking a button on a pop-up window, installing a software package or agreeing to add functionality to your Web browser. These applications often use trickery to get you to install them, from fake system alert messages to buttons that say "cancel" when they really do the opposite.

It is very important to remember that you can get spyware by visiting many web sites you trust and visit frequently. You don't have to visit a site "you shouldn't have" to get spyware!

Piggybacked software installation - Some applications -- particularly peer-to-peer file-sharing clients -- will install spyware as a part of their standard install. If you don't read the installation list closely, you might not notice that you're getting more than the file-sharing application you want. This is especially true of the "free" versions that are advertised as an alternative to software you have to buy. There's no such thing as a free lunch.



While it officially claims otherwise, Kazaa has been known to include spyware in its download package.

Drive-by download - This is when a Web site or pop-up window automatically tries to download and install spyware on your machine. The only warning you might get would be your browser's standard message telling you the name of the software and asking if it's okay to install it.



Internet Explorer security warning

If your security settings are set low enough, you won't even get the warning.

Browser add-ons - These are pieces of software that add enhancements to your Web browser, like a toolbar, animated pal or additional search box. Sometimes, these really do what they say they do but also include elements of spyware as part of the deal. Or times they are nothing more than thinly veiled spyware themselves. Particularly nasty add-ons are considered browser hijackers -- these embed themselves deeply in your machine and take quite a bit of work to get rid of.



Bonzi Buddy is an "add-on" application that includes spyware in its package.

Masquerading as anti-spyware - This is one of the cruelest tricks in the book. This type of software convinces you that it's a tool to detect and remove spyware.



When you run the tool, it tells you your computer is clean while it installs additional spyware of its own.

Network Security.

Now that we have an understanding of what spyware is, how it is used, and how it attacks your computers and networks lets think about network security in K12.

Almost every school district records student information to some sort of server. This information is generally inputed to student information servers by staff members and administrators for reporting purposes.

Let's do some "what if" scenarios.

- 1. What if** - your student information server gets infected with spyware and it's the type of spyware that gathers information on the server and sends it to the bad guys. Your student records are now compromised!
- 2. What if** - your server gets infected with spyware and it's the type that records the administrators username and password. Now who owns your student information server?
- 3. What if** - your server is not protected by a firewall and has become infected by spyware. At this point your entire network is at risk.
- 4. What if** - you allow peer-to-peer file sharing on your network.

The above brings up some important questions that should be addressed by every school district.

- A.** Is a firewall enough and will it protect my entire district? (probably not)
- B.** Is my antivirus software protecting me against spyware?
- C.** How do I really know for sure my district does not have spyware?
- D.** What network tools are in place to protect our student information servers and how do I monitor them?
- E.** What network tools are in place to monitor/report on spyware and other network attacks?
- F.** Is my school district being proactive about network security?
- G.** My school district has network security policies in place. Are they being enforced and if so, how do I know this?

It is not enough to just say that "I have a firewall" or "I have virus/worm software" installed on every workstation. You must **know** that it is working and something **must tell you** when your network has been attacked. Remember; attacks can come from the "inside" or the "outside."

Real World Example.

Below is an example of a school district that has spyware on a workstation in their district. This district has a firewall and the firewall is configured to only allow the users in the school to access the internet using http, https, and a few other services. Spyware has taken over one workstation and the firewall logged the results.

Firewall Logs

Obtaining and implementing a firewall is the first step in preventing spyware and many other network attacks.

Below is a log from a Juniper NetScreen firewall indicating a server or workstation on a K12 network that is infected with spyware. The workstation or server is on IP address 192.168.1.2 and is trying to "phone home" to "the Mother Ship" on the Internet and possibly send confidential information. Note that the attempts were stopped by the firewall as no data was transferred. No **Bytes Sent** or **Bytes Received**.

It is interesting to note where this server or workstation is trying to go. Destinations are in the red boxes.

Date/Time	Source Address/Port	Destination Address/Port	Translated Source Address/Port	Translated Destination Address/Port	Service	Duration	Bytes Sent	Bytes Received
2006-03-05 10:39:14	172.16.1.2:1601	205.251.29.152:6348		Rogers Cable Inc, USA	TCP PORT 6348	0 sec.	0	0
2006-03-05 10:39:13	172.16.1.2:1606	205.250.47.21:17424		TELUS Canada	TCP PORT 17424	0 sec.	0	0
2006-03-05 10:39:13	172.16.1.2:1605	201.16.141.37:2061		Companhia, Brasil	TCP PORT 2061	0 sec.	0	0
2006-03-05 10:39:12	172.16.1.2:1602	201.244.219.163:26162		Montevideo, Uruguay	TCP PORT 26162	0 sec.	0	0
2006-03-05 10:39:12	172.16.1.2:1603	205.246.155.97:32718		AAFES/Barracks, USA	TCP PORT 32718	0 sec.	0	0
2006-03-05 10:39:12	172.16.1.2:1601	205.251.29.152:6348		Quebec, Canada	TCP PORT 6348	0 sec.	0	0
2006-03-05 10:39:11	172.16.1.2:1607	203.45.67.55:20213		Canberra, Australia	TCP PORT 20213	0 sec.	0	0
2006-03-05 10:39:11	172.16.1.2:1600	12.205.51.132:28574		Bresnan Com., USA	TCP PORT 28574	0 sec.	0	0
2006-03-05 10:39:10	172.16.1.2:1606	205.250.47.21:17424		TELUS COM, BC	TCP PORT 17424	0 sec.	0	0

In the example above the firewall did stop this workstation or server from "phoning home" however it is very important to understand that the spyware is also phoning home using http which is allowed in the firewall policy. In other words, the firewall stopped some of the attacks but not all.

