

# **Spyware: When You Look at Your Computer, Is It Looking Back at You?**

By Sharon D Nelson, Esq. and John W. Simek  
© 2005 Sensei Enterprises, Inc.

Most computer users have no idea how rampant spyware has become, or how invasive it can be. Would you be surprised, even terrified, to hear that we find spyware on the **majority** of law firm computers we examine? The percentage skyrockets when we examine home computers, which are generally less protected. So do you ever work from home? It is truly frightening to think how vulnerable client data is to spyware. How much does spyware cost? Not much - \$30-\$100 is a common range, a cheap price for a heinous invasion of privacy.

If you've never thought much about spyware, consider this. In a recent survey, 67% of network administrators rated spyware as this year's most significant problem, with viruses running at 23% and phishing running far behind at 10%.

## **What constitutes spyware?**

No one quite agrees, but generally speaking, it is software installed on a computer without the target user's knowledge and meant to monitor the user's conduct. Some spyware will record everything the user does, the sites visited, instant messaging, e-mail, and document preparation. Some spyware is used to gather personally identifiable information like passwords, credit card numbers and Social Security numbers, all useful for those interested in fraud and identify theft. Other spyware programs will hijack your web browser, reset your home page, add toolbars, alter search results or send popup ads that cannot be closed, all intended to hawk some vendor's products.

Spyware has become insidiously clever recently – many programs come with a reinstaller – as soon as you attempt to remove it, it reloads itself. Many forms of spyware hide in Windows files and even mimic the file names so the average user would have no idea that the files are in fact shielding spyware. The latest wrinkle with spyware is that it can turn the infected machine into a spam zombie. This means that your computer is being used as a relay point to send spam messages without your knowledge. This is probably not a law firm's first choice of how to use its computer network.

## **What is adware? Is it spyware?**

Those who are responsible for adware will have conniptions if you tell them their products are spyware, but in fact they usually are, even though they are a lesser form of it. If you click something and agree to install adware, it cannot be classified as spyware.

However, if you (or very likely, your children) want to install a neat screensaver, cool game, or swap music/movie files via a peer-to-peer (P2P) sharing program, chances are that the downloader will never read the user agreement and will simply hit “I agree.” This is how most adware and spyware finds its way into a computer system. Mind you, there are other more insidious ways as well including “drive-by downloads” from web sites, malicious cookies, etc. True adware, however, isn’t meant to steal your personal financial information or monitor your personal shenanigans. Usually it is used to send information to marketers about your surfing and buying habits to assist them in general marketing and to target you in particular, especially with popup ads, spam and their unwelcome brethren.

### **What are some of the indicators that spyware may be present?**

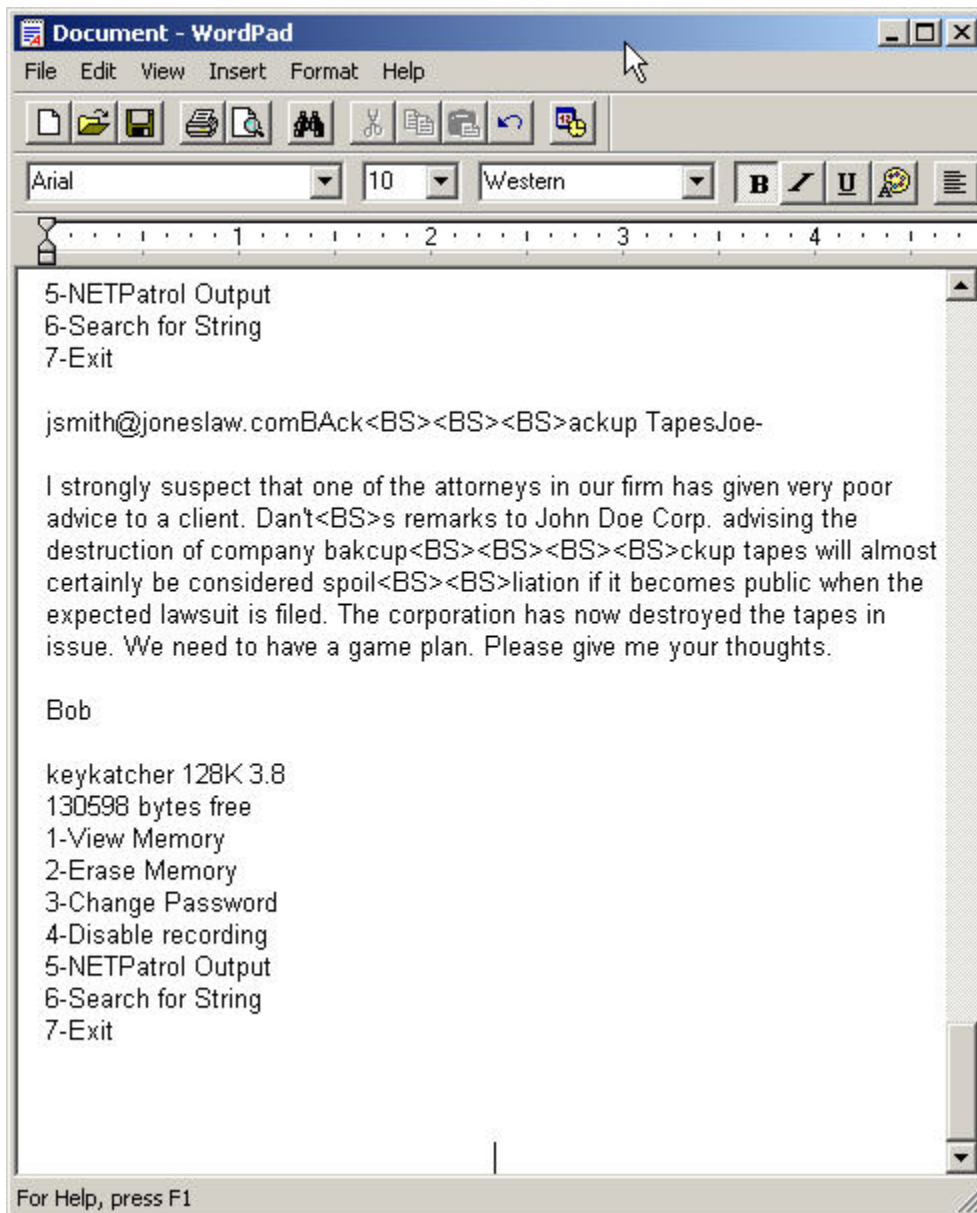
- A sudden proliferation of popup ads
- A change in the Internet home page
- The appearance of new toolbars
- The appearance of new icons in the system tray at the bottom of your computer screen
- Random error messages
- The appearance of new programs in the start-up group
- A marked sluggishness in computer performance
- A sudden tendency of the computer to lock up or blue screen
- Significant increase in hard drive activity

### **Who is likely to have spyware?**

The more correct question is – who doesn’t have spyware? Although studies disagree, it is clear that between 80-95% of all computers have some form of spyware on them. In November of 2004, America Online and the National Cyber Security Alliance released a study in which 77% percent of computer users felt they were safe from spyware. In point of fact, 80% of their systems were infected with spyware. If you look at your computer and think it’s looking back at you, it may well be doing exactly that.

Keystroke loggers (monitoring every keystroke) are much more rare. They seem to have three primary uses: business spying, relationship spying, and monitoring children. Take a look at our sample screenshot from the well known keystroke logger Key Katcher, showing one attorney writing to a colleague in his firm. The image is complete with

misspellings and corrections (BS means backspace), every keystroke having been captured. Imagine the chaos this e-mail could cause if someone were monitoring the lawyer's machine.



## What is the status of laws regarding spyware?

As of January 2005, there is no federal anti-spyware law. Last year, the House of Representatives overwhelmingly (399-1) passed the so-called SPY ACT (The Securely Protect Yourself Against Cyber Trespass Act), but the bill stalled in the Senate, reportedly due to the efforts of lobbyists for marketing groups and software manufacturers. Rep. Mary Bono reintroduced the bill on January 4<sup>th</sup>, and many commentators believe it will be passed this year.

The SPY ACT would require a user's permission before software is downloaded onto a computer. It would prohibit unauthorized software from changing a browser's default home page, changing the security settings of a computer, logging keystrokes and activity, and delivering advertisements that the user can't close without turning the machine off or ending all sessions of the browser. The bill would allow fines of up to \$3 million for those who manufacturer software that would surreptitiously procure personal information from a user's computer. Many spyware functions would be defined as unfair business practices subject to Federal Trade Commission fines.

Attempts to use the federal wiretap act with respect to spyware have not been very successful – clearly, the law needs to catch up to reality.

Among the states, California and Utah enacted legislation designed to outlaw spyware. Antispyware legislation is currently pending in Michigan, Pennsylvania, New York and Iowa. Our own state of Virginia has both a computer trespass and computer privacy statute so spyware is a definite no-no here, even if the computer is a joint family asset. A quick scan of other states revealed similar laws in Kansas, Tennessee, Rhode Island, Washington, and North Carolina. Clearly, attorneys must be cognizant of the laws in their own jurisdiction.

## **How do you combat spyware?**

Among the highest rated antispyware programs are Spy Sweeper, Ad-aware Pro, Spyware Eliminator, AntiSpy, XoftSpy and Spyware Doctor. In addition, Microsoft recently acquired highly rated GIANT Anti-Spyware and has release a beta product. Beware, though, for no one program will catch all spyware. Experts recommend running two or three antispyware programs weekly to maximize your chances of eliminating all spyware on your system. Many of the programs run in the \$30-\$40 range.

Too many people believe they are ok if they have up-to-date antivirus software. Wrong. A lesser number believe they are safe if they've checked the installed programs listing, the add/remove panel, the standard start up area, and they've pressed Control Alt Delete simultaneously on their computer without anything mysterious showing. Also wrong. The entire point of spyware is to cloak itself so that standard methodologies will not detect it.

Besides having good antispyware programs, you want to make sure your operating system and web browsing software are updated regularly in order to close vulnerabilities that may have been patched by the manufacturer. Also, download free software only from sites you know and trust. Read the license agreements of any software you download. Keep your browser security setting at "Medium" or higher to minimize "drive-by downloads." Don't click on links in popup windows – they may contain spyware. Don't click on links in spam, which often carry spyware. Make use of personal firewalls on home machines. Consider changing browsers to FireFox, which will also minimize "drive-by" downloads.

Scared yet? Here's the next step!

## **How do you know if you have spyware on YOUR computer?**

Use the free systems audit at [www.webroot.com/services/spyaudit\\_03.htm](http://www.webroot.com/services/spyaudit_03.htm)

You may be very surprised, even horrified, at the results.

Who's watching you?

*The authors are the President and Vice President of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax) [sensei@senseient.com](mailto:sensei@senseient.com) (e-mail), <http://www.senseient.com> (web site)*