December 2004

# Spyware: The Ghost in the Machine

Tom Stafford
*University of Memphis*

Andrew Urbaczewski
*University of Michigan - Dearborn*

# Spyware: The Ghost in the Machine

**Thomas F. Stafford**
University of Memphis
tstaffor@memphis.edu

**Andrew Urbaczewski**
University of Michigan – Dearborn
aurbacze@umd.umich.edu

## ABSTRACT

Computer users face a new and growing threat to security and privacy. This threat is not in the form of direct attacks by viruses or hackers, but rather by indirect infiltration in the form of monitoring programs surreptitiously installed on users' computers. These monitoring applications are called spyware, and serve to record and transmit to third parties a user's computer uses and behaviors. Frequently used by marketers to harvest customer data for segmentation and targeting purposes, spyware can serve to direct targeted advertising to user's computers. Spyware is, for the most part, legally used, since installations typically come as part of the licensed "clickwrap" agreement that users agree to when downloading free utility and file sharing programs from the Internet. In some cases, spyware is installed as part of legitimate computer applications provide by business to their customers, to provide updating and communicative functionality to application users. But, it appears that the ability to monitor remotely and communicate with computers is an opportunity attractive enough to attract the attention of third parties with non-legal intentions. This tutorial focuses on the roles and functions of spyware, its use in both legitimate and non-legitimate ways, and a range of preventions and protections for avoiding and removing spyware that is installed on end user computers.

### Keywords

Spyware, computer security, privacy, internet, hackers, surveillance

## WHAT IS SPYWARE?

In this tutorial, we seek to educate the audience on spyware, its users and uses, the potential harms, and remedial actions users can take to protect their privacy. Spyware is the name given to the class of software that is surreptitiously installed on a user's computer and monitors a user's activity and reports back to a third party on that behavior (Anon, 2004; Daniels, 2004; Doyle, 2003; Taylor, 2002). Software that performs the sort of user-monitoring that modern spyware is becoming known for existed in many forms throughout the personal computing age (some programs were designed to capture logon ID and password information on mainframe dumb terminals in the 1970's (Ferrer and Mead, 2003)), but it has only become a major concern of the general Internet populace in the last two years, as Internet service companies like AOL and Earthlink declare their concern about software designed to monitor computer user behavior (Anon, 2004). Although many believe that spyware applications are still relatively innocuous and benign (Shultz, 2003), expectations of technology futurists at Gartner are that spyware will soon be the tool of choice for identify theft operations, including password harvesting, and credit card number theft (Radcliff, 2004). Industry experts believe that up to 85% of PC's now have some form of spyware installed and operating (Farrow, 2003).

Spyware can take many forms, including Adware, Browser Hijackers, Dialers, Drive-By Downloads, Scumware, and the popularly known term, Spyware (Mikusch, 2003). A common characteristic of each variant is that they are all designed to install on user computers for purposes that accrue to the commercial, financial, or personal interest of some third party. Adware tracks user Web behavior and targets specific pop-up ads based on the behavior profile and often comes as a surreptitious add-on to popular peer-to-peer file sharing programs like KaZaa, Bearshare, and Limewire. Browser hijackers change the default web page setting on user browsers without permission, and may even make registry changes to prevent you from switching back to your preferred default homepage. Dialers are programs that use a PC's modem to dial numbers that result in expensive toll charges for the user (and handsome kickbacks for the spyware owner), such as 900 numbers, expensive 10-10-xxx access code users, and overseas connections. Drive-by downloads are surveillance applications that install themselves on computers without user knowledge or consent, while scumware changes website content by linking Web page keywords to the site of a third party. Spyware as a specific application (it is also a general term used to describe all of the above) reports on user computer behaviors to a remote server.

Trojans are a major class of spyware whose purpose is to give access to the PC to an outsider (Farrow, 2003). A backdoor is a type of Trojan that allows a remote user full access to the machine at some later point. These are often remote control programs like Back Orifice or SMTP engines that are used by spammers as relays to send e-mail messages. Keystroke loggers are a special type of Trojan that captures every keystroke and records it to a file (Farrow, 2003; Ferrer and Mead, 2003). The most obvious purpose for this type of spyware is to capture credit card numbers, passwords, and other information that a remote user could use for various forms of identity theft.

Web bugs are 1-pixel graphics or cookies that are used by websites to track an individual's computing behavior (Doyle, 2003). These are often hidden in an HTML mail message (to identify if it has been read or not) and to place a cookie on a user's hard drive for future retrieval by the spyware. What makes web bugs particularly nasty is that even the most careful user can become a victim of a web bug simply by reading a message or viewing a web page.

Spyware is often used for monitoring purposes, legitimate or otherwise (Ferrer and Mead, 2003). Commercial monitoring software, as used by businesses to monitor resource utilization, can be viewed as a legitimate systems management application in the business environment, but operates as spyware, all the same. Software applications such as NetNanny, Cybersitter, and WinWhatWhere can be installed by a concerned third party on a user's computer for monitoring purposes. An example might be an employer monitoring computer and network usage on the job, or a parent concerned about a child's computer use. These cases are certainly legal, and generally appropriate. In the case of installation by a spouse or significant other on a shared computer, the legal issues are minimal but ethical issues are significant. This special case of spyware use is considered separate from surreptitious Trojans because the commercial monitoring software that is installed in such cases comes with licensing fees and is usually installed on computers by someone the user knows as opposed to a mysterious third party somewhere on the Internet. Outside of a business monitoring its own resources, and the issues related to jointly owned computers on which spyware may be installed, unauthorized third party spyware installations raise legality issues related to the Federal wiretapping statutes (Farrow, 2003), with the Department of Justice considering unauthorized spyware installations to be a felony offense. The typical method of avoiding prosecution revolves around the common practice of bundling spyware with licensed commercial applications, and including an affirmative installation statement in the "clickwrap" license agreement that comes with the licensed "carrier" application (Schultz, 2003).

## WHO USES SPYWARE, AND WHY?

Spyware can be used by anyone who has a desire to know something about a person and his/her computing habits. Businesses concerned with employee computer use, hackers seeking illegal gains, marketing organizations seeking to enlarge CRM databases for advertising and targeted selling purposes, the government, and even software publishers such as Microsoft, fit this description. For example, Microsoft is known to track computer user music listening habits through the Windows Media Player application, when Internet enabled (Farrow, 2003). The FBI's Carnivore program is a case of legally used spyware, in the name of national security (Ferrer and Mead, 2003).

A primary purpose for the use of spyware in the open market is for market segmentation and audience targeting (Radcliff, 2004). It is becoming increasingly popular in e-business circles to use spyware as a means to gain additional revenues when operating in the online space; businesses are increasingly making the use of spyware to gather valuable customer data a part of their mission (Foster, 2002). Of these, a more prominent recent example is that of Gator (Hagerty and Berman, 2003). This software company promotes bargain search utilities and e-Wallet services, which bring with them a surveillance package that serves to direct targeted advertising at user computers. Though the "clickwrap" license agreement provides the legal cover for the installation of the software, it has not served to protect them from trademark and copyright infringement suits arising from the placement of advertisements that compete with e-commerce Web sites that its users might visit. The Hertz rental car agency has sued over pop-up ads promoting their competitors upon customer visits to Hertz, while Dow Jones and the Washington Post have copyright violation suits pending against Gator (Hagerty and Berman, 2003).

Some businesses use applications that operate like spyware for legitimate purposes, such as providing an active agent on customer computers to check for upgrades and to promote new features of software (Anon, 2004). An example of this sort of usage is found in the Kodak company's inclusion of BackWeb Lite as part of their digital camera imaging software application; BackWeb is one of the "spybots" that popular spyware detection and removal applications routinely identify in computer sweeps, but Kodak specially adapted a version of BackWeb to automate their software upgrade process and for purposes of "pushing" certain camera-related promotions out to consumers. Sometimes the spyware is used by companies for product activation reasons, as with software sold by Quicken, Microsoft, and Macromedia. Along with simple product activation, it can be used to force registration and deliver information about the consumer to the vendor or software coder. This can then be used for a variety of marketing purposes.

Hackers, it is feared, already employ spyware for many reasons, and are likely to do so more frequently in the future (Doyle, 2003; Radcliff, 2004). Some hackers may use Trojans as a means of creating a network of compromised computers to use for a Distributed Denial of Service (DDoS) attack. Others may use the same means for creating a network of computers for delivering spam at a future date. Hackers may also use keystroke logging software to capture personal information, such as passwords and credit cards. The hackers may themselves then use this information for identity theft, or they may sell or trade this information with others so that they may commit similar acts.

## WHAT HARMS MAY SPYWARE CAUSE?

Consumers loathe spyware for several reasons. Not the least of these is the potential for invasion of privacy and the appropriation of personal information surreptitiously by unscrupulous marketers. The pop-up ads that adware versions of spyware generate are rarely popular among the computer users targeted for their attentions. However, there is a more important issue in the specific case of a company using spyware legally (through clickwrap agreement to a "carrier" application) or even in the case of a company seeking to use it for the most objective and positive reasons. Legitimate uses of spyware that are not well written tend to interfere with users' computer functionality (Anon, 2004), since most spyware applications tend to make lots of registry entries (Radcliff, 2004). In the case of Kodak and BackWeb Lite, typical deinstallation of the spyware application with Spybot Search and Destroy (a popular shareware spyware detection and removal tool, found at http://www.safer-networking.org/ ) results in the identification of nearly 60 registry entries. While the spyware can be removed, the registry alterations typically have to be done manually, and can be tedious.

However, the key concern with spyware, privacy aside, is the consumption of computing resources as it runs in the background of PCs. It often runs stealthily, so that the user is not able to detect that an instance of the spyware is running, and the user's first clue that spyware may be running on a system is that the performance degrades considerably for no apparent reason. Tasks which used to take a couple of seconds now may take much longer as the computer waits for resources consumed by spyware to become free. When a user has several instances of spyware running concurrently, then the problem will magnify itself even more. Users then may defragment their hard drives or perform other maintenance still to no avail. Moreover, as tricky as spyware is to detect, it may be even tougher to remove. Removing spyware may cause your Internet connection to fail if it alters the Winsock stack (e.g., Foster, 2002). Removing it may also cause other legitimate software (like the program that it rode along with) to cease functioning correctly. All of the time and frustration encountered leads to serious costs for the users.

Privacy invasion is a more chilling concern. Some, like Sun's Scott McNealy, have told Internet users to ignore potential privacy violations, since there can be no privacy expected online (Wired News, 1999). For others though, it is not so simple. The idea that someone out there is collecting personal information without our permission goes against basic tenets of liberty and freedom that are set out in documents like the US Constitution; certainly, the parallels to the most potent privacy law applicable, the Federal wiretap statutes, are interesting and potentially applicable to unauthorized spyware installations (Farrow, 2003). When keystroke logging is enabled, the privacy concerns escalate to become quantifiable threats to a person's well-being. The threat of identity theft, once thought to be a minor annoyance, is a reality today. Individuals have found their PIN numbers and passwords compromised, credit card and social security numbers stolen, and other identifying information captured by outsiders. These outsiders then use this information to drain bank accounts, apply for driver's licenses and credit cards in others' names, and complete other deeds that are no longer traceable to the real perpetrator. This is one of the fastest growing crimes, and is expected to be even more prominent in the near future, according to the Gartner Group (Radcliff, 2004).

## WHAT CAN USERS DO TO PROTECT THEIR PRIVACY

The leading culprit in spyware transmissions is the free Internet download of a software application; notable examples of popular downloadable applications that carry spyware with them include Bonzi Buddy, Comet Cursor, and Gator (Coggrave, 2003), as well as Xupiter Toolbar, Bargains.exe and a host of peer-to-peer applications that have recently proliferated for file sharing (Taylor, 2002). If downloading applications from the Internet, users should be aware that the "clickwrap" licensing agreement that comes with such software generally will state that the licensing company has the right to monitor your use of the application or to collect personal information for certain purposes, and since a download will not proceed until "I Agree" has been clicked on the license agreement, the download itself serves as evidence that users did give consent for the piggybacked spyware to be installed on their computer. This is the step that most companies take to ensure they are not prosecuted under the applicable statutes that would consider unauthorized installation of such spyware to be illegal. Hence, the best protection is not to download peer-to-peer applications, or any free software one is not familiar with or is unwilling to fully examine, license-wise, before executing a download.

To protect against spyware installed surreptitiously, or for those cases where one simply agreed to the license terms without reading the full text of the agreement, there are numerous removal applications, some of which are also free. Spybot Search and Destroy (http://www.safer-networking.org/) is effective, and is considered to be easier to use than the other alternative, Lavasoft's Ad-Aware (e.g., Foster, 2002). For the Mac user, the best alternative is considered to be the Spring Cleaning application, which is commercially available for around $50.00 (Taylor, 2002).

## CONCLUSION

As with e-mail spam, once a technique is innovated for using the Internet as a commercial tool, or as an aid to fraud, the usage of the technique only increases. We can likely expect far more creative spyware attacks on the privacy of users in the future, along with the increasing number of legal commercial applications that are being developed for customer relationships management purposes. Awareness of the threat is the best protection, since the nature of the threat to computer users will naturally evolve over time. It would appear that the routine sweeping of computers for spyware will be a standard weekly practice that will take place right alongside the virus checks we've gotten so used to in recent years.

### References

1. Anonymous (2004), "Spyware: Spycatcher," *New Media Age*, January 8, 25.
2. Coggrave, F. (2003), "How to Tackle the Spyware Threat," *Computer Weekly,* November 18, 30.
3. Daniels, J. (2004), "Scumware.biz Educates about Dangers of Adware/Scumware," *Computer Security Update,* 5,20.
4. Doyle, E. (2003), "Not all Spyware is as Harmless as Cookies: Block it or your Business Could Pay Dearly," *Computer Weekly,* November 25, 32.
5. Farrow, R. (2003), "Is you Desktop being Wiretapped," *Network Magazine,* 18,8, 52.
6. Ferrer, D., and Mead, M. (2003), "Uncovering the Spy Network," *Computers in Libraries,* 23,5, 16.
7. Foster, E. (2002), "The Spy Who Loves You," *Infoworld*, 24,20, 60.
8. Hagerty, J., and Berman, D. (2003), "Caught in the Net: New Battleground over Web Privacy: Ads that Snoop," *Wall Street Journal*, August 27, A1.
9. Mikusch, R. (2003), "Adware, Spyware – Oh My!" *Beyond Numbers*, 427, October, 16.
10. Radcliff, D. (2004), "Spyware," *Network World,* 21,4,51.
11. Schultz, E. (2003), "Pandora's Box: Spyware, Adware, Autoexecution, and NGSCB," *Computers & Security*, 22,5, 366.
12. Taylor, C. (2002), "What Spies Beneath," *Time*, 160,15, 106.
13. Wired News (1999), "Sun on Privacy:Get Over It," http://www.wired.com/news/politics/0,1283,17538,00.html accessed February 20, 2004.