Webroot Software, Inc.

Technical White Paper

Anti-Spyware: Augmenting Your Current IT Security Strategy

by Douglas J. Hurst

Anti-Spyware: Augmenting Your Current IT Security Strategy

Technical White Paper

Index:

Anti-Spyware: Augmenting Your Current IT Security Strategy

Technical White Paper

"Antivirus software still does an excellent job of protecting against viruses in the wild; however, other products, in association with corporate security policy, are now becoming increasingly important to safeguard the network and critically sensitive corporate data." - Datapro

Executive Summary:

As the landscape of security and privacy threats to corporate networks continues to evolve, IT professionals need to be mindful of spyware. For the purposes of this paper, spyware is defined as software that is surreptitiously installed on a system and that can monitor many aspects of the system, record information, and broadcast it back to the software's creator.

As enabling technologies allow for an ever increasing number of users to connect to corporate networks remotely, and spyware delivery methods become more insidious, users become more vulnerable to exposing their systems to spyware. This susceptibility is making endpoint security a top priority for IT professionals, as each vulnerable PC contains electronic assets and sensitive data that must be protected.

Because remote users may not have the complete security defenses available to them and, unlike viruses, spyware behaves like intentionally installed software, the current suite of corporate security tools and policies (such as Firewalls and Anti-Virus) are no longer enough to contain this emerging privacy and security threat. However, new tools are available to help augment current security efforts. These new tools are spyware detection/removal software, or "anti-spyware."

Webroot's Enterprise Spy Sweeper Edition is an anti-spyware tool created specifically to help IT professionals close the security gap on spyware.

"More than 20 million people have installed adware applications" - GartnerG2

Spyware Defined:

Spyware is any program that allows a user's activities to be monitored without their knowledge. Spyware can record a user's every move, including: web sites visited, documents viewed and created, online buying habits, applications used, email and IM conversations, even personal information such as name, age, gender, credit card numbers, user names and passwords. There are four major categories of spyware:

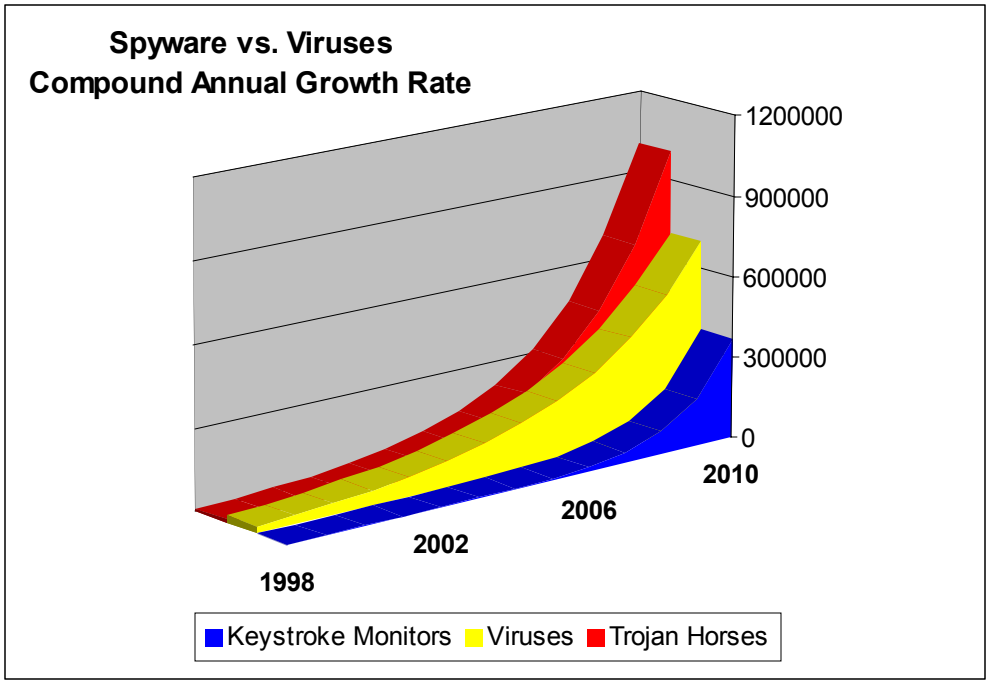
System Monitoring Tools - are applications designed to monitor computer activity to various degrees. These programs can capture virtually everything done on the computer, including recording all keystrokes, email, chat room dialogue, web sites visited, documents opened and viewed, and programs run. System monitors typically run in the background so that the user is unaware of being monitored. The information gathered by the system monitor is stored on the user's computer in an encrypted log file for later retrieval. Some programs are even capable of emailing the log files to another location. Traditionally, system monitors had to be installed by someone with administrative access to the user's computer, such as a system administrator or another individual who shared your computer. Recently, however, there has been a wave of system monitoring tools disguised as email attachments or 'freeware' software products that do not require administrative level access to install.

Adware - is advertising-supported software that displays pop-up advertisements whenever the program is running. This software can usually be downloaded from the Internet for free, and it is these advertisements that create revenue for the sponsoring company. Although seemingly harmless (aside from the intrusiveness and annoyance of pop-up ads), adware can install components onto your computer that track personal information (including your age, sex, location, buying preferences, surfing habits, etc.) for marketing purposes. Most advertising-supported software does not inform users that it installs adware onto a system.

"Spyware growth is exponential and is projected to outpace more traditional threats like viruses within the next few years."

Trojan Horses - are malicious programs that appear as harmless or desirable applications. Trojan horses are designed to cause loss or theft of computer data, and to destroy a user's system. Some trojan horses, called RATs (Remote Administration Tools), allow an attacker to gain unrestricted access to the user's computer whenever the user is online. Attackers can perform activities such as file transfers, adding/deleting files or programs, and controlling the mouse and keyboard. Trojan horses can be distributed both as email attachments and bundled with another software program.

Keyloggers - are programs that can monitor and record the user's every keystroke. Users then risk identity theft as keyloggers can reveal user names, passwords and other confidential information.



Source: FBI, Department of Justice, FCC, Pew Internet Project

"One third of European companies have been infected with spyware applications on their networks" - Emerging Internet Threats Survey 2003

Spyware Delivery Methods:

The surprising fact about Spyware infections is that a majority of the time, users give permission for the software to be installed. Commonly, users simply retain default settings and licenses during software installation, and it is quite likely that spyware has been installed without the user realizing it. This is mainly due to the overwhelming amount of information in the End User License Agreement (EULA), as well as the fact that many of these 'agreements' are ambiguous in nature and designed to be difficult for users to fully understand the implications of agreeing to the license.

Such a cavalier attitude toward EULAs allows spyware creators to bundle their software with another vendor's application. By using the functionality of the primary software to serve as a diversion and by using the ambiguous EULA to cover the legalities associated with installation, spyware publishers are able to slip their software into the average user's computer virtually undetected. One example of this scenario is 'Freeware'. Publishers of these applications are essentially trading the functionality of their software for the rights to sell user information (e.g. browsing patterns, personal records and marketing data) to third-party companies. The most recognizable users of this business model are the peer-to-peer file sharing services such as Kazaa, Morpheus and Grokster.

More insidious spyware delivery methods exist as well. 'Drive-by-Downloads' are HTML links (usually hidden in SPAM), that when clicked on, initiate an automatic download process. Computer viruses can also leave spyware behind long after they have been removed. The Fizzer worm is an example of how hackers can deliver an internet relay chat back door, a denial-of-service attack tool, a keystroke-logger Trojan, an HTTP server and other components all in one worm.

"To properly remove spyware takes a detailed understanding of the spyware itself, how and where its various elements are installed (files, folders, registry entries, etc), and the related dependencies between the spyware elements and any other applications."

Spyware Detection And Removal:

Current firewall and anti-virus technologies are not designed to detect and remove spyware. Firewalls do not stop spyware infections because spyware is commonly embedded in programs that users give permission to download. Antivirus tools fail to detect spyware because spyware does not include the viral mechanisms or behaviors detected by normal anti-virus pattern recognition techniques. It takes a specific, detailed description of the spyware for successful detection and removal to take place.

The spyware publisher business model is predicated on being able to continually broadcast user data and behavior information back to third party companies. This economic incentive has motivated spyware publishers to develop sophisticated techniques to avoid detection and removal. Many spyware programs have been coded to be virtually 'invisible' to end-users and some even include reinstallation or self-repair features to further complicate the removal process.

In addition, spyware often shares functional interdependencies with another free, downloadable product. Often, the 'downloaded application' will stop working if the spyware component is removed. Moreover, simply uninstalling the application will usually leave the spyware components untouched, and reinstalling the application will also reinstall the spyware.

Specific removal of spyware, therefore, requires a detailed understanding of the spyware itself: how and where its various elements are installed (files, folders, registry entries, etc) and the mutual dependencies between spyware elements and any associated applications.

"There are projected to be 29,000 'hotspots' by 2004" - Gartner

"In 2003, laptops will account for greater than 50% of the PC market for the first time and at some-point 75% of these laptops will be connected to a wireless network"

Spyware Infection Scenarios:

Certain environments lend themselves to spyware infections. Some settings in which computer users find themselves at risk for spyware exposure include:

1)Office
Employees may inadvertently download spyware as part of a bundled package including a desired freeware application. Unbeknownst to the employee, the downloaded spyware runs in the background, recording information such as the user's web browsing habits, name, email address and possibly passwords and credit card numbers.

This information is relayed back to the software creators who might use it for their own purposes or sell it to third parties.

2)Remote User at Home or 'Hotspots'
Remote users tend to use their machines more like a personal device and less like a corporate asset when connecting outside the work environment.

For example, users may download popular file sharing programs such as Kazaa, Morpheus or Grokster for entertainment purposes. Part of the downloading process for file-sharing programs typically includes the installation of an adware program. The adware monitors the user's surfing habits and sends targeted pop up advertising based on which sites the user frequents.

The gathered data (minus user identification information) is then sold to marketing or demographic research companies.

3)Kiosk or Internet Cafe Users
In this scenario, users surf computers at local internet cafes, where they may opt to make internet purchases. Prudent users enter secure sights to make sure that their purchase information is encrypted.

However, these machines may have been previously infected with keyloggers, and the shopper has inadvertently compromised his/her identity, passwords and credit card numbers.

"Legislation like the Health Insurance Portability & Accountability Act(HIPAA) require healthcare companies to implement policies and procedures to secure the sensitive personal health and medical information of the individuals they serve."

"For financial institutions, legislation such as the Gramm-Leach-Bliley Act and Sarbanes-Oxley require them to take specific action to protect all information assets, not just customer information."

Threats to the Enterprise:

The emergence of spyware in corporations means that organizations are making themselves vulnerable to unknown outside parties such as competitors, hackers or advertisers. These intruders can gather confidential company information without consent, create worker productivity issues and drain bandwidth resources.

Particularly sensitive are the insurance and financial services industries, as they deal with large volumes of sensitive data, including personal health and financial information. Data protection standards mandated by federal legislation, along with consumer cries for privacy and security, have forced organizations to reassess their current policies to address electronic asset protection. The repercussions of compromised data can extend past federal regulators, and may include liability for violating non-disclosure agreements, compromised competitive advantage, and exposing employees and corporations to many types of fraud.

But the threats of spyware go beyond the risk of compromised intellectual property. Employees have become targeted by marketers through spyware infections. As spyware becomes more sophisticated, marketers are finding it irresistible to use this technology to target advertisements toward people at work, during their most significant portion of time on-line. This invasion during working hours (much like e-mail spam) forces employees to manage these distractions, compromising productivity. And depending on the nature of the infection, many spyware programs have been known to cause system failure and general system instability, leading to larger productivity issues.

Another more subtle problem arising from spyware is bandwidth consumption. Spyware programs continually broadcast information over corporate networks, sapping valuable bandwidth. If companies are not careful, they may throw money at superfluous bandwidth.

Moving forward, IT professionals will need to address these threats as they redouble their corporate security, privacy and Internet policy efforts.

"Spyware threats have become commonplace, and have even outpaced viruses as the number one on-going danger facing on-line PC users today."

Augmenting Your Current IT Security Strategies:

When addressing the spyware threat in a corporate setting, IT professionals should consider several issues when implementing an anti-spyware solution. The anti-spyware software should work in a complementary fashion with the current privacy, security and Internet policies. Also, organizations must ensure the solution meets the demands of the enterprise. Finally, professionals should look for software that is as dynamic in nature as the spyware threat itself.

Anti-spyware like Webroot's Spy Sweeper is designed to work in conjunction with current Anti-Virus and Firewall technologies, thus helping IT professionals round out their overall security effort in a fashion that augments existing strategies.

Most current anti-spyware applications are targeted for the consumer market and thus do not have the functionality to scale well in the corporate environment. Spy Sweeper addresses this issue by providing enterprise-level support for network administrators, giving them the ability to control spyware across the network.

Due to the dynamic nature and the increasing rate in emergence of spyware, it is vital that companies implement anti-spyware solutions that are constantly being updated for the latest spies and running the latest version of spyware detection software. Subscription models like Webroot's Spy Sweeper will keep users constantly secure by delivering:

The Highest Level Protection - Regular updates to spy definition databases offer subscribers the most comprehensive protection available against all the latest spyware threats.

Free Software Upgrades - Automatically receive and download upgrades to the software for the duration of the subscription.

The ramifications of spyware in the corporate environment are significant when considering the effects on worker productivity combined with the threats to network and data security. Anti-spyware such as Webroot's Spy Sweeper can help IT professionals augment their privacy and security efforts by addressing many of the threats created by spyware.

Webroot Software, Inc

Technical White Paper

Webroot Software, Inc. is a leading provider of privacy, protection and performance software for home and business computer users. Founded in 1997, Webroot has focused on delivering peace of mind with innovative software solutions that guard your computing privacy, protect you and your children online, and improve computer performance. Webroot's award-winning software programs deliver powerful, advanced features with interfaces that are quick to learn and easy to use. Best-sellers such as Window Washer, Child Safe and Accelerate have introduced thousands of computer users to Webroot's full suite of privacy, protection and performance solutions for home and office.

For more infromation, Please visit www.webroot.com

WORLD HEADQUARTERS

Webroot Software, Inc.
P.O. Box 19816
Boulder, CO 80308-2816 U.S.A.
303.442.3813
800.772.9383

www.webroot.com

FOR SALES INFORMATION
IN THE U.S., CALL TOLL-FREE
800.772.9383