webroot® Software, Inc.

Privacy. Protection. Peace of Mind.

White Paper

Anti-Spyware Software: Securing the Enterprise Network

Webroot Software, Inc.
2560 55th Street, Boulder, CO 80301

Toll Free: 800.870.8102
Telephone: 303.442.3813
Facsimilie: 303.442.3846

www.webroot.com

Contents:

Executive Summary

Spyware is a categorical name for any program that tracks user's online activities and secretly transmits information to a third party. The effects of spyware range from annoying interruptions, like pop-up ads, to security breaches and loss of intellectual property. The pervasiveness of spyware in corporations today illustrates the extent to which businesses are making themselves and their data vulnerable to unknown outside parties, such as competitors, hackers, or advertisers.

In a recent Earthlink/Webroot Spy Audit report, of 1,483,517 computers scanned, more than 50 million pieces of spyware were detected.

The Internet has proven to be integral in conducting daily business activities, and the advent of enabling technologies increasingly allows for an expanding number of users to connect to corporate networks remotely. At the same time, spyware delivery methods have become more insidious. In a recent sampling of 1,483,517 computers scanned, more than 50 million pieces of spyware were detected.[1] The rapid growth of spyware infections threatens sensitive data while simultaneously consuming network bandwidth, slowing desktop performance, and draining IT resources. Endpoint spyware security is now a top priority.

The current suite of corporate security tools and policies (such as firewalls and antivirus solutions) do not adequately contain this imminent privacy and security threat. A traditional antivirus solution is of little value against many types of spyware because spyware programs do not fit the self-propagating definition of a virus. In addition, the straightforward detection and removal of viruses does not work with spyware as it typically has both good and bad properties and good and bad commercial uses.[2] Not every keystroke logger and browser helper object is installed with negative intentions, but every virus is.

The straightforward detection and removal of viruses does not work with spyware as it typically has both good and bad properties and good and bad commercial uses.

In the last few years, multiple anti-spyware products have been introduced to the marketplace; however, these tools have been designed for desktop users and have not been scalable to corporations. As enterprise anti-spyware products begin to emerge and the spyware threat continues to grow, corporations need to quickly establish a strategy for handling the threat.

[1] http://www.earthlink.net/spyaudit/press/
[2] Peter Firstbrook, "Spy vs. Spy Part One: Understanding the Risks", META Delta 2963, June 15, 2004.

Threats to the Enterprise

With spyware, intruders are able to gather confidential company information without consent, create worker productivity issues and drain bandwidth resources. Particularly at-risk are the healthcare, 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, such as HIPAA and Sarbanes Oxley, along with consumer demands for privacy and security, have forced organizations to realign their current policies to address electronic asset protection. The repercussions of compromised data can extend past federal regulations, and may include liability for violating non-disclosure agreements, compromising 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. As spyware becomes more sophisticated, marketers are finding it irresistible to use this technology to target advertisements toward people at work, taking advantage of users most significant portion of time online. This invasion during working hours, much like spam, can hinder productivity by forcing employees to manage these distractions. Spyware also decreases the productivity of IT support staff, forcing them to deal with unnecessary user support requests. The final solution for many IT departments is to decommission and rebuild computers as they become so riddled with spyware that they no longer function properly.

Often the material displayed by spyware goes far beyond being a mere distraction. Objectionable material displayed by spyware on an unsuspecting user's desktop potentially subjects the user and the corporation to harassment and related claims. Additionally, many spyware programs have been known to cause system failure and general system instability, leading to larger productivity issues. In April, Microsoft estimated that 50% of all PC crashes were due to spyware.[3] In June, Merrill Lynch stated that they understand that close to 25% of Dell's support calls are due to spyware-related system performance degradation.[4]

In April, Microsoft estimated that 50% of all PC crashes were due to spyware.

In June, Merrill Lynch stated that they understand that close to 25% of Dell's support calls are due to spyware-related system performance degradation.

[3] http://www.computerworld.com/securitytopics/security/story/0,10801,92554,00.html
[4] Ed Maguire, Merrill Lynch comment, Security Software: Gartner Security Summit Highlights, June 10, 2004.

A recent study showed that 45% of files located in the popular file-sharing program Kazaa were infected with some type of harmful program, such as viruses, worms, or Trojan horses

Another often overlooked problem arising from spyware is bandwidth consumption. Some spyware programs continually broadcast information over corporate networks, sapping valuable bandwidth that could otherwise be used for legitimate communication. If companies are not aware that spyware is responsible for wasting their bandwidth, they may incur unnecessary expense by purchasing additional bandwidth. Moving forward, IT professionals will need to incorporate anti-spyware solutions into their corporate security, privacy, and Internet policy efforts. The cost of additional bandwidth significantly outweighs the cost of anti-spyware software.

Spyware can Invade Even the Most Protected Networks

A surprising fact about spyware infections is that, in many instances, users inadvertently give permission for the malicious software to be installed. Often, users simply retain default settings and automatically click through licenses during software installation. There is an overwhelming amount of information in a typical End User License Agreement (EULA), and many of these "agreements" are specifically designed to be ambiguous in nature and difficult for users to fully understand.

Cavalier attitudes toward EULAs can allow spyware creators to legally 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. Not only can the installation of these programs introduce spyware; a recent study showed that 45% of files located in the popular file-sharing program Kazaa were infected with some type of harmful program, such as viruses, worms, or Trojan horses.[5]

[5] TrueSecure, Dec. 2003

Spyware creators trick users in other ways. Simple tactics include counter-intuitive messages that indicate a certain plug-in is required to access or correctly view a web site and installation messages that read, "To install this software, click 'NO'".

More insidious spyware delivery methods exist as well. "Drive-by downloads" are HTML links, often hidden in spam, that when clicked, initiate an automatic download process. The BuddyLinks adware program was the first designed to exploit a user's AOL instant messenger program and send itself to everyone on a user's buddy list. Once clicked, the link employs drive-by download abilities to install, and ultimately propagate itself onto other unprotected systems.

Computer viruses can leave spyware behind long after they have been removed.

Computer viruses can also leave spyware behind long after they have been removed. News reports have recently uncovered the first examples of spyware programs trying to proliferate through worm-like distribution tactics.[6]

The latest discovery is a new type of blended threat that exploits security holes in Microsoft Internet Information Services (IIS) and Microsoft Internet Explorer (IE). Javascript components were planted on web sites that instructed the user's browser to download an executable from another server and install it. These executables contained keystroke loggers, proxy servers and other back doors providing full access to the infected system.[7] The payload frequently contained the Trojan horse Backdoor:W32/Berbew, also known as Backdoor-AXJ, Webber, or Padador. When this Trojan horse runs on the user's computer it monitors Internet access to capture logon names and passwords, sometimes opening fake dialog boxes that prompt the user to enter confidential information such as ATM card codes, credit card numbers, and more.[8]

[6] http://www.cnn.com/2004/TECH/internet/02/11/instantmessenger.ad.ap
[7] http://www.eweek.com/article2/0,1759,1617234,00.asp
[8] http://www.microsoft.com/security/incident/Download_Ject.mspx

Juju Jiang installed keystroke loggers at over a dozen Kinko's stores in New York and gathered more than 450 online banking usernames and passwords from unsuspecting customers using Internet terminals.

In September 2003, attackers broke into the email of Valve founder Gabe Newell... In a deliberate attack, they installed keystroke loggers on many computers at the game developer's studio to capture source code.

Adware typically uploads user information and downloads targeted advertising over TCP port 80 which is commonly left open on firewalls as it is used for HTTP, or Internet, traffic

Neither firewall nor antivirus solutions were able to proactively block this threat to personal information as the attacks took place via channels that are usually kept open for typical Internet communications.

Even individuals who have only casual access to systems can install damaging spyware. A notable case of this occurred at Kinko's in New York where Juju Jiang installed keystroke loggers at over a dozen stores and gathered more than 450 online banking usernames and passwords from unsuspecting customers using Internet terminals.[9]

Once an attacker obtains usernames and passwords, systems believed to be secure become vulnerable. Attackers may then access sensitive customer information, or in the case of Valve Software, corporate intellectual property. In September 2003, attackers broke into the email of Valve founder Gabe Newell, possibly utilizing a security hole in Microsoft Outlook. In a deliberate attack, they installed keystroke loggers on many computers at the game developer's studio to capture source code. "This [keystroke] recorder is apparently a customized version...created to infect Valve (at least it hasn't been seen anywhere else, and isn't detected by normal virus scanning tools)," said Newell in a message board posting in October 2003. The source code for Half-Life 2 was stolen, delaying the release of the highly anticipated PC game and costing Valve and Vivendi Universal Games an inestimable amount of revenue.[10]

Spyware Detection and Removal

Current firewall and antivirus technologies are not designed to detect and remove spyware. Firewalls do not effectively block spyware infections because spyware is commonly embedded in programs that users willingly download. And, once installed on a system, most spyware applications disguise themselves as trusted programs, allowing them to communicate freely with the Internet over TCP ports that are commonly left unprotected on firewalls. Adware typically uploads user information and downloads targeted advertising over TCP port 80 which is commonly left open on firewalls as it is used for HTTP, or Internet, traffic.[11]

[9] http://www.cybercrime.gov/jiangPlea.htm
[10] http://www.money.cnn.com/2003/10/07/commentary/game_over/column_gaming/
[11] http://www.computerworld.com/securitytopics/security/story/0,10801,92784,00.html

Antivirus tools fail to detect spyware because spyware does not include the viral methods of propagation or behaviors detected by normal antivirus pattern recognition techniques. In addition, most spyware programs bring with them hundreds, if not thousands of additional "traces" including everything from .dll files to graphic images. Often times, removing only the spyware executable still leaves dangerous traces behind.

Monetary incentive also separates the virus world from the spyware world. Spyware publishers make money based on the data they gather or the number of people they are able to trick or entice into visiting web sites.

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 other free, downloadable products. Often, the "downloaded application" will stop working if the spyware component is removed. Moreover, simply uninstalling the "downloaded application" will usually leave the spyware components untouched, and reinstalling the "downloaded application" will also reinstall the spyware.

It takes a specific, detailed description of each spyware application for successful detection and removal to take place. Successful detection and removal of spyware requires a detailed understanding of the spyware itself: how and where its various elements are installed (files, folders, Registry entries), the mutual dependencies between spyware elements and any associated applications and the tasks that the spyware was designed to carry out.

Successful detection and removal of spyware requires a detailed understanding of the spyware itself: how and where its various elements are installed (files, folders, Registry entries), the mutual dependencies between spyware elements and any associated applications and the tasks that the spyware was designed to carry out.

Evaluating Corporate Anti-Spyware Solutions

When addressing spyware in a corporate setting, IT professionals must consider several issues in choosing and implementing a solution. First, the anti-spyware software should work in a complementary fashion with current privacy, security, and Internet programs and policies, including existing antivirus and firewall technologies, thus helping IT professionals round out their overall security solution.

Second, the solution needs to solve the problem. Some spyware "solutions" only identify the presence of spyware and do not handle the more complicated task of removal. Also, the detection capabilities of different solutions vary widely. Some of the better solutions remove spyware components meticulously, without damaging the underlying applications and/or operating systems; others do not. Corporations need the most accurate, thorough and current set of spy definitions and proactive shields available to keep pace with the constant innovations in spyware development.

Third, the solution cannot create more challenges than the problem it solves. Deploying, managing, and updating the solution needs to be straightforward and consume minimal IT resources. The software needs the flexibility to adapt to different environments and types of users with minimal impact on systems and bandwidth.

Finally, the anti-spyware software needs reporting and alerting capabilities. IT professionals must have a clear view of network activity and have the ability to present that information to management in a clear and concise manner. Alerting capabilities should let IT professionals know everything from new spy definition availability to detection of critical types of spyware within the organization. System reports need to provide overview coverage as well as the ability to assess individual systems or spyware programs to understand patterns and impacts. Such an understanding is a critical component of a successful anti-spyware campaign.

Until recently, most anti-spyware applications were targeted at the consumer market and lacked the functionality to scale well in a corporate environment. As the threat and impact of spyware continues to grow, leading anti-spyware software vendors are responding to the need of corporations by delivering enterprise class solutions.

Traits of an Effective Corporate Solution:

- *Centrally managed*
- *Enterprise-wide scalability*
- *Proactive defense*
- *Intuitive scanning features*
- *Protection for remote/laptop users*
- *Thorough quarantine and removal processes*
- *Customizable reporting and alert options*
- *Compliance with other software programs*
- *Regularly updated, comprehensive spy definition database*
- *Technical and customer support*

About Spy Sweeper Enterprise

Webroot Spy Sweeper Enterprise is an award-winning corporate anti-spyware solution that provides centralized desktop-level protection against spyware, adware and other unwanted software programs. Providing the most comprehensive detection and removal of spyware available, Webroot Spy Sweeper Enterprise offers:

- Comprehensive, corporate-wide detection and elimination of spyware and adware
- Automated deployment of spyware definitions and software updates
- Options to schedule group-based and company-wide spyware sweeps
- Ability to create and enforce customized protection policies
- Customizable, detailed reports and summaries on malicious threats
- Advanced support for remote and laptop users while outside the corporate network

About Webroot Software, Inc.

Webroot Software, a privately held company based in Boulder, Colorado, creates innovative privacy, protection and performance products and services for millions of users around the world, ranging from enterprises, Internet service providers, government agencies and higher education institutions, to small businesses and individuals. The company provides a suite of high-quality, easy-to-use software that guides and empowers users as they surf the Web, protecting personal information and returning control over computing environments. Webroot's software consistently receives top ratings and recommendations by respected third-party media and product reviewers.

For more information about Webroot Software or Spy Sweeper Enterprise, please visit www.webroot.com or call 800-870-8102.

2560 55th Street, Boulder, CO 80301

Toll Free: 800.870.8102
Telephone: 303.442.3813
Facsimilie: 303.442.3846

www.webroot.com