



A Websense® White Paper

Protecting Organizations from Spyware

Abstract: Once considered only an annoyance, spyware has evolved from a nuisance to a malicious threat. Preventing spyware from infiltrating an organization requires security measures at multiple points on the network, gateway, and endpoint. This paper describes the impact of spyware on organizations and explains how Websense® software can be used to help combat this growing problem.

Table of Contents:

Introduction.....	3
An Evolving Threat.....	3
Criminal Intent	4
The Impacts of Spyware	4
IT Help Desk Support	4
Productivity	4
Performance	5
Financial	5
Legal	5
Combating Spyware.....	6
Anti-Spyware Legislation and Activities.....	6
The Websense Solution.....	6
o Network Protection	6
o Endpoint Protection	6
o Streamlined Operations	7
Conclusion.....	7

Introduction

As the name implies, spyware applications “spy” on user activities and relay collected information back to the originating website or computer. Some of these programs have historically been considered benign and mere nuisances. “Adware” programs present pop-up banners and relay information about a user’s web surfing activities back to the host so that advertisements can be specifically targeted to that user. However, true spyware programs are far from benign, as they are designed to scan systems, monitor activity, and relay confidential information to other computers or locations.

An Evolving Threat

Spyware has evolved, becoming yet another category in a growing list of malware. Some spyware can install rootkits, keyloggers, redirectors, and software intended to exploit application vulnerabilities. Several of these spyware applications use operating system exploits to install affiliate and other unwanted, unrequested software programs. Others attempt to gain network access in order to steal CPU or network cycles, to install more applications on the system, or enable the theft of proprietary information, including proprietary company data such as client databases, customer information, and so on.

Spyware can be acquired in a variety of ways:

- Secretly bundled as part of a downloaded shareware or freeware program
- Sent as an email or instant messaging attachment
- Installed via a drive-by download when simply visiting a website or viewing an HTML email message
- Through web browsers using ActiveX controls or browser helper objects (BHOs)

Adware presents advertising windows (pop-ups) when it runs. Many adware applications also track user information, including web surfing habits.

Spyware is a program placed on a user’s computer without permission for the express purpose of secretly gathering information about the user and relaying it to advertisers or other interested parties.

BHOs are small, automated programs that monitor visited websites, switch advertising or home pages, download updates, or export data.

A **backdoor** is an access point to a computer program that bypasses security access measures.

A **dialer** is a program that searches for and then commandeers modems, usually causing them to dial expensive toll numbers.

A **rootkit** is a collection of programs that enable administrator-level access. Rootkits typically contain spyware, keyloggers, and tools for creating backdoors.

A **redirector** transfers network traffic to a location other than that which the user intended.

Keyloggers record keystrokes and then upload the information to the host.

The 2005 FBI Computer Survey estimates that viruses, network intrusion, computer theft, and other security incidents cost U.S. businesses more than \$67.2 billion a year.

Criminal Intent

Websense Security Labs™, the security research organization of Websense, Inc., has found that newly evolved crimeware is being created, tested, and deployed by organized criminal groups. These groups intend to monetize an expanding array of information stolen from unsuspecting users using increasingly sophisticated code designed to be more and more difficult to protect against or detect.

Websense Security Labs has also noted an increase in the use of redirectors, including crimeware that changes host files and other DNS-specific information, BHOs that redirect HTTP traffic to fraudulent sites, and crimeware that may install network-level drivers or filters to redirect to fraudulent locations. These ploys are extremely effective, as users have no way of knowing they have been redirected. All of these tools are installed on users' computers without their knowledge for the purpose of compromising information which could be used for identity theft or theft of credentials for criminal purposes.

In the second half of 2005, the motives for creating malicious websites continued to trend away from annoyances, such as changing default homepages and adding bookmarks, to increasingly malicious purposes such as running exploit code to open backdoors or changing browser address bars to redirect users to fake banking and other sites.¹

The Impacts of Spyware

IT Help Desk Support

Historically, spyware's major impact has been on the Help Desk because of spyware-related system reliability and performance issues.

Microsoft reported that 50% of its customers' computer crashes are traceable to spyware.²

The unwanted programs themselves are also viewed as a growing security threat. Help Desk calls tend to underreport the scope of the spyware problem because users typically don't complain until their systems have become almost totally unstable. They wait until they can't tolerate it anymore or their computers stop functioning completely.

Productivity

Even the most benign types of spyware impact productivity. Users have to click to dismiss unwanted pop-ups, taking valuable time away from performing their job functions. More malicious spyware can infect desktops and laptops and affect productivity significantly through downtime, as those desktops and laptops require reformatting or rebuilding by the Help Desk. The need for IT Help Desk staff to investigate system slow-downs caused by spyware also takes them away from other, important IT job functions.

¹ Websense Security Labs Second Half 2005 Security Trends Report

² Staff Report, Monitoring Software on Your PC: Spyware, Adware, and Other Software, United States Federal Trade Commission, March 2005, <http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf>, accessed on April 7, 2006, p. 8.

Performance

Spyware adversely impacts network performance: spyware programs running in the background can affect a network's stability, speed, and overall performance.

Financial

Spyware infections can result in significant financial costs. Cost of ownership goes up dramatically on endpoints (desktops and laptops) when they become infected with spyware. Removing the culprit programs and rebuilding or re-imaging the machines takes time. Machines are unusable during this time, resulting in additional losses in productivity. IT efforts in performing these rebuild tasks also have associated financial costs.

From an e-commerce perspective, spyware erodes the faith consumers have in the internet, frequently resulting in a drop in e-commerce activity.

*Overall, 91% of internet users say they have made at least one change in their online behavior to avoid getting unwanted software programs like viruses and spyware on their computer...
48% of internet users say they have stopped visiting particular Web sites.³*

The theft of intellectual property can undermine an organization's competitive edge and position in the marketplace. The resulting financial losses can be devastating.

Legal

Spyware infection presents the possibility of legal liability when proprietary customer or employee data is hijacked. Pervasive security threats have encouraged regulatory protective measures including the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). These laws require that companies control access to their network infrastructure, customer records, and personal information. Spyware compromises privacy and exposes companies to legal liabilities—including significant civil and criminal penalties—due to this breach in confidentiality of customer data. Spyware is also increasingly being used in targeted attacks against governments and organizations to gain access to sensitive and proprietary information.

Malicious spyware applications may be inadvertently installed by users and can go undetected for extended periods. Until they are discovered and removed, a continuous outflow of confidential customer, personal, or organizational data is then leaked to unknown third parties.

Spyware creators are unconcerned about new laws and pending legislation. The fact that spyware authors will now be subject to significant penalties is encouraging. However, organizations must incorporate anti-spyware measures into their overall security strategy in order to prevent the acquisition and spread of spyware within the organization.

³ Fox, Susannah, Spyware: The threat of unwanted programs is changing the way people use the internet, Pew Internet & American Life Project, July 6, 2005, http://www.pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf, accessed on April 7, 2006, p. 7.

Combating Spyware

Anti-Spyware Legislation and Activities

Growing concerns over spyware have forced the U.S. Congress to evaluate serious anti-spyware proposals. The House passed HR 29 in May 2005. This legislation requires software companies to obtain a consumer's consent before installing programs that can collect personal information and send it to third parties. The measure prohibits activities like collecting personal information by tracking a user's keystrokes, redirecting a user's browser to another website without permission, and delivering online advertisements that cannot be closed.

A second bill, HR 744, which was passed on the same day, does not dictate specific technological requirements, but imposes fines and prison sentences for individuals convicted of tapping into personal computers with the intent of committing fraud or damaging a machine. Congress is currently evaluating additional anti-spyware legislation.

Non-government groups, such as the Anti-Spyware Coalition, are also working to combat the spread of spyware by defining spyware and best practices for combating it, providing prevention tips to the public, and encouraging dialogue on spyware.

The Websense Solution

Websense Web Security Suite™ is a leading internet security solution that protects organizations from spyware, malicious mobile code, and phishing and pharming attacks. Unlike some other solutions, it also blocks spyware and key-logger backchannel communications from ever reaching their host servers.

Network Protection

At the network level, Websense Web Security Suite blocks sites that host spyware applications and are used for drive-by installations; malicious sites that exploit browser vulnerabilities or are used to post information to or from spyware; and sites that host CGI mail parsers from which information captured by spyware could be extracted. Websense Web Security Suite scans and classifies over 450 million websites per week for malicious activity. Customer databases are then automatically updated with the new classifications.

Websense Web Security Suite also blocks sites used as part of IRC or web-based bot networks and requires that web traffic be authenticated and that SMTP traffic be limited.

Websense Web Security Suite identifies new threats quickly, resolving the issue and decreasing threat exposure time. Real-time security updates are available within minutes of the discovery of a new high-risk threat with no administrative intervention required—unlike other solutions, which may take days to deploy. Websense Web Security Suite also manages instant messaging (IM) and IM attachments, which can contain spyware.

Endpoint Protection

Websense Web Security Suite blocks threats before they reach the endpoint and prevents spyware infections by limiting privileges to users (i.e. no local admins) and by limiting privileges to registry and key files (/etc/hosts and BHO registry keys, for example). Computers are prevented from accessing sites identified as dangerous, thus preventing drive-by downloads of spyware and other malicious applications.

Websense Client Policy Manager™ extends security to the endpoint, adding endpoint "lockdown" capabilities and web security for remote and mobile users. Client Policy Manager establishes levels of desktop "lockdown" to prevent the launch of unauthorized applications or mitigate the propagation of security attacks. All endpoints are protected, even when they are disconnected from the network.

Streamlined Operations

Websense Client Policy Manager optimizes IT operations by ensuring that only "approved" configurations are running, and allows IT to be proactive by eliminating calls and dispatches for desktop rebuilds due to performance or application compatibility problems.

Conclusion

Websense Web Security Suite and Websense Client Policy Manager™ provide organizations with a premier web security, endpoint security, and web filtering solution. All Websense solutions are easily managed, automatically updated, and supported by the Websense Master Database, sophisticated analysis techniques, and superior Websense technology. Websense Web Security Suite includes the Websense Web Protection Services™—SiteWatcher™, Brand-Watcher™, and ThreatWatcher™—to help protect organizations' websites, brands, and web servers.

From the relatively benign adware program designed to display an advertising pop-up to applications that install root-kits, keyloggers, redirectors, or ransomware, all spyware poses problems and presents associated costs to the organization. Websense Web Security Suite and Websense Web Security Suite – Lockdown Edition help companies mitigate these risks by preventing spyware from infiltrating the organization's network and gateway and running on desktops and laptops.

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), protects more than 25 million employees from external and internal computer security threats. Using a combination of preemptive ThreatSeeker™ malicious content identification and categorization technology and information leak prevention technology, Websense helps make computing safe and productive. Distributed through its global network of channel partners, Websense software helps organizations block malicious code, prevent the loss of confidential information and manage Internet and wireless access. For more information, visit www.websense.com.