PROCESS™ SOFTWARE

A HALO TECHNOLOGY HOLDING COMPANY

Overcoming the Challenges of Spyware in an Enterprise

White Paper

INSIDE

- Spyware: Trends, Techniques, Sources, Impact, Legislation
- Antispyware: Requirements, Deployment Options, SpyCatcher Enterprise™

Overview

What if a competitor gained access to one of your company's secured systems residing behind a firewall without your knowledge? These systems contained all your trade secrets. Sound impossible? Not according to law enforcement authorities in Israel, who detained 18 people in connection with a malicious code attack in 2005. The attackers allegedly used spyware to commit industrial espionage. This is just one example of how spyware can potentially impact your business. Many businesses are unknowingly susceptible to spyware, including organizations that take every precaution by deploying firewalls, virus and web filters, and anti-spam technology. This whitepaper identifies the effects of spyware in an enterprise, and provides an overview of the enterprise antispyware deployment options.

Spyware Defined
spyware is any software that:

- is installed on your computer without your knowledge or consent, or
- tries to make it difficult (or impossible) for you to remove it, or
- sends information about you, your computer, your files or your Internet use to someone without your knowledge or consent, or
- sends information about you and discloses this to you in an obfuscated way

Trends – How Spyware Impacts Your Bottom Line

Spyware has become ubiquitous. Nearly 85% of all computers have been infected at some point, according to a survey by the Poneman Institute. Unlike virus developers who are motivated by mischief and ego, spyware developers are motivated by financial gain through theft and fraud. Spyware is a profitable business for criminals, so they will not easily be deterred. The FBI estimates that spyware and other computer-related crimes cost US businesses $67 billion per year. See Table 1 for examples of corporate victims of spyware.

Spying Techniques

Spyware is usually invisible to users. Computer or network performance degradation, more display ads, or redirected browser defaults are hints that spyware is present. In more severe cases, computers and networks are unusable.

Trojan Horses and Keyloggers

Detecting spyware can be a challenge even for many antispyware vendors because spying techniques are an evasive threat. In the Israeli espionage case, a Trojan horse was planted on the rival company's system. A Trojan horse contains a computer program that is either hidden inside another program or that masquerades as something it is not in order to trick potential users into running it. An example is a program that appears to be a game or image file but actually performs some other function. A Trojan horse may spread itself by sending copies of itself from the host computer to other computers.

One spyware program can contain multiple spying functions. Trojan horses can be used to gain remote access to a computer, which then executes a keylogger program. A keylogger runs on a computer and records all the keyboard keys that are processed. Although keyloggers could have some benefits (allowing you to recover work that was lost), in practice they are used to spy on people. Since they capture everything you type, your passwords, credit card numbers, and personal correspondence can all be recorded. Some keyloggers are designed only for spying, trying to make it difficult for the user to discover the program is running. In the espionage case, the software installed on the competitor's system was a custom-coded attack that many antispyware solutions couldn't detect with a signature-based solution. This solution is reactive and identifies spyware only after an attack occurs. A fingerprint is added to a vendor's signature database to prevent similar future spyware outbreaks.

Browser Hijacking

Another means of spying is through the use of browser hijackers. This program will modify browser functions such as search engine tools and the default home page, or redirect URLs to different sites. Criminals can also use a dialer which invokes a victim's modem to call expensive numbers.

Adware

Adware is software that delivers advertising content in a manner or context that may be unexpected and unwanted by users. Adware is not normally a threat, but is usually considered a nuisance. It might have been installed by another application. It can display advertisements even if you have a popup blocker on your computer and it can monitor your computer usage to generate ads that you are more likely to respond to. Adware can consume processing power and network bandwidth, slowing down your computer and interrupting your workflow.

Corporate Victims of Spyware

- One in two UK businesses have been affected by spyware while 14% admitted they were unaware of spyware and its effects, according to research published by PC World Business (PCWB).
- Many German Internet users attempting to visit the website for Hertz were instead shown advertisements for rival car-rental firms, if Claria software was installed. Hertz sued, and a German court ordered Claria to stop the practice.
- The personal information of up to 300,000 LexisNexis customers was compromised when attackers sent out an email containing a keystroke logger program (InfoWorld April 25, 2006)

Table 1

Sources of Spyware

There are many ways users can end up with spyware on their PC, including one or more of the following:

- Web surfing
- File sharing
- Email
- Instant messaging
- Freeware or shareware

The greatest source of spyware is the Internet. Over 285 million clicks are made to hostile web sites every month as a result of using a search engine (Ben Edelman, SiteAdvisor Research Analyst). Spyware is found in organic searches as well as sponsored web site searches.

A common way to infect users with spyware is a drive-by download attack. A drive-by download is the automatic installation of software on a user's computer when visiting a web site or viewing an HTML-formatted email, without the user's consent. Drive-by-downloads typically exploit security holes or lowered security settings on a user's computer. An example is JavaScript embedded in HTML code that is designed to exploit a vulnerability in the user's web browser.

Malicious spyware is often found on web sites that provide free software downloads or file sharing, and on web sites used for social networking. A company which produces the free software often gets paid by advertising companies for each computer that becomes "infected" with the spyware. To protect their revenue, the "free" software companies will sometimes force you to run the advertising spyware to use their free software. Often

buried in the license agreement will be a disclaimer stating that information about you and your browsing habits will be sent to the company's web site.

Impact of Spyware

Spyware negatively impacts an enterprises' bottom line and is a major security threat. This is why it has become one of the top priorities in recent years among IT departments and management, according to IDC's 2005 Enterprise Security Study. Spyware affects an enterprise in the following ways:

End-user productivity declines.
Users are unable to continue working when spyware renders computers useless.

IT productivity declines.
Spyware now accounts for 30% of all help desk calls, according to Gartner. IT administrators must spend time removing spyware and rebuilding infected computers — time they could have devoted to more productive tasks (see Table 2 - Calculating the Cost of Spyware).

Availability is affected
Spyware puts a strain on network bandwidth and PC performance — wasting resources, time, and money.

Confidentiality is compromised.
Spyware can put proprietary information into the hands of criminals and competitors. The loss of confidentiality can damage your enterprise's reputation, brand, customer loyalty, and bottom line.

Spyware can introduce secondary vulnerabilities.
Some spyware programs can establish a foothold for other malware to be installed, further infecting computers. Spyware also leads to spam and vice versa. When spyware finds e-mail addresses, it sends them back out over the Internet to be traded, shared or sold to spammers. When spam is delivered to a user who clicks to see an advertised product, spyware can secretly download as the advertisement unfolds. This creates an administrative nightmare for IT professionals, not to mention the legal implications it introduces as inappropriate content floods inboxes.

Regulatory compliance is violated.
When spyware captures confidential information or secretly peruses files and applications, regulatory compliance with the following legislation is impossible: Health Insurance Portability and Accountability Act, established to ensure the privacy of patient information; the Sarbanes-Oxley Act, established to ensure that financial statements are resistant to fraud; the Gramm-Leach-Bliley Act, established to safeguard customer information; and even the California Data Privacy Law (California SB 1386), established to protect the confidential information of state residents.

Calculating the Cost of Spyware

The cost of spyware outbreaks can vary. It depends on factors such as the severity of the threat level, the number of PCs infected, and other intangible costs. Table 2 estimates the total annual Help Desk cost of spyware for a company with 1,000 computers. Industry averages are used to calculate the rate of infection for 1,000 PCs and the time it takes remove and repair these systems. In addition to Help Desk costs, there are a lot of other intangible costs that are difficult to quantify.

Annual Spyware Help Desk Cost	
Number of PCs……..	1,000
Annual Salary of IT Help Desk…….	$65,000
Loaded Salary of Help Desk……..	$104,000
Number of Spyware Incident (30% per quarter x 4 quarters)……..	1,200
Number of Hours Spent (assumes 2.5 hours/incident)…….	3,000
Help Desk Cost per Hour…….	$52
Total Annual Help Desk Cost ……	**$156,800**
Intangible Cost	
Loss of Intellectual Property	
Cost of Stolen Data	
Exposure of Trade Secrets	
Compromise of Customer Data	
Consumption of System and Network Resources	
Employee Productivity	

Table 2

Legislation

Antispyware legislation was introduced in the US House and Senate in 2005, yet there is no specific federal antispyware law on the books today. Existing federal laws, which include Section 5 of the Federal Trade Commission Act, the Electronic Communication Privacy Act, and the Computer Fraud and Abuse Act have been used to target spyware distributors. In addition, lawsuits have been filed under state consumer protection laws. There are also various state antispyware laws that are in effect.

Although the courts have had some success with shutting down spyware operations, industry experts believe consumer education and technology must also be used to combat spyware effectively.

Enterprise Antispyware Requirements

It is important for organizations to deploy an antispyware solution that meets their needs. Deploying the wrong solution can cost an enterprise more in the end by wasting resources and time. The basic requirements for an enterprise antispyware solution are the following:

- The core technology must be able to accurately detect the most obscure spyware without disabling legitimate applications.
- It must catch spyware proactively before any damage is done.
- The ability to remove spyware and prevent its re-installation is essential.
- There should be a centralized management console that makes it easy to deploy and update users' PCs.
- Users should not have to update or manage their own desktops.
- The antispyware solution must work seamlessly with other applications deployed in your enterprise.
- The antispyware solution should scale to the growing needs of an organization.

Detection Technology

Security companies often use signature-based solutions to detect spyware. Some vendors have assembled a vast list of spyware fingerprints for their products, erroneously believing that the biggest could provide the best protection. In reality, signature-based solutions are inherently limited because they are a reactive security solution. Spyware detection occurs only after a particular piece of spyware has been identified. Signature-based solutions are powerless to stop new threats. Worse, an increasing amount of spyware can mutate itself, constantly staying one step ahead of signature-based solutions.

In response to the limitations of signature-based antispyware technology, many security vendors added behavioral blocking to their antispyware solutions. Behavioral blocking technology does not try to recognize a threat by its code, but instead by its actions. It is essentially application-level surveillance. Though powerful, behavior-based spyware detection is limited in that it is not precise enough to differentiate between destructive and constructive behaviors. Also, it's extremely challenging for IT administrators to create standard behavior-based security policies capable of accurately identifying spyware throughout an enterprise. That's why security policies created with behavior-based solutions tend to be too lenient or restrictive.

Contextual analysis goes one step further than behavioral analysis. It takes into account the context in which a particular suspicious behavior occurs. For example, keyloggers use a particular behavior to capture your keystrokes as you type that is also used by normal applications – Adobe Photoshop and the software for Dell's touch pads use the same technique to capture user hotkeys. Whereas behavioral analysis cannot differentiate between a keylogger and Photoshop, contextual analysis recognizes that Photoshop uses its information in a benign, beneficial way and safely isolates the keylogger.

Installation & Deployment
An enterprise antispyware solution should be easy to install, manage, and upgrade whether your environment has 100 computers or thousands of computers. A central management console is needed to reduce the time and cost of the deployment process. The antispyware solution should be able to fit into your existing infrastructure. For example, it should support LDAP directories or work in environment where no directories are used.

Management & Reporting
The following features should be considered when evaluating an antispyware solution:

- The solution should have a web-based management console, which makes it easy to centrally manage security policies, spyware scanning, administration, and reporting.
- Automated spyware sweeps should be transparent to end-users and can be scheduled to run at any given time or at regular intervals.
- An enterprise should be protected from the re-installation of spyware after it has been removed.
- Safe remediation of spyware must be efficient.
- Suspicious application should be identified and quarantined until an administrator can determine their status.
- Executive-level summaries, detailed reporting, and alerts regarding suspicious applications and files should be available. This provides administrators with immediate visibility into which computers may have been infected in an outbreak.

Security
An enterprise should consider the following security features:

- End-users should not be responsible for determining what is and what is not spyware. An enterprise antispyware solution should be able to execute the security policies determined by the organization.
- An enterprise antispyware solution should complement, not conflict with other security solutions such as anti-spam or anti-virus software.

Enterprise Antispyware Deployment Options

Gateway
A growing number of network security appliances installed at the gateway promise antispyware detection and blocking. Appliance-based antispyware products rely on latent content filtering to block traffic to or from web sites known to host spyware. But these devices only provide protection at the network level, and not at the individual client level. More importantly, appliance-based solutions offer no mechanism to remediate spyware or prevent reinstallation on individual PCs, and they can’t protect mobile devices.

Security suite
With all of the issues that an IT department faces on a daily basis, they may find an antispyware add-on to a security suite is an attractive solution. It appears to have an initial lower cost of ownership because they already have experience with the management interface console and feel that little training will be needed. However, most vendors that offer security suites were originally developers of anti-virus software. The reactive approach of the signature-based solutions used to eradicate viruses does not work on spyware. The potential financial impact of having spyware on your systems for any amount of time is too great. Given that the effectiveness of the scanning technology is an important criterion for selecting an antispyware solution, organizations need a technology that is specifically designed to deal with the unique characteristics of the spyware threat.

Client-side solution
Organizations with tight IT budgets and limited time to address the spyware problem may ask their employees to use a free client-side antispyware solution. While the up-front cost is attractive, the total cost of ownership is much higher than an enterprise solution. By implementing a client-side solution, there is a greater potential that spyware still exists in that organization. Free antispyware software providers will not offer the quality spyware scanning engine that is found in an enterprise-grade solution. Freeware also tends to have conflicts with other security software running on a PC, causing the system to crash or other programs to malfunction.

Client-side antispyware has a higher cost associated with installation, upgrades, management, and help desk incidents than enterprise solutions. There are also other intangible costs associated with an organization not being able to enforce their security policy because they lack the knowledge of what is running in their network.

Best-of-Breed
Best –of – breed solutions are designed specifically to tackle the unique characteristics of spyware. These solutions proactively prevent the most sophisticated spyware programs and keep it from re-installing. These solutions are designed to run in an enterprise environment and will complement existing security software.

SpyCatcher Enterprise

SpyCatcher™ Enterprise is a best-of-breed solution. It is the first and only antispyware solution that proactively protects enterprise computers from next-generation spyware, such as hyper-mutating and custom-coded attacks. Patent-pending Adaptive Protection Technology™ goes beyond signature- and behavior-based technologies, providing contextual intelligence that quickly and accurately identifies newly emerging threats. SpyCatcher Enterprise provides the fastest, most complete and safest spyware remediation as well as easy, enterprise-class management.

SpyCatcher features include:

Continuous Real-Time Protection

- Identifies and stops emerging threats with new patent-pending technology called Profiling Engine ™
- Prevents spyware from automatically reinstalling

Identifies Threats that Evade Other Antispyware Solutions

- Detects spyware deeply embedded in the operating system and scans system memory, registry files, hard disks, network drives, and other devices for spyware.
- Analyzes fingerprints as well as meta data information (such as file size, location, and associated registry entries).

Safe Remediation

- Safe spyware removal without harming enterprise computers.
- Quarantines potential spyware and alerts administrators.

Enterprise-Class Management

- Web-based management console allows anytime/anywhere access, which maximizes IT productivity.
- Automated spyware sweeps are transparent to end-users and can be scheduled to run at any given time or at regular intervals.
- Enterprise environment integration ensures that SpyCatcher Enterprise seamlessly co-exists with and augments existing IT investments, such as anti-virus solutions.
- Scalability makes it easy to manage and control thousands of enterprise computers.
- Reports & alerts provide many levels of reporting into which computers may have been infected in an outbreak.

About Process Software

Process Software is a premier supplier of communications software solutions to mission critical environments since 1984. With a loyal customer base of over 3,000 organizations, including Global 2000 and Fortune 1000 companies, Process Software has earned a strong reputation for meeting the stringent reliability and performance requirements of enterprise networks.

References

"A Crawler-based Study of Spyware on the Web" University of Washington, http://www.isoc.org/isoc/conferences/ndss/06/proceedings/html/2006/papers/spycrawler.pdf, 2005

"The Safety of Internet Search Engines", www.siteadvisor.com, May 2006

"Antispyware Groups: Legislation Still Needed" NetworkWorld, www.networkworld.com, 9/21/06

"Computer Crime Costs $67 Billion", CNET News, http://news.com.com/, 1/20/06

"Spyware Enforcement", Center for Democracy and Technology, www.cdt.org , October 2006

"Spyware", US-CERT, www.us-cert.gov , 2005

"Anti-Spyware Coalition Definitions Document", Anti-Spyware Coalition, www.antispywarecoalition.org, June 29, 2006

"Israeli Attack Represents a Dangerous New Breed of Spyware", Gartner, June 2, 2005

To learn more about SpyCatcher™ Enterprise,
please call Process Software at 1.800.722.7770 or visit www.processc.om

PROCESS™
SOFTWARE
A HALO TECHNOLOGY HOLDING COMPANY

www.process.com

Process Software
959 Concord Street
Framingham, MA 01701

Telephone:
U.S./Canada 800.722.7770
International 508.879.6994

Web: www.process.com
E-mail: info@process.com

Fax: 508.879.0042