Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Neutralizing Spyware in the Enterprise Environment

Intelligent Security

Check Point protects every part of your network—perimeter, internal, Web— to keep your information resources safe, accessible, and easy to manage.

Contents

Executive summary

Spyware impacts the enterprise environment by causing significant financial damage and posing a serious regulatory compliance threat. To counter the spyware threat facing the enterprise, an integrated security solution should be implemented that neutralizes spyware and systematically detects and removes spyware from laptops and desktops. Any effective anti-spyware solution must first prevent enterprise data loss and block unauthorized network entry. Next, there must also be systematic eradication of spyware that cannot be bypassed, restoring network bandwidth and PC system resources. Finally, ongoing management of the overall endpoint security posture is critical to maintaining a spyware-free PC environment. To achieve all of this, administrators need an integrated solution with a single management interface for overall endpoint security policy coordination and to perform ongoing reporting and analysis to diagnose endpoint security issues.

The rising tide of spyware

By using subterfuge, social engineering, and cutting-edge techniques to infiltrate PCs, spyware has spilled over into the enterprise, becoming a potent threat. It arrives often by way of third-party applications, silent browser "drive-by" installations, and even instant messaging (IM) or streaming video. Hewlett Packard (HP) makes a conservative estimate that spyware costs businesses $138 per incident. Multiply that by the National Cyber Security Alliance's finding that eight out of every 10 PCs are infected with spyware and you begin to see how much this costs your enterprise. While this is already a significant cost, it does not even begin to account for the financial damage posed by network security breaches and intellectual property theft. Beyond acknowledging the threat of spyware, it is imperative to understand the nature of the spyware threat as it pertains to the enterprise environment.

Understanding spyware

Profit is now a central reason for spyware. With its ability to transmit data from a host to the Internet and allowing remote access into the corporate network, confidential documents and customer data are ripe for the picking by hackers. More troubling, data stolen or remote access made into the enterprise network is often encrypted. Attempts to use perimeter filters to control unauthorized data being sent may not be able to decipher this encrypted traffic. Spyware also has the ability to bring in and install additional malicious software onto a host without consent. A disturbing trend was confirmed in 2004 by the CSI/FBI report where theft of proprietary data ranked third in terms of U.S. dollar losses due to cyber-security breaches, following only viruses and denial of service attacks.

[1] HP. "Spyware—the business cost" http://h71028.www7.hp.com/eNewsletter/cache/110968-0-0-224-121.aspx

[2] "AOL/NCSA Online Safety Study." http://www.staysafeonline.info/news/safety_study_v04.pdf

Spotting spyware in the enterprise

Determining if your enterprise has been infiltrated by spyware is not always straightforward. Enterprises dealing with PC system slowdowns or network-band-width spikes are witnessing the telltale signs of spyware infiltration. However, the silent effects of spyware are even more damaging. Trojans enable hackers to gain unauthorized entry into the network, placing valuable customer data and intellectual property at risk. Keystroke loggers capture and then send hackers information such as user passwords, internal Web-site URLs, and a host of other internal-only data. With these spyware tools, PC systems may not exhibit signs of infection. In addition, even after workstations are scanned and cleaned, problems can recur because today's spyware programs can reinstall themselves automatically. This is the insidious and sophisticated nature of today's spyware that necessitates a proactive security response at the endpoint PC.

Stopping spyware

To combat spyware proactively requires a strong defense on every endpoint —both desktops and laptops—to account for the many ways that spyware enters and threatens the enterprise. First, the anti-spyware solution must establish a beachhead stemming the threat of spyware. By blocking unauthorized com-munications in and out of the PC, it keeps any existing spyware from sending out confidential enterprise data or acting as a rogue server allowing unauthorized remote access to the internal network. Next, spyware must be detected. Then, spyware needs to be removed, if possible, or quarantined at the least. A key aspect of this process is anti-spyware client protection that prevents client tam-pering by spyware or users attempting to disrupt the anti-spyware software. And finally, to stay ahead of the growing universe of spyware, anti-spyware software needs to enforce regular spyware scans and automatically obtain engine and definition updates.

For enterprise environments, central management and consolidated reporting are additional requirements to successfully stopping spyware. Administrators use a centralized management console to develop and deploy anti-spyware policies and to access consolidated reporting for a coordinated response across all endpoint PCs.

However, enterprises cannot afford to add yet another security client to their desktops and laptops, nor can their administrators afford to learn another management console interface. Instead, enterprises are finding anti-spyware security is simply an ingredient of a larger endpoint security solution. This eases IT headaches with only a single client to deploy and one central management console for all endpoint security policies, encompassing anti-spyware.

The solution: Check Point Integrity

Check Point Integrity™ Anti-Spyware—based on industry-leading ZoneAlarm® anti-spyware technology—stops spyware and ensures continuous improvement of security practices. As an integrated module of the core Integrity product, Integrity Anti-Spyware can be deployed without the need to install a separate client. The anti-spyware capabilities in the unified Integrity client are centrally managed from the Integrity server console. Administrator-scheduled spyware scans take place in the background, transparent to users so as to not impact their productivity. Scans will detect spyware using signatures ensuring efficient

spyware detection. Signatures may consist of registry keys or known executable names. Integrity Anti-Spyware then removes or quarantines any spyware found on the PC. The Integrity client protects itself from any user or spyware tampering and ensures that scans take place on the PC. Administrators can also specify spyware scan levels ranging from quick searches of common locations for spyware to in-depth searches of the entire PC for any spyware traces. In addition, exception lists can be created to enable use of authorized monitoring or remote access troubleshooting tools.

Keeping anti-spyware ahead of the latest threats is critical for adequate security. Check Point Security Services conducts original spyware research and receives real-time data from the Zone Labs® DefenseNet™ community consisting of millions of ZoneAlarm® users. These users automatically contribute critical information such as spyware MD5 checksums and OS-specific spyware file locations. Using this real-time information, the Security Services team can develop the detection and removal rules before enterprises can be compromised. Both Integrity servers and Integrity clients can be configured to automatically contact the SmartDefense™ Anti-Spyware Service on a regular basis to obtain the most recent definitions.

Finally, the complete Integrity endpoint security solution gives administrators control over the endpoints' access into the enterprise network. Integrity verifies endpoints comply with security policies—running up-to-date antivirus, anti-spyware, and a personal firewall—before network access is granted. Unsecured PCs are quarantined and automatically brought back into compliance. Then, by blocking unauthorized communications, Integrity establishes the secure beachhead neutralizing spyware. After automatic scans remove the spyware, the Integrity client reports back to the central management console allowing administrators to analyze overall anti-spyware security and adjust user education or corporate policy if spyware continues to be found.

Steps to secure the enterprise from spyware:

- Deploy Check Point Integrity™, a centrally managed endpoint security solution that controls application communications in and out of the PC. Program events are centrally logged allowing consolidated administrative reporting of programs attempting network access.

- Enable the Integrity Anti-Spyware module and deploy a baseline spyware security policy consisting of automatic treatment options for each category of spyware. Automatic treatment—observation, quarantining, or removal— improves security while minimizing end-user involvement.

- Schedule regular scans to discover new spyware applications and services for quarantining, removal, or observation. Integrity makes sure that scans take place, and it will log and report scan results back to administrators for analysis.

- Use Check Point SmartDefense™ Anti-Spyware Service for automatic anti-spyware engine and definition updates, ensuring that the latest defense mechanisms against spyware are in place.

- Finally, configure Integrity to enforce regularly scheduled anti-spyware scans, which makes sure scans have been completed before network access is granted, providing the maximum spyware protection.

Conclusion

Neutralizing spyware in the enterprise environment takes the combined efforts of a total endpoint security solution. Integrity shields your enterprise's PCs, prevents confidential information exposure, and blocks unauthorized hacker entry, effectively neutralizing spyware's primary threat. Then, Integrity's best-in-class anti-spyware detection and removal is critical to cleaning spyware from infected machines and restoring network bandwidth and PC system resources. To stay ahead of the latest spyware threats, an effective anti-spyware service must have access to real-time spyware information, ideally from millions of trusted sources. With central management, real-time monitoring and reporting, and network access policy enforcement, Integrity endpoint security will help you to maintain a spyware-free PC environment. Integrity Anti-Spyware is the only solution today to offer enterprise-class, integrated protection to defeat spyware.

About Check Point Software Technologies

Check Point Software Technologies Ltd. (www.checkpoint.com) is the worldwide leader in securing the Internet. It is the market leader in the worldwide enterprise firewall, personal firewall, and VPN markets. Through its NGX platform, the company delivers a unified security architecture for a broad range of perimeter, internal, and Web security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices, and partner extranets. The company's ZoneAlarm product line is one of the most trusted brands in Internet security, creating award-winning endpoint security solutions that protect millions of PCs from hackers, spyware, and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from more than 350 leading companies. Check Point solutions are sold, integrated, and serviced by a network of more than 2,200 Check Point partners in 88 countries.

CHECK POINT OFFICES

Worldwide Headquarters
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: **http://www.checkpoint.com**

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.