

White Paper

Stopping Spyware at the Internet Gateway

Lessons from Real-World Spyware Attacks



www.cpsecure.com

Executive Summary

Spyware is a form of malicious software that spies on computers and steals sensitive data. It differs from viruses and spam, is too often used to refer to adware, and varies in impact from annoying to economically damaging. An examination of real-world spyware attacks gives specificity and concreteness to the spyware discussion. Such spyware cases highlight the following best practices:

- Cover both desktop computers and the internet gateway in a layered defense;
- Cover web, email, and other internet traffic; and
- Cover the full spectrum of spyware and other malicious software.

The internet gateway is the ideal place to stop spyware. If spy programs can be stripped out of internet traffic at the gateway, before they can install themselves on desktop computers, then the threat of spyware may be substantially reduced. For gateway anti-spyware then, the real-world attacks suggest three key requirements:

- Real-time scanning performance;
- Comprehensive internet traffic coverage; and
- Comprehensive spyware and malware coverage.

Deployment of gateway anti-spyware that meets these requirements with desktop anti-spyware in a layered defense is the most effective way to counter today's spyware threat.

1. Spyware and Its Impact

Spyware is a form of malicious software that spies on computers and steals sensitive data. It is different from viruses in the way it launches attacks. Spyware programs attack in a stealthy, targeted manner to steal information, whereas traditional viruses attack in an open, mass-propagation fashion to disable as many computers as possible. Spyware is also different from spam in its impact on organizations. While spam may be a great nuisance that decreases the productivity of computer users and consumes system resources, spyware compromises the confidentiality of sensitive institutional and personal information.

There has been much recent attention on spyware, yet spyware remains an ambiguous term. Too often, when the term spyware is used, it is used to refer to what is actually adware, a type of advertising display software that is more of a nuisance than a security threat. As a result of this blurring of spyware and adware, discussions of the spyware threat often give equal weight to worker productivity and system performance issues as to information theft. The implication is that problems caused by adware are at the same level as problems caused by spyware used by cybercriminals. This white paper recognizes that there are several types of programs that may be classified as spyware, but it holds that some are more dangerous than others (see figure 1.1).

Figure 1.1: Spectrum of Spyware Impact



To be sure, the daily impact of adware may be more noticeable, but that does not mean more dangerous varieties of spyware do not exist and cannot attack a given organization. An organization needs protection against the full spectrum of spyware, from the most annoying to the most damaging.

2. Real-World Spyware Attacks

Recent examples of real-world spyware attacks indicate that the spyware threat is increasing in sophistication and prevalence. Clearly, there is much more to spyware than pop-up ads and browser redirects.

International Identity Theft Ring (August 2005)

An international identity theft ring that uses spyware to steal confidential personal information was unearthed in August. Credit card details, Social Security numbers, usernames, passwords, and other private information for an estimated 27,000 customers of over 50 international financial institutions were found. The criminal group captured this sensitive personal data through web-based Trojan horses that contained keylogger and backdoor spy programs. A computer user who visited the spyware-hosting website, perhaps as a result of a browser redirect or phishing email, would be attacked with an automatic drive-by download that installed Trojan horse and backdoor spyware.

UK Critical National Infrastructure (June 2005)

In June, the UK's National Infrastructure Security Co-ordination Centre announced that the British critical national infrastructure had been bombarded for several months with sophisticated, industrial-strength Trojan horse attacks. The attacks targeted specific individuals privy to commercially or economically sensitive information at over 300 key government, financial, transport, telecommunications, military, health, and energy organizations. The Trojan horse and backdoor spyware arrived through email and through websites that phishing email recipients were deceived into visiting. Once installed, the spyware programs collected user names, passwords, and system information; scanned drives; and uploaded documents and data to remote computers.

Israeli Corporate Espionage (May 2005)

The Israeli corporate scene was scandalized in May with news of the biggest case of industrial espionage in Israel's history. 15 leading Israeli corporations had hired private investigators to spy on their rivals using Trojan horse spyware. Tens of thousands of confidential documents were stolen from target companies. The Trojan horse and backdoor spy programs attacked via email and CD-ROMs sent by regular mail and allowed a person to control a computer, make changes to its programs, monitor all of its contents, and send documents and pictures to FTP file-storage servers in Israel and overseas.

Eyeveg Spyware Worm (May 2005)

The Eyeveg worm demonstrates that even traditional virus and worm technologies may be repurposed with spyware capabilities. The spyware worm is embedded in an HTML attachment of an email and activates when the HTML renders. It drops a Trojan horse keylogger that loads into web browsers to capture data sent to SSL servers. The Trojan horse also includes a backdoor program that can upload/download files, copy/delete/find/start files, and retrieve system information. As with traditional worms, Eyeveg seeks to propagate itself, in this case by hijacking email addresses and emailing itself to more computers.

Sumitomo Mitsui Bank (March 2005)

In March, British police foiled a plot to steal £220 million from Sumitomo Mitsui Bank in London. Cybercriminals had compromised the bank's computer systems and secretly deployed a keylogger program that was perhaps part of a Trojan horse. The spyware relayed password and access information to the criminals, who intended to transfer the funds electronically. A man in Israel was arrested after allegedly trying to transfer £13.9 million into an Israeli account.

These spyware cases provide real-world data for the development of anti-spyware best practices. All the cases involved spyware that truly spied on computers to steal sensitive information, namely Trojan horse and backdoor spyware. These spy programs reached their targets through both web and email traffic. The above cases also highlight that spyware attacks are becoming increasingly creative and sophisticated. Attacks may use browser redirects and phishing email to bring their targets to websites that then deploy spyware via web traffic. Spyware may also propagate widely when it is used in combination with worms and traditional email-borne viruses. Thus, spyware is not a standalone threat – it is often deployed as part of a blended attack involving other types of malware.

These cases indicate that anti-spyware best practices should include the following:

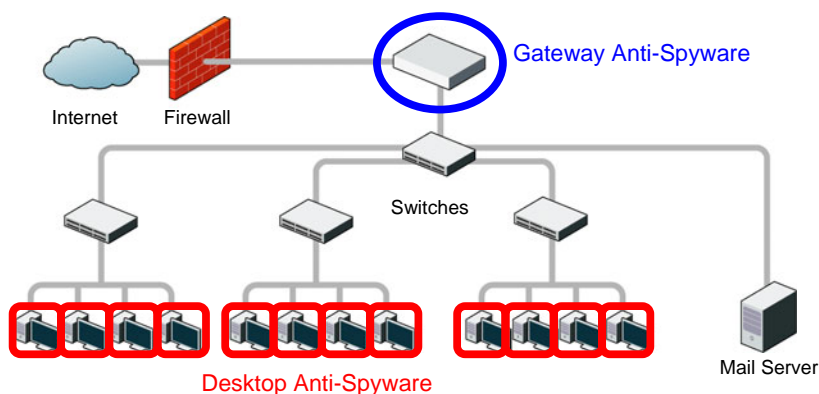
- Cover both desktop computers and the internet gateway in a layered defense;
- Cover web, email, and other internet traffic; and
- Cover the full spectrum of spyware and malware.

This paper will consider each of these best practices in more detail below.

3. Layered Anti-Spyware Defense

Anti-spyware best practices, like anti-virus (AV) best practices, begin with a layered defense that covers desktops and the gateway (see figure 3.1).

Figure 3.1: Diagram of Layered Anti-Spyware Defense



At the desktop level, anti-spyware is difficult but necessary. First and foremost, it is important to understand that desktop anti-spyware is a reactive measure. The main task is to find and remove spyware that is designed to be hard to find and hard to remove. Desktop anti-spyware products from pure-play anti-spyware vendors may have good coverage of adware-types of spyware but often fall short on coverage of Trojan horse and backdoor spy programs. The best approach then may be to use a desktop AV product that includes spyware signatures and a desktop anti-spyware product from another vendor. Enterprise-class management and reporting capabilities are other important factors to consider.

The internet gateway is the ideal place to stop spyware. Unlike desktop anti-spyware, gateway anti-spyware is a proactive measure. The main task is to prevent spyware from entering the network and installing on individual computers. This is in fact not a new idea. A key lesson from AV deployments is that the gateway is a strategic point from which to scan internet traffic and protect an entire network against internet-borne malicious software. In the same way, if spy programs can be stripped out of internet traffic at the gateway, before they can install themselves on desktop computers, then the threat of spyware may be substantially reduced.

4. Gateway Anti-Spyware Scanning

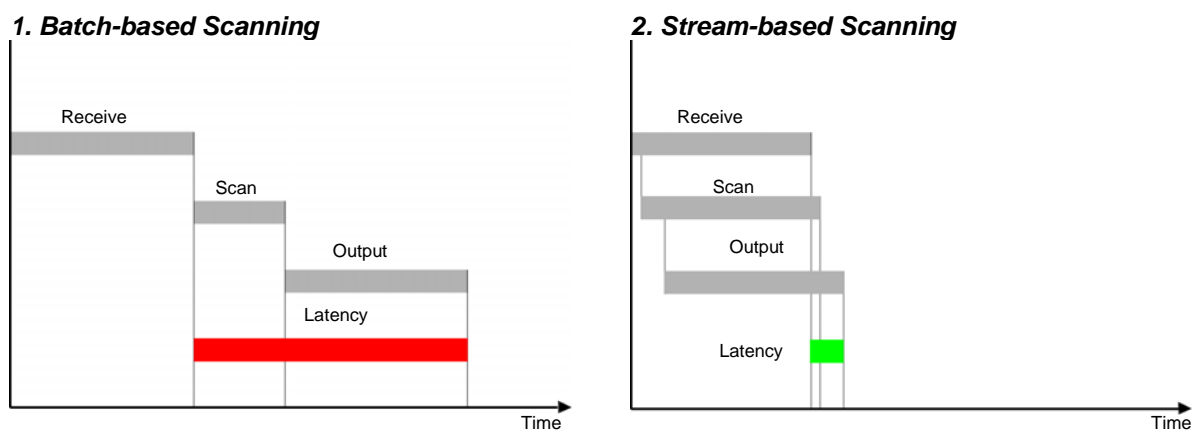
The core of any gateway anti-spyware defense, as with anti-spyware on the desktop, must start with spyware scanning. Other technologies may be useful complements, but the most reliable and effective way to identify and remove spyware from internet traffic is signature-matching.

Gateway scanning for spyware, however, is problematic. It requires an extremely high performance scanning technology that can handle real-time web traffic for large numbers of computers without turning the gateway into a network bottleneck.

Today's scanning technology, used in desktop and gateway AV products, was mostly designed before the internet era. It therefore is not optimized to scan real-time internet traffic. Its architecture is batch-based, which means scanning commences only after an entire file is received, and outputting starts only after the entire file has been scanned (see figure 4.1.1). In short, processing takes place in sequence, or serially. When applied to spyware threats in high-volume web traffic, this scanning approach introduces unacceptable levels of latency and will bring mission-critical web activities to a standstill.

A better approach suited to the nature of real-time web traffic would be based on the simple observation that network traffic travels in streams. In such a stream-based scanning architecture, a scan engine would start receiving and analyzing traffic as the stream enters the network (see figure 4.1.2). The receiving, scanning, and outputting processes would occur concurrently. In other words, processing would take place in parallel, thus minimizing processing time and ensuring that network performance is not reduced. A stream-based scanning architecture therefore would meet the challenge of scanning high volumes of real-time internet traffic, without turning the internet gateway into a network bottleneck.

Figure 4.1



5. Gateway Anti-Spyware Requirements

The spyware cases discussed earlier also suggest certain gateway anti-spyware requirements. The first and most important requirement of gateway anti-spyware is real-time scanning performance. If a product cannot deliver real-time performance, then it cannot scan high volumes of web traffic for spyware. If it cannot scan enterprise-class web traffic, then it cannot truly protect against spyware, since web traffic is one of the main vectors of spyware attacks. So in this case, it is no longer a matter of a trade-off between security and performance. An organization must have both. High performance is necessary if there is to be any gateway anti-spyware security.

After real-time performance, a second requirement of gateway anti-spyware is comprehensive internet traffic coverage. All major avenues of internet traffic must be scanned for spyware. In the past, it may have been sufficient to cover only one major internet protocol such as SMTP for email traffic. Today, however, spy programs do not limit themselves to SMTP email. They attack through multiple protocols, including HTTP, POP3, IMAP, FTP, and even HTTPS. Note that coverage of web and email traffic by separate gateway products may introduce security gaps when certain varieties of spyware attack simultaneously through both web and email vectors. Gateway anti-spyware therefore must scan web, email, and other internet traffic to ensure that spyware does not infiltrate the network through undefended vectors or gateway security gaps.

A third requirement is comprehensive signature coverage. A signature library must include all known spyware and, more broadly, all known malware. Note that some anti-spyware vendors count every variation of a given spyware as a separate instance of spyware and therefore claim extensive spyware libraries. Spyware signatures should be comprehensive and range from adware-types of spyware to Trojan horse spyware, backdoor spy programs, password tools, and hacker tools. Note also that some signature libraries are actually open-source collections that cover less than half of all known spyware and malware. Moreover, these open source libraries raise the critical issue of who is responsible for delivering timely emergency signature updates when a new spyware or malware program attacks. Since spyware is often part of a blended malware attack, the library should include not only spyware but also all known malware ranging from traditional viruses and worms to the newest Trojan horse spy programs and spyware worms.

Conclusion

Spyware is a new and increasing threat to organizations. It is important to understand this threat from a real-world perspective in order to develop anti-spyware best practices and requirements. This paper sets forth that anti-spyware best practices begin with a layered defense at the gateway and desktop levels. At the gateway, anti-spyware is most effective for proactively stopping spyware from entering the network and installing on individual computers. The core of gateway anti-spyware, like desktop anti-spyware, is spyware scanning. But the key issue with scanning real-time web traffic for spyware is scanning performance. Key requirements for gateway anti-spyware therefore include real-time scanning performance, as well as comprehensive internet traffic coverage and comprehensive spyware and malware coverage. Deployment of gateway anti-spyware that meets these requirements with desktop anti-spyware in a layered defense is the most effective way to counter today's spyware threat.



About CP Secure, Inc.

Founded by gateway anti-virus pioneers, CP Secure, Inc. is a leading innovator of real-time anti-malware solutions for enterprise-class organizations. The company's Content Security Gateway appliances are powered by patent-pending stream-based scanning technology to protect networks in real-time against spyware, viruses, worms, and other malware. CP Secure operates globally, in North America, Europe, and Asia, and may be found on the web at www.cpsecure.com.

20065 Stevens Creek Blvd., Building C
Cupertino, CA 95014, USA

Tel: +1 888.722.6847
+1 408.873.7778
Fax: +1 408.873.7779
Email: info@cpsecure.com

Copyright © 2005 CP Secure, Inc. All rights reserved. All product information is subject to change without prior notice. CP Secure, the CP Secure logo, and Content Security Gateway are trademarks of CP Secure, Inc. All other brand, product, service, and company names are registered trademarks, trademarks, or service marks of their respective holders and are acknowledged.
CPS-WP-051026