

I D C E X E C U T I V E B R I E F

Spyware and Other Web-Based Malware: The New Security Threat and Its New Solution

February 2006

By Brian E. Burke

Adapted from Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc by Brian E. Burke and Rose Ryan; IDC #34023, November 2005

Sponsored by CP Secure, Inc.

Introduction

Web-based malware, such as spyware, Trojan horses, and worms imbedded in images, is becoming both a security and system management nightmare. IDC believes, for example, more than three-quarters of all corporate machines are infected with various forms of spyware. As the number of Internet users rapidly grows, the Web is becoming the new threat vector for hackers, virus writers, and cybercriminals. Users need only to browse a Web page or open a Web email to trigger Web-based malware.

Fortunately, Web security technology is evolving from Web-address filtering to gateway-level scanning of all Web traffic in real time. This Executive Brief examines the new security threat environment arising from increased Web usage and the emergence of stream-based scanning as a new solution against spyware and other Web-based malware.

Web Traffic: The New Threat Vector

Until recently, email-borne viruses were the most attractive weapon of hackers who sought to damage or disrupt business operations. The digital threat environment is rapidly changing, however — both in the vulnerabilities malware writers are targeting and in their motives for writing sophisticated malware. Yesterday's weak link in the IT security chain was network traffic based on the Simple Mail Transfer Protocol (SMTP); today's weak link is network traffic based on the Hypertext Transfer Protocol (HTTP).

Web Vulnerabilities: Browsers and Sites

The new vector of malware attack is the Web. A growing number of malicious programs are exploiting security weaknesses in Internet browsers and Web servers to install spyware or other malware on corporate machines. Attacks targeting Web browser vulnerabilities illustrate the sophisticated techniques hackers have developed to spoof, or fake, Web sites and how easily malicious code can steal usernames, passwords, and other vital information.

Today's malware programs also attack Web sites. This problem is not limited to suspect Web sites that host malware, but extends to Web sites used by employees in the course of their work. Some malware programs, such as the Nimda worm, are designed to turn mainstream Web sites into malicious Web sites that distribute Web-based malware. So even when an employee visits a reputable Web site, an infected Web page there can exploit a site visitor's computer remotely without the visitor even having to physically click on any links. Just by visiting a normal Web site as part of normal business activities, an employee may be secretly attacked by Web-based malware such as spyware or worms.

Web-based malware programs attack through not only the infected pages of rogue and mainstream sites, but also via Web mail and corrupted images. For example, a user may use a Web browser to access an external mail system and open an email containing a worm-infected JPEG image. The image will then render itself automatically without any user interaction, and the imbedded worm will attack the user's computer and spread rapidly inside the organization. That worm may also contain a spyware payload that deploys and hides in computers. As a result, Web security concerns are at an all-time high among organizations seeking protection from a rash of spyware, Trojan horses, worms, and other Web-borne menaces.

Spyware: Today's Web-Based Malware

The most prevalent form of Web-based malware today is spyware. The number of Web sites distributing spyware has increased explosively as spyware creators continue to extend their distribution channels. Spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC demand-side research, up from fourth place two years ago.

Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number help-desk calls related to spyware are forcing corporations of all sizes to take action.

Though the consequences of spyware may be as minor as annoying advertising pop-ups, spyware has the potential to do significant damage to desktop and mobile PCs — as well as to the entire network. Spyware has the ability to capture virtually all online activity. From monitoring all keystrokes, email snooping, and scanning files

on the hard drive to changing system or registry settings, spyware is both a privacy and enterprise security threat.

An Increasing Threat Fueled by Criminal Money

Spyware is more sophisticated than traditional email-borne viruses, and the motivation of a spyware writer is drastically different from that of a virus writer. Spyware is not being created by the younger generation of script kiddies who create viruses, seeking personal pride or notoriety. Spyware writers, unlike virus writers, are motivated by profit and financial gain.

The evolution from mischievous hobby to a money-making criminal venture has attracted a new breed of sophisticated hackers and organized crime. Hackers are now much less concerned with destroying systems and knocking out Web sites. They realize that they can generate money from stealing confidential personal information and corporate data, and selling it to spammers or those involved in organized crime and fraud. IDC believes this profit-driven motivation will cause the number of attacks to increase in sophistication, frequency, and severity.

Indeed, users do appear to be aware that the sophistication of malware attacks is increasing. IDC demand-side research indicates that companies regard the growing sophistication of attacks as the top security challenge over the next 12 months. Therefore, the sophistication of spyware and other Web-based malware attacks is a major challenge that requires a new security solution.

Web Security: Traditional and New Approaches

As the number of Internet users continues to grow exponentially worldwide, the Web has become an increasingly more attractive target for writers of spyware, Trojan horses, and worms. Fortunately, Web security technology is also continuing to evolve.

Traditional Web Filtering and Web Antivirus

The explosive growth of the Internet brought with it an entirely new set of risks spanning employee productivity, legal liability, IT resource constraints, and corporate security. Businesses quickly applied basic Internet access control products to limit risks associated with employee misuse of the Web. Employee surfing of pornography, racist, hate, and other nonbusiness-related sites was the main concern of companies that first implemented this type of solution.

The primary technology used in this approach was a database of URL addresses for objectionable content, built and maintained by the vendor, which provided regular updates to its customers. Known rogue Web sites would be categorized and blocked. Web mail and newly infected mainstream sites, however, highlight the limitations of this approach. Traditional Web filtering only addresses known malware-hosting Web sites and does not actually address spyware

and other Web-based malware directly, so it offers a coarse level of security with limitations.

Traditional antivirus solutions offer a more granular level of security, but gateway scanning performance is a challenge. When today's antivirus scan engines are used to protect the Web vector, they struggle to keep up with the high volume of Web traffic generated by the large number of users connected to the Internet. This is because traditional antivirus scanning technology is batch-based. Scanning commences only after an entire file is received, and outputting starts only after the entire file has been scanned.

The result of batch-based scanning is Web latency, or unacceptable delays resulting in poor Web user experiences. Often the latency caused by Web antivirus scanning may be so bad that Web traffic grinds to a halt. Some traditional antivirus solutions attempt to get around the performance challenge by caching static Web content that has already been scanned, but this approach assumes that most Web content is unchanging. When a high volume of content is non-cacheable, then the latency of batch-based scanning returns. Other solutions limit the breadth or depth of content that is scanned. In other words, they sacrifice accuracy for added performance. But today's Web-based attacks are especially sophisticated. These new threats — often called blended threats — are complex and modular, with lightweight pieces of code designed to be hidden while they download more malware. Indeed, to defend against blended threats, which attack through multiple Internet vectors, a solution must scan not only Web traffic but also email traffic. The current level of Web scanning latency and accuracy is quickly becoming unacceptable for both IT departments and users.

A New Approach: Stream-Based Scanning

IDC believes next-generation Web security solutions must address the performance and latency issues of traditional antivirus solutions without sacrificing accuracy. Effective Web security solutions must deliver real-time performance in order to scan high volumes of Web traffic for spyware, Trojan horses, worms, and other types of malicious code. Such solutions must also scan all content deeply to ensure accurate detection of today's sophisticated malware. IDC believes implementing real-time protection at the corporate gateway is the most effective way to proactively stop spyware and other types of Web-based threats from entering the network and infecting individual computers.

Invented by gateway antivirus pioneers, stream-based scanning is based on the simple observation that network traffic travels in streams. In a stream-based scanning architecture, the scan engine starts receiving and analyzing traffic as the stream enters the network. The receiving, scanning, and outputting processes occur concurrently. In other words, processing takes place in parallel, thus minimizing processing time and ensuring that network performance is not reduced.

The result is that the time to scan a file is much faster than traditional antivirus solutions — a performance advantage that is easily noticeable to the end-user on the Web. With this high performance, breadth and depth of content scanning is maintained for high detection accuracy. Stream-based scanning technology enables the scanning of very high volumes of real-time Web traffic for malware, without bringing enterprise Web activities to a standstill and without sacrificing Web security effectiveness. Therefore, Web security requires a stream-based scanning architecture that enables real-time scanning of Web traffic for spyware and other malware.

Stream-based scanning is patent-pending technology developed by CP Secure, Inc., a vendor of real-time anti-malware solutions for enterprise-class organizations. CP Secure's Content Security Gateway anti-malware appliances are powered by stream-based scanning technology.

Conclusion

IDC believes that as Web-based threats such as spyware become more malicious and sophisticated, Web security solutions will play an increasingly valuable role as a security enhancement to traditional antivirus, Web filtering, and firewall deployments.

Given the real-time nature of HTTP and HTTPS protocols and their data streams, more sophisticated real-time scanning capabilities are needed to ensure that traffic within these Web-based paths remain free from sophisticated attacks.

Stream-based scanning provides a unique approach to addressing today's sophisticated threat environment. IDC believes emerging technologies, such as stream-based scanning, should be positioned specifically to complement a security policy and products already in place.

Stream-based scanning offers organizations key business-value propositions — addressing performance, accuracy, and effectiveness to an equal degree. Stream-based, real-time scanning of Web-based traffic supported by a comprehensive signature library provides an effective defense at the gateway against spyware and other Web-based malware threats.

COPYRIGHT NOTICE

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at gms@idc.com or the GMS information line at 508-988-7610 to request permission to quote or

source IDC or for more information on IDC Executive Briefs. Visit www.idc.com to learn more about IDC subscription and consulting services or www.idc.com/gms to learn more about IDC Go-to-Market Services.

Copyright 2006 IDC. Reproduction is forbidden unless authorized.