FIGHTING SPYWARE AND ADWARE IN THE ENTERPRISE

SARAH GORDON

While obvious security threats like fast-spreading worms have a tendency to garner news headlines, other stealthy security risks threaten businesses every day. Increasing amounts of spyware and adware programs have the ability to facilitate the disclosure of business information and risk privacy, confidentiality, integrity, and system availability. Corporations usually accumulate a vault of information that could cause serious problems if it were shared with the wrong contacts or, even worse, taken. Spyware’s evolution from simple cookies to a range of sophisticated user-tracking systems has left many businesses without the control over their proprietary data and operations.

A recent IDC survey identified spyware as the fourth greatest threat to enterprise security. Security threats infiltrating businesses today vary from an array of viruses, Trojan horses, and worms that pose a threat to consumers’ confidential data. Many will recall the first computer virus that appeared in 1981, requiring users to physically transport an infected disk to another computer for the virus to spread. Since that time, the amplified use of technology, along with improved computer speed, has provided malicious programs with the ability to spread rapidly, export personal and confidential data, and bog down computer systems. The widespread distribution of more recent virus threats such as Sasser, Blaster, and MyDoom spread rapidly and brought entire networks to their knees. Even more complex than traditional threats, a new destructive force called “blended threats” combines a number of dangers together to form one powerful enemy.

Despite their elusive nature, adware and spyware vary in both prevalence and impact. In some instances, these programs can perform innocuous activity such as keeping track of Web sites visited for advertising purposes, with little impact other than the consumption of resources. Other times, these programs will perform overtly malicious activity, such as logging keystrokes and exporting sensitive data. If left unattended or unnoticed, they have the potential to wreak havoc on computers and networks by tying up system resources and making computers completely inoperable.

It is difficult to calculate the amount of spyware and adware that exists at any given time. An AOL/National Cyber Security Alliance (NCSA) Online Safety Study recently found that...
80 percent of scanned computers actually had some form of spyware or adware present.

In reality, it is not unusual to become infected with more than one type of spyware or adware. After surfing popular kid-focused Web sites for one hour, Symantec found 359 pieces of adware left behind on a computer. This February 2005 study detected 17 adware threats and two spyware threats after browsing six sports sites. Additionally, 64 pieces of adware and two pieces of spyware were detected on five travel Websites, and 23 instances of adware and four instances of spyware were revealed on six gaming sites.

**DANGERS OF SPYWARE**

Although similar, spyware and adware perform different functions. Spyware scans computer systems, monitors Internet activity, and relays information to other computers in cyberspace. Adware has much more limited capabilities. Adware monitors Web browsing habits or preferences and transmits that information to third parties that use it for target advertising. Despite their differences, these two cousins acquire information without explicit permission or notification.

In a scan of 3 million computers systems over nine months, Earthlink found 83 million instances of spyware. Most often, employees introduce spyware into their computer systems by downloading free Internet programs such as shareware or freeware software. Spyware can also be hidden in links to e-mail messages, instant messaging clients, or in the terms of some software end user license agreements (EULAs). Hundreds of popular file-sharing programs, games, utilities, and media players come bundled with these malicious programs.

It is relatively easy to install spyware by neglecting to read EULAs and naively accept license agreements. Some spyware conforms to strong standards that present users with an easy-to-read EULA, clearly stating what the program will do. Other forms of spyware come bundled with desired software without the users' knowledge.

Spyware uses various methods to retrieve and supply data to another person. Spyware programs such as E-Blaster will track e-mail, instant message usage, and keystrokes in stealth mode. They then send periodic e-mails containing the logged information to a predefined e-mail address. Even beyond logging keystrokes, some spyware will perform screen captures, scan PCs, and corrupt data. They will also trap e-mail or instant messaging traffic and harvest sensitive personal information. Confidential information such as passwords and account numbers disclosed and acquired through the Internet provide enough information for anyone with a malicious intent to exploit.
ADWARE — THE MENACE

Analyst firm Gartner Inc. estimates that more than 20 million people have installed adware, spyware’s less harmful cousin. Despite the prevalence of adware, most employees do not recognize the dangers associated with it. Similar to spyware, some forms of adware will install themselves without any human interaction. Adware can risk the disclosure of confidential data by unknowingly redirecting individuals to “look-alike” Web sites. Internet users can also download adware by simply visiting infected Web sites. In some cases, adware downloads when users click on links in e-mail messages or instant messaging clients, or it comes bundled with other software, with or without an EULA.

When responding to pop-up advertisements, employees should exercise caution and perform due diligence. The most familiar and prevalent form of adware appears as Internet pop-up windows or bars that track Web browsing habits or preferences. This form of adware will track sites visited, browsing habits, and apparent likes and dislikes. Data is then sent to companies that purchase the services of an adware provider. This gives advertisers the capability to create tailor-made advertisements that are applicable to the user’s interests. Although adware provides information obtained by unauthorized access, it does not typically use any kind of personal identifier during the collection of data.

THE BATTLE AGAINST SPYWARE AND ADWARE

The most effective way to reduce risks from programs classified as security risks is to use a complete security solution that deals with a wide range of threats. In particular, organizations need a solution that categorizes programs according to their functionality and allows them to choose an acceptable risk level. Integrated technologies (anti-virus, firewall, and intrusion protection) should work together to provide defense-in-depth. For example, while an anti-virus solution works to protect a system against spyware, a firewall allows an organization to create a list of recipients’ personal information and to block unwanted advertisements. Furthermore, when a firewall detects that an application is trying to establish an outbound network communication (as a spyware program would to relay information to the outside world), it should automatically close the port and prevent the transmission.

Other issues to consider include the number of spyware definitions supported by a particular solution, the process used for finding new spyware programs, and how the definitions are updated.

To strengthen their defenses, businesses should also consider implementing additional security precautions, such as securing encrypted Internet connections, implementing more restrictive Web browser settings, and disabling the acceptance of third-party cookies.
In addition to the use of strong technologies, there are policy measures that can help firms reduce their risks. For example, make sure that you know and trust the authenticity of any software before you download and install it. Read the EULAs of software programs to make sure you know what you are getting; and make sure that you understand, and agree with, the program’s functionality. Examine EULAs carefully to make sure they are in agreement with your security policy. Also, as some spyware is installed using ActiveX controls, consider requiring a prompt for ActiveX to execute within Web browsers.

Stringent rules for downloading and installing software should play a role in establishing this stronghold. Restricting employees from downloading software without the express permission of the IT department is a sure way to maintain defenses. It is imperative to know and trust the authenticity of any software before downloading and installing it. The adage “Just say no!” takes on a whole new meaning when regulating the installation and downloading of unauthorized computer software.

The Federal Trade Commission warns that “Before using a file-sharing program, you may want to buy software that can prevent the downloading of spyware or help detect it on your hard drive.” Due to the breadth of security threats and risks, it is vital that organizations heed this warning and use security products that can not only deal with spyware and adware, but the entire breadth of Internet security threats. Anti-virus and firewall products allow users to protect themselves from malicious code such as viruses and Trojans, as well as expanded threats, which include spyware and adware.

Intolerance for these annoying and harmful programs has reached new heights. To combat adware and spyware, organizations and governments across the globe have started taking action to secure their defenses. Recently, the U.S. House of Representatives unanimously voted to tighten jail sentences for those who use spyware with malicious intent. Under the Internet Spyware (I-SPY) Prevention Act of 2004, individuals found guilty of using spyware to steal private information for the purpose of misusing it or to compromise a computer’s defenses could face up to two years behind bars. Those using spyware to commit other federal crimes face up to five years in prison — on top of their original sentences.

Government regulation, however, has its limits. Organizations working to protect themselves from all sides should heed warnings to reinforce security defenses by implementing strict security policies.

Various laws and acts require systems storing or transmitting certain types of data, primarily personal information related to health or finance, to conform to various types and levels of privacy protection. Any time a new program is introduced into a system, there is a potential risk. Organizations required to comply with various acts — the Health Insurance
Portability and Accountability Act (HIPAA) for healthcare organizations or Graham-Leach-Bliley (GLB) for financial services — need to ensure that newly introduced programs or processes do not introduce unnecessary exposure or risk.

As the spate of new, recent legislative and FTC activity attests, public intolerance of spyware has reached a new plateau. In the enterprise environment, spyware is rapidly becoming a serious security concern, particularly as most corporate networks allow HTTP traffic, the means by which spyware is propagated. As dependence on Internet connectivity in the enterprise increases for day-to-day business operations, risks from spyware and adware programs will continue to require a multi-level defense, as well as adherence to good security policies. Security administrators should take extra measures to maintain a strong security posture on client systems. It takes cooperation among end-user groups, technical support, and security teams to ensure that a company’s response to spyware keeps pace with this growing threat to privacy.

Sarah Gordon is Senior Principal Engineer at Symantec Security Response.

Consolidating user credentials into a single identity and protecting this with multi-factor authentication can avert online fraud

Protocom Development Systems (www.protocom.com) advises enterprises that deploying credential management solutions such as enterprise single sign-on and authentication technologies will assist them in establishing the fundamental elements for secure B2B transactions, and preventing online fraud.

“Enterprise’s reliance on online transactions has caused grave implications for data protection. At any one time, the data stored and transmitted in business-to-business, customer-to-business, or employee-to-business transactions, without the necessary security precautions, is vulnerable to attack,” Protocom CEO Jason Hart said.

Most instances of online theft, such as phishing or rogue administrator fraud, attack vulnerabilities in an enterprise’s security landscape, such as weak proof-of-identity practice, poor user credential management, or a lack of online event auditing. Enterprise single sign-on technologies strengthen enterprise networks against these threats by consolidating user credentials into a single identity, enforcing stringent verification of this identity, strictly managing user application authentication and access to online data, and auditing online events.

“Enterprise networks have never been more vulnerable to fraud. The sheer volume of credentials a user needs to perform daily jobs, combined with a notable lack of strong user verification at the enterprise network login, makes it easier than ever for fraudsters to gain access to sensitive data,” Hart added.