2004: The Year of Spyware

By David A. Vargas, CISSP

David A. Vargas is president of Vargas Advanced Technologies Group (VATG) Inc., a network security integration company located in Reston, Virginia. He has lectured both nationally and internationally on networking and network security. VATG's web site can be found at: www.vatg.com

By now, you've heard about the latest bane in computer security: spyware. Despite a spate of media attention and recent congressional action, most computer users host these malicious applications and do not realize it. What makes spyware so insidious—and why you should be concerned about it—is that it easily bypasses traditional security mechanisms, such as firewalls and antivirus programs. What's more, spyware probably runs rampant on the computers of your remote users, further exacerbating what most security professionals consider one of the largest security vulnerabilities.

Spyware applications got the name because they install themselves without the end user's explicit knowledge and then spy on the user's computer activities. Although there has been some debate in the industry as to what constitutes spyware, this author defines spyware as follows:

> ***Spyware:*** *Any application that hides its presence and performs tasks that a reasonable person would find objectionable.*

Spyware actions may range from seemingly innocuous (but potentially dangerous) pop-up generation, to stealing sensitive information, to opening a *back door* that gives an attacker complete access to a system. Some of spyware's more disturbing capabilities include the following:

- Recording surfing habits and addresses of Web sites visited
- Recording online spending habits and credit card information
- Extracting the content and e-mail addresses from each e-mail sent and received
- Detecting passwords and other confidential information
- Recording the contents of instant messages
- Recording keyboard keystrokes
- Turning on the computer's Web cam
- Reading any system file
- Changing system configurations (especially registry entries)
- Hijacking browsers

Spyware: *Any application that hides its presence and performs tasks that a reasonable person would find objectionable.*

Potential Risks

Spyware's powerful capabilities expose organizations to the following risks:

Reprinted with permission from the February issue of TechnoScope, copyright 2005, American Society of Association Executives, Washington, D.C.

- ***Loss of data confidentiality.*** Because spyware circumvents existing security mechanisms, it has a better chance of accessing business data and intellectual property.
- ***Threat to data integrity.*** Once installed on a computer, spyware can modify or corrupt any data stored on that system.
- ***Resource consumption.*** Spyware must communicate to achieve its goals. The additional traffic may impact the performance of an organization's local and wide area networks.
- ***Reduction in productivity.*** Some spyware is so poorly written that it slows down, or even crashes, the victim. Newer spyware applications so deeply embed themselves that their target systems require complete rebuilds to restore them to normal.

Spyware applications are not new, but they have garnered recent attention because they have evolved from simple tools used to gather marketing-related information (known as adware), to sinister tools that install themselves without the user's knowledge and cause serious damage.

Spyware applications are not new, but they have garnered recent attention because they have evolved from simple tools used to gather marketing-related information (known as adware), to sinister tools that install themselves without the user's knowledge and cause serious damage.

Spyware was originally used to increase the income of shareware developers. Users could use a program for *free* but a spyware application would collect information on surfing habits that would later be sold to an online advertiser. Some of the more intrusive varieties of spyware not only force the user to surrender private information, but also deactivate the application if they don't get it. For example, when a user installs an advertiser-sponsored shareware program, he or she supplies information that the spyware sends to a server, which then sends the user specifically targeted ads. However, spyware can also masquerade as or accompany desired programs and secretly transmit information.

Some of the more common methods of acquiring spyware are discussed below:

- ***Web surfing.*** Spyware has become less dependent on direct user interaction, automatically installing itself when a user surfs a hostile site or responds to a malicious pop-up. "Drive-by downloads," for example, occur when a clicked banner or pop-up surreptitiously installs a spyware application. At one of our customer sites, 1,000 spyware applications were found on one computer alone—all installed through casual Web surfing.
- ***Installing shareware and freeware applications.*** Those who download free software are at particular risk for spyware infection. As mentioned previously, free services typically collect information about your Web browsing habits to better target you for advertising from others. As a result, applications such as Kazaa and Grokster require that users agree to a licensing agreement that allows the installation of spyware. On the other hand, some programs automatically install spyware without the knowledge or informed consent of the user.

Reprinted with permission from the February issue of TechnoScope, copyright 2005, American Society of Association Executives, Washington, D.C.

- ***File sharing.*** The actual files downloaded from peer-to-peer (P2P) networks, such as Gnutella, can be camouflaged spyware, not to mention other malicious forms of software such as viruses, worms, and Trojan Horses.
- ***Clicking on e-mail attachments.*** E-mail attachments are commonly used to propagate all types of malicious software, including spyware. When the user clicks on the attachment, the spyware automatically (and surreptitiously) installs itself.

Protection

Unlike viruses, spyware is more difficult to deal with because it is either completely invisible or appears to have a legitimate purpose. Regardless, spyware will quietly monitor the victim—constantly—until the application has been removed. However, this can prove to be quite tricky. Spyware applications are hidden to minimize the possibility of interfering with them. For example, disabling spyware often disables the shareware program that installed it. One particular spyware product disables the user's Internet access if attempts are made to delete it. Some spyware applications reinstall themselves upon boot-up. Other spyware applications are so deeply entrenched that removing them requires a complete rebuild of the target system.

The best spyware protection strategy deploys a tried-and-true network security concept known as Defense-in-Depth, which protects systems by implementing multiple layers of protection.

The best spyware protection strategy deploys a tried-and-true network security concept known as Defense-in-Depth, which protects systems by implementing multiple layers of protection. Below are a few nontechnical and technical protection strategies that will help to shield your systems against spyware.

Nontechnical Protections

- ***Educate and train your users.*** The best protection against spyware is knowledge. Organizations should conduct consistent and frequent education and training that makes users aware of the implications of installing free applications, visiting certain types of Web sites, opening attachments from unknown persons or attachments they were not expecting, and so forth. Users should also be taught the importance of promptly reporting unusual computer behavior and how to adequately protect any computer that remotely accesses the corporate network.
- ***Address the topic in your organizational security policy.*** Security policies should clearly prohibit access to the kinds of Web sites that can propagate spyware, such as porn and, increasingly, shopping sites. In addition, policies should require that all installed software first be approved by management and then checked by the information technology department. Security policies should also specify the minimum security requirements for remote devices.

Reprinted with permission from the February issue of TechnoScope, copyright 2005, American Society of Association Executives, Washington, D.C.

Technical Protections

- ***Use spyware scanners.*** Spyware scanners, such as Lavasoft's Ad-Aware (see Figure 1) and Spybot's Search & Destroy, are specialized antivirus-like applications that locate and remove spyware and provide real-time protection to prevent re-infection. Yahoo! recently released a test version of a browser add-on, called Anti-Spy, that downloads a list of known spyware and then checks for its presence during a scan. Unfortunately, most spyware scanners are standalone products designed for home use. However, scanner manufacturers have started releasing enterprise-level products that include many of the centralized management capabilities found in antivirus products. Regardless of the type of scanner used, their signature files should be updated daily and they should be used to scan systems daily.
- ***Aggressively deploy antivirus programs.*** Antivirus software can also detect and delete some forms of spyware—especially those that get transmitted with viruses or are installed as Trojans. In fall 2004, both Computer Associates and McAfee released spyware modules for their enterprise antivirus products. Antivirus signature files should be updated daily, and all systems should be scanned weekly.
- ***Consider alternative Web browsers.*** Spyware applications exploit weaknesses in Web browsers to surreptitiously install themselves. Because Microsoft's Internet Explorer runs on 90 percent of the world's desktops, it is the most common target. As a result, there has been an increased interest in alternative browsers, such as, Firefox, Mozilla, and Opera. While using less popular browsers will provide temporary protection, they will eventually be targeted once they become popular. The issue of user resistance to change may negatively impact a move to alternative browsers.
- ***Be diligent with client-side security.*** Although this point might seem cliché, too many client systems are still insecure. To ensure that client systems cannot be exploited by spyware, or any other type of *malware* for that matter, they should be hardened and always have the most recent security patches installed.
- ***Encourage secure remote access.*** Remote users, such as teleworkers and mobile users, are unquestionably the weakest link in the security chain. Because information technology departments have so little control over them, they pose one of the greatest security threats. Spyware developers know these systems are vulnerable, so they are the types of systems most frequently targeted. As a result, organizations should strongly encourage remote users to adequately protect their systems with updated antivirus and spyware scanning software, personal firewalls, secure browser settings, and so forth.

Despite this recent activity, the best protection against spyware still remains a defense-in-depth strategy that emphasizes end-user education and training.

Albeit rather basic, the above recommendations should provide a great deal of protection against the current spyware threat. If these strategies are still

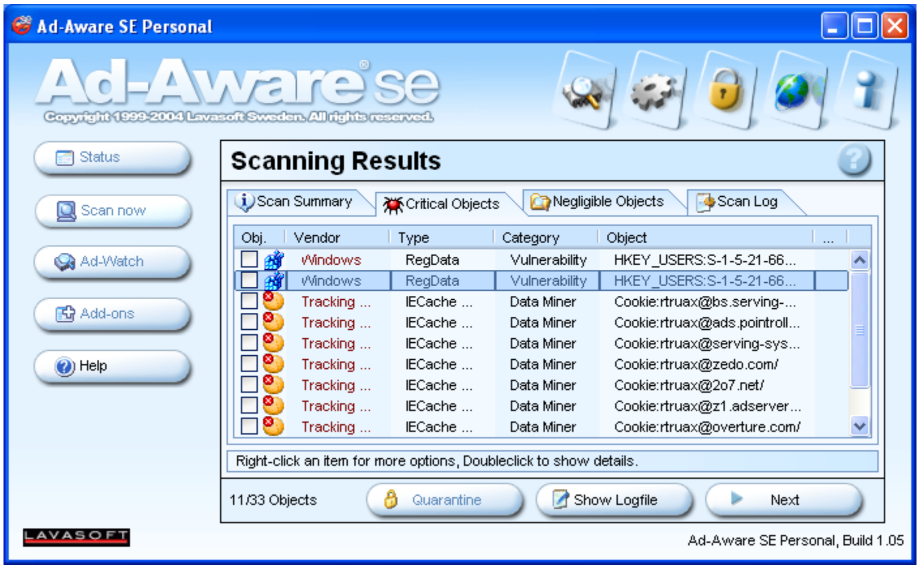
Reprinted with permission from
the February issue of TechnoScope,
copyright 2005, American Society
of Association Executives,
Washington, D.C.

insufficient, you may have to consider more technical solutions such as the configuration of outgoing filtering on your firewalls.

Looking to the Future

In retrospect, 2004 will probably be considered *The Year of Spyware*. Due to the dramatic impact these applications have had on end-user computing, countermeasures are quickly beginning to appear. Anti-spyware technology is being added to intrusion-prevention systems and VPN services, in addition to antivirus products. And in December 2004, the Federal Trade Commission filed the first federal lawsuit against a spyware developer.

Despite this recent activity, the best protection against spyware still remains a *defense-in-depth* strategy that emphasizes end-user education and training.



Scanning Results

Obj.	Vendor	Type	Category	Object	...
□	Windows	RegData	Vulnerability	HKEY_USERS:S-1-5-21-66...	
□	Windows	RegData	Vulnerability	HKEY_USERS:S-1-5-21-66...	
□	Tracking ...	IECache ...	Data Miner	Cookie:rtruax@bs.serving-...	
□	Tracking ...	IECache ...	Data Miner	Cookie:rtruax@ads.pointroll...	
□	Tracking ...	IECache ...	Data Miner	Cookie:rtruax@serving-sys...	
□	Tracking ...	IECache ...	Data Miner	Cookie:rtruax@zedo.com/	
□	Tracking ...	IECache ...	Data Miner	Cookie:rtruax@2o7.net/	
□	Tracking ...	IECache ...	Data Miner	Cookie:rtruax@z1.adserver...	
□	Tracking ...	IECache ...	Data Miner	Cookie:rtruax@overture.com/	

Right-click an item for more options, Doubleclick to show details.

11/33 Objects

Ad-Aware SE Personal, Build 1.05

Figure 1:

LavaSoft's Ad-Aware.

Reprinted with permission from the February issue of TechnoScope, copyright 2005, American Society of Association Executives, Washington, D.C.