Spyware can sneak onto systems, monitoring them, capturing user data, and transmitting it to third parties. Find out how it works and how to guard against it.

Wes Ames

Understanding Spyware: Risk and Response

Spyware—programs that monitor a computer user's activities and capture data about the user, storing the information so a third party can access it—is a relatively new phenomenon, affecting more than 50 percent of Windows operating systems failures, as reported by users to Microsoft ("Battling 'Spyware': Debate Intensifies on Controlling Deceptive Programs," Microsoft, 20 April 2004, http://www.microsoft.com/presspass/features/2004/apr04/04-20Spyware.asp). Although only in its adolescence, spyware has had an immediate impact on the Internet community and could severely threaten security. IT professionals have used the term spyware generically and specifically, with different intent. Many have heard of spyware, but few realize the specific distinctions between spyware, adware, scumware, or other species in the malware genus. The "Terminology Brief" sidebar defines several of these terms. Some terms have multiple definitions, but the sidebar covers the most common and accurate uses.

Spyware countermeasures are just now maturing beyond their initial capabilities, with many choices available to enterprises and individual users. As this field matures, threats and responses are becoming more sophisticated. One major concern has been the time lag between how quickly threats have evolved compared to how quickly countermeasures become available to deal with the threats. Spyware has evolved rapidly because of the profit motivation that spurs it forward.

Inside

Terminology Brief

The good news is that countermeasures will grow dramatically in the near future, also because of a strong—and only recently recognized—profit potential. This will help the response catch up to the threat, but only if IT professionals understand how spyware works.

HOW DOES SPYWARE WORK?

Spyware varies from mild to wild, as does user risk. At the mildest level—such as that of a simple cookie, in which a user can access a known Web site without reentering his username and password—the resulting risk is minimal. But some privacy advocates have no risk tolerance and will therefore not allow even the most basic cookie. The second and third levels of exposure are an entirely different story. These can easily exceed individuals' and enterprises' risk tolerance.

First level: Basic cookies

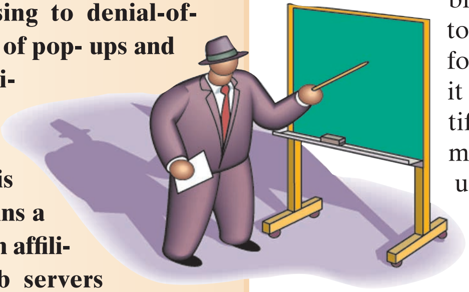
The most basic level of Web server recognition is based on a simple cookie identification for a single, specific site. Simple cookie identification enables the site to recognize the user when he returns to the site, and it allows the site to associate the user with the known stored data he has provided. This is generally useful to the user, who presumably agreed to share his typed data with the site. So the user is aware of and generally accepts this recognition and considers it low risk. This useful feature lets sites like booksellers or airlines recognize you and provide your customized preferences immediately. You rarely see simple cookie identification mentioned as a type

1520-9202/04/$20.00 © 2004 IEEE

of spyware, but some consider it as such because of the user identification and associated data storage that occurs at some sites.

Second level: Associated cookies

Many agree that real spyware stems from associated cookies, greatly increasing user exposure and risk. Associated cookies work by identifying a single user each time he connects to any member site. These cookies track activity and store data gathered from the user's interaction with each member site. Advertising companies form agreements with the member sites, which allow these advertisers to place references on the site. The references are to spyware data servers—they could be a simple image file reference with a picture or even just a single pixel. These references cause the user's browser to travel to the referenced spyware site and attempt to acquire the reference. Once there, the spyware site looks for a recognizable cookie on the user's system. Finding none, it sends one with a unique ID called a globally unique identifier (GUID) that identifies the user any time he visits a member site. Figure 1 illustrates the interactions among the user, and the member and spyware sites.



This GUID is the user's ID, and the spyware site associates all the user data with the GUID. The spyware data server tracks a user's activities and captures any information exchanged with the member site's server. If a user types in his name, account, password, or any other data, the spyware data server *could* store it with the user's GUID. When a user conducts a search or makes a purchase, the spyware data server can store that transaction in its master database. The server's goal is usually to collect user information—such as the user's name, e-mail, street address, or demographics—that is useful for targeted advertising. The server sometimes gathers other data, such as credit card information, account names, and passwords.

The problem with this scenario is that users do not see, access, or control this data; they are typically unaware of the entire process. The advertising group completely controls the distribution of user data. Although associated cookies cannot query a user's system or invoke new applications, they can record and share all of the user's activity and captured keystrokes at the member sites. Importantly, the cookies can share data without the user's knowledge. Associated cookies are a serious concern for individuals and enterprises.

In all fairness to legitimate advertisers, there is no proof of their intent to capture sensitive user data. The problem is that users definitely expose sensitive information, and companies have no obligation to inform users about the treatment and distribution of this data.

Third level: Application based

The third level of spyware is application based, and it can become totally malignant to systems and users, causing severe security exposure and risk. A key problem is that users cannot restrict application-based spyware. Such software can gain complete control of the user's system, starting whenever the user turns on the system. These applications can query the system for any desired data and can transmit anything and everything from the user's system to an outside source.

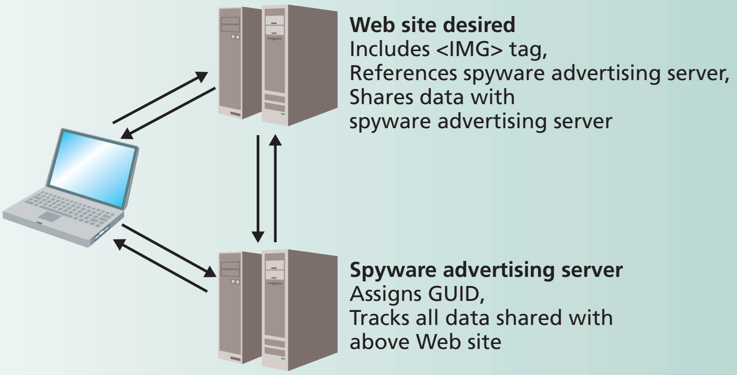
Advertisers use application-based spyware for all the reasons described previously, but this technique does not have to wait for the user to share data with a member site. Application-based spyware can open a receiving channel to accept upgrades, install new applications, and generate

Terminology Brief

- ***Adware or adbot*: This type of software generates advertising, often pop-ups. The technology employed to accomplish this simple task varies widely, and the results can range from tolerable advertising to denial-of-service levels of pop- ups and browser redirection.**
- ***Associated cookie*: This cookie contains a GUID that an affiliation of Web servers recognizes.**
- ***Cookie*: A Web server sends a small file of information, called a cookie, to be stored on a user's system. This cookie identifies the user upon his return.**
- ***GUID (globally unique identifier)*: Found in some cookies, a GUID is a unique string that identifies a specific user.**
- ***Hijacker*: This application attempts to replace your home page with another page, usually for advertising purposes or to increase traffic at a target site. Another variation of this technique will attempt to hijack a query, sending (or redirecting) it to pages other than the referenced page. In doing so, it can send users to sites they might never otherwise visit.**
- ***Malware*: The shortcut term *malware* refers to malicious software. Use of the term can be specific to software that causes harm (such as viruses or worms), or it can include any undesired software.**

advertising, all without explicit user permissions. The intelligence community also uses this type of software for investigations, and hacking communities use it for intrusions. Anyone can spy on someone else by purchasing one of many commercially available variations of application-based spyware. All keystrokes, data, and applications are accessible. Application-based spyware is clearly the category with the greatest possibility for abuse.

Figure 1. Associated-cookie-driven interactions among the user, and the member and spyware sites.


Web site desired
Includes <IMG> tag,
References spyware advertising server,
Shares data with
spyware advertising server
Spyware advertising server
Assigns GUID,
Tracks all data shared with
above Web site

Here, the user accesses a Web page from a desired site, which is also a member site that permits associated cookies to store user information at a second, spyware site. The page displays from the member site, but it references the user to the spyware site. The spyware site's data server gives the user a GUID cookie and stores all the user data from the member site.

HOW DOES APPLICATION SPYWARE GAIN CONTROL?

Application-based spyware uses very different techniques than simple and associated cookies. There are two common methods for sneaking application-based spyware onto a system, plus a third that is particularly worrisome.

Piggybacking on desired applications

The first method is to attach the spyware application to a desirable program that the user downloads. The spyware loads when the application loads, and the activities of the spyware remain hidden to the user. The spyware might be a separate executable file or it might be embedded in dynamic linked libraries (DLLs) that the host application invokes. Once activated, the spyware application configures itself to run without user knowledge or intervention. Significantly, the EULA (end-user license agreement) often discloses the existence of application-based spyware. The EULA is frequently long and tedious—and often intentionally difficult to interpret. It can include a buried reference to the spyware. A EULA might further hide the information by referencing a totally different agreement that includes the spyware description. Some companies using application-based spyware do not bother to mention it in their EULAs at all. Users often accept EULAs without understanding all the disclosures and risks. At the private-user level this is a concern; at the enterprise level, it is intolerable.

The popularity of file-sharing programs makes them a common download. It also makes them great vehicles for spyware. As a single-source example, CNET (http://www.cnet.com) offered shareware more than two years ago for several popular file-sharing programs. At the time, shareware came with Kazaa (http://www.kazaa.com), Morpheus (http://www.morpheus.com), BearShare (http://www.bearshare.com), LimeWire (http://www.limewire.com), and Grokster (http://www.grokster.com), common spyware programs. Users downloaded the shareware from CNET more than 250,000 times. Users have downloaded multiple application spyware programs in this and similar environments (http://news.com.com/2100-1023-801599.html?legacy=cnet). Today, you can find many other sources for similar software that also contains application spyware. This leads to the conclusion that users have downloaded spyware to a major percentage of the computing community.

Installing a utility program

The second popular way spyware gains control of a system is to offer utility services within the spyware itself. These programs offer services such as storing and retrieving passwords, accounts, addresses, and phone numbers. They might enhance e-mail messages or offer a new form of toolbar. In addition to performing these tasks, these utility services install software that can operate with complete freedom in your system. Once again, the user has granted freedom to an application that might take actions beyond his awareness. This is sometimes, but not always, covered in the EULA the user agreed to at installation.

Executing Java or ActiveX

Using a Java or ActiveX Web site application is the third method of transferring application-based spyware to a user's system. Once activated, the Java applet or ActiveX code can download and invoke the spyware. The result is the same as in the previous two methods, but these actions occur *completely* without a user's knowledge.

This is the most offensive form of installation and is akin to hackers breaking into a private company's computer system. As a research method, I secured a private system with firewall and antivirus security measures, then locked down the browser to enable Java and ActiveX only after asking. I then went fishing. I searched hacking sites, then switched to gambling and pornography sites, which commonly involve the most spyware activity. I also searched sites that employed this installation method. This investigation quickly yielded multiple sites that attempted to install active application-based spyware on my system without my knowledge or permission. I discovered these attempts by simply browsing through various sites. This is tantamount to external hackers breaking into private business systems; it should be illegal in just the same way.

Other considerations

Another important consideration is that a combination of several spyware techniques can exploit a vulnerability in an application to install spyware despite user permissions. For example, last year users shared the program SurferBar (also known as surfrbar or Junksurf) via e-mail distribution. The HTML-formatted e-mail contained a hidden link to a site that dropped an executable into the C drive, and then exploited a known vulnerability in Internet Explorer to automatically execute a Visual Basic script. Once installed, this nasty application placed multiple files on the system and refreshed the system's registry keys, start-up page, and Internet Explorer references every 10 seconds. Removing the application was well beyond the average user's abilities. The application added many references to pornography and gambling sites, and resulted in a denial-of-service attack, loading the browser with so many references that it became unusable.

SurferBar was a form of adware, but it could have easily been delivering an application-based form of stealth spyware. The majority of those receiving it might never know they were affected. This creative evolution is the future of spyware and other forms of malware, and the evolution is continuing. Driven by the profit motive, it will not go away. It will continue to grow and find more creative ways to learn personal information. Individuals and companies must develop strategies to effectively combat today's threats, as well as those that are likely to appear in the near future.

SYMPTOMS AND EFFECTS OF SPYWARE

Clearly, any system exposed to the Internet, using a browser or e-mail, can become a spyware victim. Symptoms might or might not occur, depending on which form of spyware you have encountered. Nevertheless, there are some simple symptoms the user should look for, and various tools exist to help detect spyware.

Spyware symptoms can include unknown disk activity, unknown CPU use, software conflicts where previously there were none, slow response, and system failure. According to Microsoft, spyware causes 50 percent of the Windows failures its users report (http://www.itnews.com.au/storycontent.asp?ID=10&Art_ID=19263). Unfortunately, a different problem might cause these same symptoms. Making a determination based on these symptoms is not easy.

In general, however, be suspicious of excessive spamming and pop-up advertising on your system; spyware might be involved. Furthermore, if your browser jumps to new Web sites you didn't specifically request, or adds new browser settings and links, spyware is quite possibly to blame. A spyware tool is the best way to detect and remove spyware.

By the end of this year, many more antivirus products will include spyware control functions.

SPYWARE COUNTERMEASURES

Several excellent spyware countermeasures are available, including Spybot Search and Destroy (http://www.safer-networking.org), Ad-Aware (http://www.lavasoftusa.com/software/adaware), and Pest Patrol (http://www.pestpatrol.com). All three packages will detect most spyware. Free or optional-donation versions, and evaluation versions, are available. Microsoft's Web site has a spyware resource section (http://www.microsoft.com/mscorp/twc/privacy/spyware.mspx). You can find more information on emerging software applications by typing *spyware* into an Internet search engine. Exercise caution when searching, though. Some unscrupulous spyware purveyors masquerade as helpful tools. Web searching for references and reviews from unbiased sources is helpful in this quest.

The spyware countermeasure products include detection and removal capabilities, and some versions of each offer various forms of resident protection. I strongly recommend that active users scan their PCs to learn the extent of spyware on their systems, then remove whatever is appropriate for their situation. Each countermeasure product discloses which items it detects (cookies or executable), and each lets the user choose which items to remove. The use of resident protection is each user's or enterprise's choice, depending on their risk aversion and their tolerance for resource consumption.

The spyware countermeasure world is changing. Many antivirus products now include spyware detection and removal, and by the end of this year, many more antivirus products will include spyware control functions. McAfee has added spyware countermeasures to its antivirus product line over the past several months, and is committed to making its product a full-service spyware countermeasure (http://www.mcafee.com/us). I talked to Bryson Gordon, a McAfee senior manager, who said, "The wide dissemination of spyware is illustrated by the number of detections we are having reported. In August of 2003, our product reported 1.5 million spyware detections. In March 2004, we saw reports of 14.3 million spyware detections." These numbers indicate that as spyware occurrences are growing, so are the abilities of these countermeasures to detect them.

For details on other antivirus applications that include spyware countermeasures, check your favorite antivirus product's Web site. Because spyware detection and removal is a new development, make sure you know the product's specific capabilities. For example, a product might have detection, but not removal, capabilities. Or, it might treat spyware and adware differently. If you are concerned about loggers (programs or hardware devices that log various types of information), does the product you are considering detect them?

The computing security industry has long appreciated a layered protection architecture, which best controls spyware and other malicious code. Personal firewalls now protect against identifiable threats more capably than ever. Some include heuristic features that can block malicious characteristics before they reach your system. Look for inbound and outbound filtering by Internet Protocol address, URL, port, protocol, application, and signature string. The product should be easily configurable to enable rapid response to evolving threats.

A strategy of strong firewall configuration coupled with spyware countermeasures will appropriately protect your system without consuming excessive system resources. If you prefer a single antivirus product to meet your spyware needs, remember that these features are still in the development stage. Using separate products is the strongest defense, but that could change in the near future.

LEGISLATION

Just as no legislation addressed viruses and computer hacking when they began, no US legislation currently addresses spyware control. At the state level, in March 2004, Utah adopted legislation—HB 323—that aims to control spyware (http://www.le.state.ut.us/~2004/bills/hbillenr/hb0323.htm). As you might expect, spyware companies voiced their objections, but many computer industry leaders also voiced objections, which was particularly interesting. Although this legislation's effectiveness remains to be seen, it has clearly brought attention to the issue. Opponents sought and won a temporary injunction to halt the legislation in June 2004.

On a national level, the US Senate is also considering an antispyware law (http://burns.senate.gov/index.cfm?FuseAction=PressReleases.View&PressRelease_id=1077). The bill, S. 2145, was in committee hearings when I wrote this article. The US House of Representatives is also drafting bills such as HR 2929 (Securely Protect Yourself Against Cyber Trespass Act) and HR 4661 (the Internet Spyware Prevention Act, http://www.cdt.org/privacy/spyware). The potential impact of such legislation is enormous; how accurately the final text captures the requirements in an enforceable fashion remains to be seen. Because congressional committees are also acting on this issue, it is highly possible that some form of legislation in this area will become law. Microsoft has proposed a different strategy, wherein the industry provides improved tools and avoids legislation that might not adequately thwart what Microsoft calls "deceptive software." In addition to including a spyware resource section on its Web site, Microsoft is improving Internet Explorer controls to thwart these applications.

Legislating a solution to high-tech spying is certainly challenging, but legislation could go a long way toward solving the problem. Imposing appropriate limits on the actions and behavior of applications is possible, especially when the computing industry and legislative bodies work together. The challenge for spyware legislation is that many corporations profit from spyware. The ability to deliver targeted spam, for example, is highly profitable. As a result, any legislation that would limit or eliminate profits from these types of invasions will face intense lobbying. It will be interesting to watch developments in this battle between personal privacy and special-interest profits. While the battle plays out, individual users should remain aware and take actions to protect their systems and privacy.

Most knowledgeable computer users probably agree that limitations are necessary on the type of data that any spyware product could legally collect or retain without the user's explicit permission. Such limitations could include restrictions on keystroke-captured account and password data, or credit card information. This simple control could begin to define the necessary legal controls on the spyware phenomena. But in the final analysis, the user remains responsible to be aware of what runs on his machine. Users who remain blissfully unaware of spyware's effects will have to deal with the conflicts and side effects of such an approach. With today's tools, users can prevent spyware problems with a little effort. The tools of tomorrow will hopefully make that task automatic. ■

Wes Ames *is an associate technical fellow and ITAS security specialist at Boeing. Contact him at wes.ames@boeing.com.*

For further information on this or any other computing topic, visit our Digital Library at http://www.computer.org/publications/dlib.