Invasive Software: Who's Inside Your Computer?

George Lawton

Technology frequently turns out to be a double-edged sword. For example, as technology has increased connectivity and network accessibility, concerns about privacy and security have grown. And as this concern has increased, invasive technologies—such as those that let third parties plant software on a PC and monitor users' activities from across a LAN or the Internet—are becoming more sophisticated.

At one end of the spectrum, new customer-relationship tools track activity with user consent. At the other end, organizations have developed sophisticated spyware that third parties can place on systems without permission, log user keystrokes, and track online movements. Invasive software can even collect sensitive information that users enter into online forms, including Social Security numbers, credit card numbers, and passwords.

Modern technology makes it easier to monitor computer users because digital activities leave tracks, noted James Dempsey, a surveillance consultant with the Center for Democracy and Technology, which advocates for privacy and other causes.

And since the 11 September terrorist attacks in the US, the political and legal focus has been less on privacy and more on security, noted Larry Ponemon, CEO of the Privacy Council.

Another complicating factor is that consumers have little legal protection

against private-sector surveillance, Dempsey added.

While many users and privacy advocates criticize invasive technologies (see the sidebar "Backlash Against Invasive Software"), some practitioners defend them as a legitimate way to gather important market-related information. Others say that not all surveillance technologies are invasive, as some involve clearly informed user consent.

NEW INVASIVE SOFTWARE

Cookies are an early example of technology that lets outside parties access users' computers. Cookies are code that a Web site's server can send to individuals' browsers and store on their hard drives. Users can provide information such as a password for a cookie to store, or a cookie can record information on its own, such as user activities while visiting the Web site.

When users visit the site again, the browser sends the information in the cookie back to the Web server so that the server can, for example, open a protected page without a password or send personalized Web pages or advertisements. Some cookies can even track user activity across multiple Web sites.

Brilliant Digital Entertainment

More than 75 million people have downloaded Kazaa software, recently purchased by Sharman Networks, to conduct peer-to-peer (P2P) file sharing over Kazaa-enabled networks.

In the third quarter of this year, though, Sharman plans to include additional software with the Kazaa application that would enable user PCs to operate as part of the planned Altnet grid-computing network.

Brilliant Digital Entertainment (http://www.brilliantdigital.com) plans to commercialize Altnet by selling its services to customers who would use participating PCs' excess computing and storage capacity to improve content distribution by moving material to the edges of the Internet and closer to recipients, said Altnet CEO Kevin Bermeister. Customers could also use the service for distributed storage and to perform massively parallel distributed computations.

Critics contend that Brilliant has not meaningfully notified users that their Kazaa downloads will include Altnet software. They say the information about Altnet is buried deep within the company's long software notification, where most users will not find it.

Another concern is that once the software is on a computer, Altnet could use the PC without having to get permission each time and do work that eats up host resources for activities that benefit only Brilliant's customers.

Bermeister said that users will have the right to deny access to network operations or leave the program altogether. Altnet plans to encourage participation with free movie and concert tickets and CDs based on the level of resources users make available.

The Privacy Council's Ponemon said that P2P-application software has had security problems. These problems could leave user systems with holes that hackers could exploit to take over a PC, upload malicious software or illegal

content (such as child pornography), or even use to attack other systems.

According to Bermeister, Altnet uses P2P technologies with built-in security, such as digital certificates designed to verify the identity of the person who sent the shared file.

Spyware

Spyware is software, installed by a third party without the user's fully informed consent, with undisclosed subroutines that track a host's Internet activity and send the information to a spymaster (see the sidebar "Finding Spyware on Your Computer").

Users sometimes receive spyware hidden in another application. The spyware then runs in the background to capture keystrokes typed by users or it can track Internet activity by running the user's traffic through a spymaster's proxy server. In some cases, spyware sets up a TCP/IP link that transmits information to the spymaster.

Various spyware products—such as Spector (http://www.spectorsoft.com), KeyKey, and WinWhatWhere—let individuals or companies track the computer-related activity of workers, spouses, and other targets.

In addition, some companies utilize marketing technologies—including VX2's RespondMiter and Ezula's ContextPro, HOTText, and TopText—that potential customers download with file-sharing software and that record their online activity.

ComScore's MarketScore monitoring technology deploys a small, short-lived applet on a PC that sets the computer's proxy settings so that all of the host's Internet traffic first flows through the company's network.

ComScore Vice President Daniel Hess said MarketScore technology is installed only with the permission of users, who receive incentives such as prizes, and only aggregates information for marketing purposes.

However, critics worry that individuals or companies that deploy spyware may not tell their targets about the application's installation, may lie about the software's nature, or may bury disclosure information deep within a long, complex licensing agreement.

Grey McKenzie, CEO of SpyCop, a spyware-detection software company, noted, "We get reports all the time about people and companies who have been infected by surveillance spyware." He said industrial spies sometimes use spyware to steal a company's important or sensitive information. "One company we talked to figured they lost close to a million dollars because of monitoring spyware."

Pop-up downloads and pop-over ads

Some Web-site hosts let software makers run pop-ups for *one-click opt-install* advertisements, which download software to the computers of users who click on them. In some cases, software makers notify users that clicking on the pop-up will download software. In other cases, called *drive-by downloads*, users aren't informed they would be downloading an executable.

Pop-ups typically install a piece of Java or ActiveX code on a PC that runs whenever a user launches the browser. The code requests that an advertiser's server pop up more windows in the browser.

Some companies that use pop-up downloads distribute software that may benefit a user, such as Gator Corp.'s eWallet, which remembers passwords and fills in online forms automatically. Privacy advocates still oppose the tactics used to install the software.

Backlash Against Invasive Software

Several individuals and groups, most of whom act anonymously, are trying to undermine the inclusion of invasive software in file-sharing programs.

For example, an anonymous software developer called Dr. Damn has stripped the advertising and user-tracking features from several popular programs and distributed them, along with other similarly neutered software, on the Clean Clients Web site (http://www.cleanclients.tk/).

"My goal is to give users a choice between running spyware on their computers and being bombarded with advertisements, and running no spyware with fewer advertisements," explained Dr. Damn.

The most popular version of file-sharing software that an unauthorized third party has stripped of spyware is Kazaa Lite, supposedly created by a Moscow resident known as Yuri and distributed at such places as http://www.kazaalite.com. Sharman Networks, owner of the Kazaa peer-to-peer software, has already begun trying to have software-access sites remove Kazaa Lite and plans to pursue court orders to stop all distributions.

Meanwhile, SpyCop, a spyware-detection-software company, has developed products that search a hard disk for code from known computer-monitoring spy programs and registry calls typically used by these applications. The products then give users an opportunity to disable the spyware.

Lavasoft (http://www.lavasoftusa.com) makes Ad-aware, a free download that scans a hard drive for known Web bugs and advertiser spyware and that lets users run a removal utility to eliminate the programs.

However, a popular, advertising-supported multimedia program called RadLight (http://www.radlight.net) comes bundled with two other programs that, as its user agreement announces, can detect and delete Ad-aware, which otherwise would delete RadLight.

Packet sniffers can also identify spyware by monitoring traffic and detecting when a PC starts sending data unrelated to user activities over the Internet. This can indicate that a spymaster is using invasive software to steal information.

Finding Spyware on Your Computer

Several Web sites have lists of alleged or suspected spyware, promise to identify whether a specific application is actually spyware, or give visitors a chance to report possible spyware.

For example, Spychecker.com has a database of alleged spyware products at http://www.spychecker.com. The Web site also lets visitors enter the name of an application to determine whether Spychecker has identified it as spyware.

TomCat PC Systems' TomCat Internet Solutions offers a similar database at http://www.tom-cat.com/spybase. Gibson Research Corp., which sells security and data-recovery products, provides a list of alleged spyware at http://www.grc.com/oo/spyware.htm and identifies suspected spyware at http://www.grc.com/oo/suspects.htm.

Gator also distributes user-tracking software via pop-up downloads. After determining browsing habits, Gator software can launch a pop-over advertisement from its servers that is designed to appeal to the user. These advertisements, paid for by Gator's customers, cover another company's banner ad.

Other pop-up downloads, implemented for companies by online marketing firms such as L90 and InternetFuel, include software that tracks users as they visit any of 600 participating major Web sites, including those for Hollywood.com and the US's public broadcasting system.

Pop-up download proponents say that tracking online activities lets advertisers provide useful ads that target user interests. Opponents, however, say pop-up downloads either should not be run because they trick users into clicking on them or they should be clearly labeled.

Jason Catlett, president of Junkbusters Corp., an organization that opposes unsolicited Internet direct-marketing communications, said online advertising rules of engagement are necessary. However, he added, these guidelines are worthless if an organization buries important consent-related information within a long, complex statement.

Dr. Damn, an anonymous software developer who has removed user-tracking programs from applications and then redistributed them, said many people don't know about invasive software and don't even know it's on their computers. He added, "As if the privacy concerns weren't bad enough, these programs take system memory, Internet bandwidth, processor power, and hard drive space. They also tend to be poorly written and cause system crashes."

Products like Panicware's Pop-Up Stopper (http://www.panicware.com) promise to stop pop-up downloads and pop-over banners. The Opera Web browser has a built-in pop-up stopper and also will not install the ActiveX components that enable many pop-ups.

E-mail tracking

Privacy Council research has found that within the last year, the portion of e-mail messages with the capability of tracking recipients' online activities has increased from 1 in 1,000 to 1 in 50. The most invasive e-mail-tracking approach is surreptitiously installing spyware on the target's machine via a Trojan horse or a virus that executes when the user opens a message or attachment.

Web beacons. The simplest approach to gathering information about a user via e-mail is a Web beacon or Web bug, which is frequently sent with mass mailings. With many e-mail applications, a message with HTML-based graphical content has links on which users must click to download images. The link can contain code that serves as an identifier for the e-mail address to which the message was sent. Clicking on the link activates it, permitting the sender to tell if a particular user responded.

Cookies. The second approach includes cookies sent in connection with HTML code that is part of an e-mail message. The recipient must connect to a Web server to access the code, allowing the server to send a cookie.

A concern with third-party e-mail cookies is that they could identify a user, via an e-mail address, with specific online activity. In contrast, many Web sites, after battles with consumer and privacy advocates, now typically do not use cookies to link specific users with their Web activity but instead aggregate multiple users' browsing behavior.

Another concern with e-mail-tracking technologies is that companies don't necessarily give consumers a chance to opt in or out, although browsers and e-mail applications provide ways to block cookies. According to the Privacy Council's Ponemon, the only legitimate use of a Web beacon is with recipient consent.

Magic Lantern

The US Federal Bureau of Investigation (FBI) is reportedly working on its own invasive software, called Magic Lantern, for investigating criminal suspects (see *Computer*, March 2002, "Key Snooping Technology Causes Controversy," p. 27).

According to an FBI affidavit and published reports, the FBI would install Magic Lantern on a computer by sending a criminal suspect an e-mail note with an attachment that, if opened, inserts a Trojan horse. When recipients launch Pretty Good Privacy encryption software, they would also activate the Trojan horse. The software would then log the suspect's keystrokes, including the PGP password, which would let the FBI decrypt user communications.

It is not yet clear whether the FBI would need physical access to a user's computer to retrieve information that Magic Lantern gathers. The FBI has refused to comment further.

Concerns include uncertainty about Magic Lantern's full capabilities, and whether hackers could subvert it for their own uses. "I'm sure any decent cracker could redirect the Lantern's output to another location, thus allowing people to spy on others," Dr. Damn said.

David Sobel, the Electronic Privacy Information Center's general counsel, said he is worried that because the software is not physically installed on a suspect's computer, the FBI would not need a court-issued warrant. He contends that Magic Lantern should be considered a wiretap that requires a warrant.

Observers have mixed feelings about invasive technologies' future. Some say that consumers and businesses that work with marketing firms will eventually weed out companies with intrusive practices.

Others say that companies will continue to want information about people and thus will demand invasive technologies.

"My gut tells me the privacy universe will get worse before it gets better," the Privacy Council's Ponemon said. "Over the next decade, there will be a war between those who will fight to maintain their privacy rights and organizations that believe privacy does not exist. Consumers need to be more diligent."

Junkbusters' Catlett said, "What is necessary are laws that require consent and give people who are harmed and whose privacy is abused the right to sue the wrongdoer."

Accordng to Dr. Damn, future laws might not help because companies can just relocate to countries without legal protection against invasive software. Thus, he predicted, more individuals will take matters into their own hands and begin distributing applications they have stripped of spyware. ■

George Lawton is a freelance technology writer based in Brisbane, California. Contact him at glawton@glawton.com.

Editor: Lee Garber, *Computer*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org