WSJ.com THE WALL STREET JOURNAL. ONLINE

April 26, 2004

THE JOURNAL REPORT: TECHNOLOGY

What's That Sneaking Into Your Computer?

New types of insidious programs are burrowing into PCs, wreaking all sorts of problems. Here's what's being done to combat them.

By DAVID BANK
Staff Reporter of THE WALL STREET JOURNAL

April 26, 2004; Page R1

John Gosbee was sitting up in bed on a cold night, surfing the Internet with his laptop on his knees. Suddenly, the computer's CD-ROM tray popped open, seemingly on its own.

"What on earth is going on?" Mr. Gosbee, of Mandan, N.D., said to himself. "It was like it was possessed," he recalls.

His laptop emitted a high-pitched "Uh-oh."

Uh-oh is right. The pranks were a setup for the message that appeared on his screen: "Dangerous computer programs can control your computer hardware if you fail to protect your computer right at this moment!" That was followed by a plug for a program called Spy-Wiper that promised to clean out any rogue software.

Christoph Niemann

As if that wasn't alarming and annoying enough, the very next day the computer at Mr. Gosbee's one-man law office was similarly hijacked. The CD and DVD trays both opened; only one closed. Then came the same ad for Spy-Wiper, which kept popping up on both machines.

"I was getting ticked," Mr. Gosbee says.

As Mr. Gosbee and countless other computer users have discovered: It's a war out there. While malicious hackers are spreading viruses all over the global computer network, advertisers and scam artists are propagating other pests that are arguably even more annoying. They're called spyware -- and the implications for consumers are only beginning to be felt.

Indeed, spyware -- small programs that install themselves on computers to serve up advertising, monitor Web surfing and other computer activities, and carry out other orders -- is quickly replacing spam as the online annoyance computer users most com- plain about. The outrage has grown to the point that politicians are threatening legislative controls on the tactic. But in their most benign form these programs have a powerful appeal to advertisers, and some marketers are banking on the idea that people eventually will grow accustomed to some use of such invasive software.

"Snoops and spies are really trying to set up base camp in millions of computers across the country," said Sen. Ron Wyden, an Oregon Democrat, at a March hearing on proposed legislation he is co-sponsoring to tackle the problem. A Republican co-sponsor, Sen. Conrad Burns of Montana, said at the hearing: "I'm convinced that spyware is potentially an even greater concern than junk e-mail, given its invasive nature."

Computer security experts say there are nearly 1,000 forms of spyware. Most spyware programs have what proponents argue is a legitimate purpose -- delivering ads specifically targeted to a user's online behavior. But even this is maddening for most consumers, judging by the numbers of those who choose to expunge such programs from their computers. Many people don't want to be bombarded with yet more advertisements, even those in sync with their particular tastes.

A ROGUE'S GLOSSARY

Spyware -- Software that monitors computing habits, such as Web-surfing patterns, and transmits the information to third parties, sometimes without the explicit authorization or consent of the user.

Key logger -- A form of spyware that logs each keystroke or other activity in a system. Such software can gather credit card numbers, passwords and other sensitive information and transmit it to third parties.

Trojan or Trojan horse -- A software program that appears to have a useful function, such as a game, but includes hidden and potentially malicious features. Trojans sometimes evade security mechanisms by tricking users into authorizing access to their computer systems.

Adware -- Software that displays advertising. Adware often includes spyware so ads can be targeted to users' interests and habits.

Cookie -- A type of file some Web sites place on users' computers to enable personalization of Web content. Most cookies are harmless, but some that record Web surfing habits and personal information are considered spyware.

Back door -- A security vulnerability installed by a virus or a Trojan to give an attacker easier–and usually secret–access to a computer system, often bypassing security safeguards.

Eula -- Shorthand for end-user license agreement, the legally binding contracts that accompany most software programs and govern the terms of use. Most users with computers infected by adware and spyware have agreed to install the programs by clicking "Accept"at the bottom of the eulas that accompany file-sharing software and other free programs.

Sources: SANS Institute, Trend Micro Inc.

Even worse, though, are the more nefarious members of the spyware species -- those that carry orders to snatch passwords and credit-card numbers and run other online scams. These include "key loggers" that record every tap on the keyboard, and "dialers" that direct computer modems to dial premium-rate numbers, running up phone-bill charges for unwitting computer users. Some spyware programs reset browser home pages, while others redirect search requests. Some can slow a computer's performance to a crawl by hogging its memory.

Network Associates Inc.'s McAfee security unit says reports generated by its VirusScan software of what it calls such "potentially unwanted programs," or PUPs, grew to nearly 2.6 million in March from 643,000 last September.

Mr. Gosbee, the North Dakota lawyer, isn't waiting for Washington to take action. He followed Spy-Wiper's trail to an Atlanta man and three Georgia corporations he says were behind both the original problem -- his computers acting up at someone else's command -- and the supposed solution. He has filed suit in the state district court in Mandan under North Dakota's computer fraud and racketeering laws against MailWiper Inc., Eskrawl Inc. and SpyDeleter Inc., all of which are associated with Rob Martinson, also named in the suit, who is listed as the CEO of MailWiper in documents filed with the Georgia Secretary of State.

Neither Mr. Martinson nor his lawyer, Scott Porsborg of Bismarck, N.D., responded to requests for comment on the suit. But in a response filed in connection with the suit, Mr. Martinson denied any illegal actions and said any problems Mr. Gosbee may have experienced "are the result of visiting infected Web pages over which the defendants have no responsibility or control." The response says Spy-Wiper is a legitimate program to delete spyware and adware.

Ads You Want?

Nonetheless, Mr. Gosbee took personal affront at the invasion of his privacy. "I thought it was rude and inconsiderate," he says.

That kind of reaction is a problem for companies that want to monitor your online behavior to find patterns that mark you as a promising target for a particular advertiser or advertisers, and then serve up those ads on your computer.

The program that WhenU.com Inc. uses to deliver ads to people's computers for its clients has been installed more than 100 million times, the marketing company says -- and uninstalled 80 million times. That's testament, says Avi Naider, chief executive of the New York-based start-up, to the user-friendliness of WhenU's software: It's easy enough for people who don't want to see the ads to stop receiving them. But Mr. Naider also acknowledges that the high uninstall rate reflects the disdain with which most consumers view the technology.

The uninstall rate for the behavior-tracking and ad-delivery software from **Claria** Corp., based in Redwood City, Calif., is about the same. The company claims access to 45 million computers in its Gator Advertising Information Network, but acknowledges that its software has been removed 155 million times over the past five years.

Despite their uninstall figures, Claria and WhenU position themselves as legitimate distributors of software and advertising that users actually want. Claria, which last year changed its name from Gator Corp., filed with the Securities and Exchange Commission earlier this month for an initial public offering of its stock.

With consumers up in arms and legislators taking note, these "desktop advertising networks" are seeking to distinguish themselves from illicit distributors of spyware, who dispense their snooping devices through Web pages that can install programs on a visitor's computer with no notice -- in so-called drive-by downloads -- or through bogus e-mail spam offers or misleading pop-up ads.

In contrast to those tactics, most people targeted by spyware consent to their own victimization, however unwittingly, by downloading other software from the Web. WhenU's spyware program, for instance, comes with the BearShare file-sharing program from Free Peers Inc., with free games from eUniverse.com Inc., and with screen savers and other doodads, like clip art and computer wallpaper, from Freeze.com LLC. Claria's GAIN ad server comes with video-player software from DivXNetworks Inc., Kazaa file-sharing software from Sharman Networks Ltd., and Claria's own Gator "e-wallet," a program for storing passwords. Many of the programs people intentionally download are available for a fee, but can be gotten free if users consent to the installation of additional data-collection and ad-serving software by clicking "I agree" when presented with the terms of the license -- terms many users never bother to read.

Once it's in place, WhenU's software traces the computer user's searches, not only at general search sites, but also in search boxes on retail and other sites. It also notes which Web sites the user visits, and the content of Web pages viewed. "The software allows us to understand what a consumer is searching for, even if they're not on a search engine," Mr. Naider says.

When a match is found with an advertiser's profile, an ad is presented instantaneously on the user's screen. The idea is not only to match the ad to the user, but also to present it at the moment when it is likely to be most effective. So, if WhenU's software is embedded in your machine and you are reading articles about London, visiting airline Web sites or pricing tickets on Orbitz.com, you might get a travel-related ad, perhaps from an Orbitz competitor.

Fighting Back

Software has long had some of these capabilities. For years, Web sites have installed "cookies" on visitors' computers -- small programs that identify repeat visitors and in some cases can tell marketers which other sites a computer user visits regularly. But while some privacy advocates have objected to cookies, these limited programs generally serve what many consumers consider a useful purpose: making life easier for repeat visitors to a Web site by eliminating the need to register every time, for instance, or by generating suggestions based on past purchases.

Spyware, by contrast, is a much more powerful tracking technology, capable of monitoring a computer user's every move online. The same capabilities that make it more worrisome from a privacy standpoint make it a powerful tool for targeting ads.

When the Federal Trade Commission solicited comments in anticipation of a hearing it held last week on spyware, consumers had no shortage of complaints. "Spyware has become rampant on my machine," one letter writer complained. "I've removed them a dozen times and my spyware-blocking software doesn't prevent them from coming back." Contacted after he sent the letter, the writer, who asked that his name not be published, says he has changed his Web-surfing behavior. "I don't go and search for anything to do with entertainment, Hollywood, music," he says. "All sorts of advertising started appearing, even when I wasn't at a particular site."

One girl in California downloaded smiley faces to decorate her e-mails. "Within hours, our computer was virtually inoperable," her mother wrote to the FTC. A Texas man complained about a pest picked up through e-mail. "Now it has gotten a porn generator going and I get 30 to 50 messages a day from different porn sites," he wrote to the commission.

Politicians are taking up the cause, and not just in Washington. Utah's governor last month signed into law the "Spyware Control Act," the first such state law, with fines of up to $10,000 per violation. The bill requires companies, even those outside the state, to make full disclosure of the changes downloaded software makes to users' PCs in Utah, what behavior is recorded, what information is transmitted to central servers, how often ads will appear and even what they will look like. It's not clear how effective Utah's effort will be -- it has been criticized as being both toothless and as an onerous burden even on legitimate software companies. Opponents may also challenge it on the basis that it effectively seeks to regulate Internet commerce beyond Utah's borders.

In Washington, Sens. Burns and Wyden, along with Democratic Sen. Barbara Boxer of California, have introduced the Spyblock Act, which would prohibit software installations without notice and consent, and require reasonable uninstall procedures. Both the federal legislation and the FTC hearings are aimed at drafting a national policy that would pre-empt state-by-state action.

Internet service providers and vendors of antivirus software are also jumping in. **EarthLink** Inc. has introduced a Spy Blocker service, and **Time Warner** Inc.'s AOL unit has a similar offering. McAfee claims its new AntiSpyware program catches almost all lurking programs. Mike Block, assistant vice president for information technology at Equitable Bank in Milwaukee, says PestPatrol Inc.'s scan wiped out pesky bugs that had resisted the free software he tried first.

Computer users can take other actions as well. For example, resetting your Web browser's security level -- which can be accomplished with a few clicks of the mouse -- can make it harder for Web sites to install programs on your computer. Installing a stronger firewall can also help by limiting the ability of spyware installed on your computer to access the Internet, which prevents it from reporting on your activity. And simply reading the fine print on "end user licensing agreements" that come with most software downloads can keep you from unwittingly inviting spyware into your system.

Going Mainstream

But even as technical and legislative solutions seek to root out the worst offenders, spyware is going mainstream.

In its IPO filing, Claria noted that its advertising clients include such familiar names as Orbitz and FTD Inc. And this month Google announced a free e-mail service with a catch: Its computers will search messages for key words and trigger related ads.

The pattern isn't new. Several years ago, consumer advocates and others derided search sites for providing sponsored links from advertisers; now such "paid search" is the fastest-growing revenue stream for companies such as Google and Yahoo Inc. Now advertisers want to go further, and target not just consumers' demographic profiles, as in television and magazine advertising, nor even just their online search behavior, but their overall behavior as they read articles, compare products and click between links.

Scott Eagle, Claria's senior vice president, says such targeting of online behavior is "zero-waste" from an advertiser's point of view. A frequent traveler who always books on, say, Orbitz, is of high value to other travel sites, Mr. Eagle says. "They might say, 'Wow, I want to talk to that person. That person is so valuable, give that person a $100 discount.'" At the same time, users who aren't interested in travel are likely never to get a travel ad, he says.

WhenU's Mr. Naider says spyware -- he prefers to call it software-based advertising -- is on the verge of mass-market acceptance. He says advertisers are willing to pay what he calls a "considerable premium" for highly targeted advertising.

"Software-based advertising is going to be extremely powerful," he says. "People are going to look back and say, 'It was so obvious.'"

--Mr. Bank is a staff reporter in The Wall Street Journal's San Francisco bureau. Michael Totty, a news editor with The Journal Report based in San Francisco, contributed to this article.

Write to David Bank at david.bank@wsj.com[1]

URL for this article:
http://online.wsj.com/article/0,,SB108258068106489627,00.html

Hyperlinks in this Article:
(1) mailto:david.bank@wsj.com