Spyware: Sneaky, annoying threat

Programs can bring computer to 'screeching halt'

NEW YORK (AP) -- David Eckstein turned on his computer one day and launched his Web browser, just as he had every day. This time, however, CNN.com did not automatically open. Instead, the page was a search engine he'd never heard of.

Eckstein tried changing the browser settings back to CNN but the search engine would return whenever he rebooted. Finally, he just gave up.

The San Francisco marketing consultant is yet another victim of spyware, an amorphous class of software that mostly gets onto people's computers without their knowledge. So resource-hungry, it often renders the machines unusable.

"It makes you want to throw your computer out the window," Eckstein said.

In the past year, the problem has become epidemic as people spend more time online and spyware developers get more aggressive.

"It makes spam look like a walk in the park," said Bob Bowman, chief executive of Major League Baseball's Internet unit, which in June started banning new advertisers from using such techniques.

As part of a government-backed study, technicians visited Jenna Dye recently in Young Harris, Georgia, and found 1,300 spyware-related items on her machine.

"It would shut itself down in the middle of doing stuff. We had lots of pop-ups. The (CD-ROM) drawers would pop open," the mother of two complained. "It's frustrating. We spent $1,800 on our computer and we didn't want to use it."

Until the machine was cleaned up, Dye and her husband would make 2 1/2 hour trips to the nearest mall to avoid shopping online. "We use it every day now again," she said.

Spyware was found on the computers of 80 percent of participants in the study, conducted by America Online Inc. and the National Cyber Security Alliance.

Since EarthLink Inc. began offering free anti-spyware tools, each scan has found an average of six such programs. When including "cookie" data files that online sources use to track user behavior, the average rises to 26.

'You don't just have one'

The most common type of spyware is more properly termed adware, its main goal to generate pop-up and other ads.

Browser hijackers, the kind Eckstein got, direct users to rogue search engines, from which spyware developers or distributors get a commission. Dialers scam users by making international phone calls that carry hefty per-minute surcharges. A rare but malicious form can steal passwords and other confidential data.

The intrusive programs aren't always well-written and can use resources inefficiently.

"Often, you don't just have one. You might have a half-dozen or even a dozen that can bring your computer to a screeching halt," said Tim Lordan, staff director of the Internet Education Foundation. "They are undermining confidence in the Internet. People are getting fed up."

The most common way to get spyware, including adware, is to download file-sharing software, screensavers and other free programs that rely on revenues from such tagalong programs to cover costs. Spyware developers consider it part of the bargain, though they also depend on users' fascination with freebies.

"A lot of them say, 'I'm going to get free smileys in my e-mail or some sort of free ... download' without realizing the resource drain the sponsoring software is going to cause," said Wayne Porter, co-founder of SpywareGuide.com.

Users themselves invite spyware by breezing through prompts and not reading licensing agreements they are required to accept. Consent to spyware is often buried there.

Many of the larger companies whose software is delivered online with freebies have tried to clean up their act to the point that many don't actually harvest data anymore, though the term "spyware" has stuck.

And their methods for disclosure and removal have improved in response to consumer complaints.

But for every reputable operation, scores of shadier ones, often located abroad, are intent on tricking users into accepting spyware without any accompanying software.

In a technique known as drive-by downloading, code embedded within pop-up ads or on Web sites that offer free songs, games or even pornography can instruct computers to begin downloading the rogue programs with minimal warning.

Sometimes, those warning prompts even are programmed to keep popping up until users finally give up and say "yes," said Neel Mehta of Internet Security Systems Inc.

And exploiting known flaws with Microsoft Corp.'s Windows operating system or the Internet Explorer browser, spyware developers can bypass the prompts entirely.

"In the rush of doing things, people get confused and end up hitting one wrong button, and all of a sudden stuff is on your computer and you can't get it off," restaurant manager Damien LaRuffa said.

'It goes and reloads it'

His Washington, D.C., restaurants lost two computers for a few days because an assistant manager apparently was tricked into accepting a fake pitch for anti-spyware software. LaRuffa said the repair bill exceeded $400.

Matt Davin, technical services manager at a repair shop in Walla Walla, Washington, estimates that half his jobs are directly tied to spyware. Customers, he said, often blame it on their kids downloading free programs.

Spyware can infect power users as well. Just ask Ricky Rodrigue, who runs Dell Inc.'s customer support center. His son invited spyware onto his home machine while downloading games, and he once found more than 100 spyware items on his work machine.

"That's how creative (they are) and how challenging it is to protect PCs," Rodrigue said.

The less innocuous programs can usually be removed manually or by running one of several anti-spyware tools, many free. The nastier ones, however, immunize themselves and persist.

"Almost every new threat released today comes with a reinstaller so that as soon as you try to remove it, it goes and reloads it," said Ron Franczyk, co-founder of anti-spyware vendor Giant Company Software Inc.

Many spyware files carry names that mimic key Windows components and even hide among them in folders typically reserved for system files.

"How do you know if you need a spool.exe?" asked Vilis Ositis, chief technology officer at Blue Coat Systems Inc. "Windows comes with thousands of files. How do you know which ones you need and which ones are spyware?"

Congress is working on a ban, and industry groups have launched efforts to educate consumers and fight back with technology. Experts believe a solution will ultimately involve a combination of law enforcement, education and engineering.

"We're at a crossroads," said Ari Schwartz, associate director of the Center for Democracy and Technology, a privacy-advocacy group.

Fail to properly address spyware, Schwartz warned, and "users will not want to use the Internet for commerce, for government services, for interaction with other people. We'll lose the great potential of the Internet."

Find this article at:
http://www.cnn.com/2004/TECH/internet/11/01/tangled.in.spyware.one.ap/index.html

□ Check the box to include the list of links referenced in the article.