

How to fight back against insidious attacks from cookies gone bad.

# Spyware



■ BY DEBORAH RADCLIFF

## What is spyware? And what harm can it do to my network?

Even in its most innocuous form, spyware is an invasion of privacy.

Spyware programs such as Cydoor, Gator, Lop.com and Xupiter install without the user's knowledge by piggybacking on peer-to-peer file-sharing programs, cute executable images or a long list of freeware.

Primarily used for target advertising purposes, spyware tracks a user's Web habits. Some programs log keystrokes and even capture and transmit screen images.

"These programs are hard to avoid because they come bundled with other things, and it's not always apparent when they're installing themselves. And once they're on computers, they can be difficult, time-consuming and costly to remove," says Michael Steffen, policy analyst with the Center for Democracy and Technology (CDT) in Washington, D.C.

At its worst, spyware becomes a dangerous tool in the hands of the wrong people.

"Today, spyware's annoying but relatively benign. But Gartner believes spyware will get more malicious in the future and be used for password harvesting, credit card number theft and other forms of identity theft," says John Pescatore, a Gartner analyst.

Mark Maiffret, chief hacking officer for eEye Digital Security, sees even more sinister uses for spyware, such as capturing and transmitting Microsoft Word and Excel documents to steal corporate secrets.

This is not to mention the unprotected tunnels being opened to the desktops by unknown programs that aren't coded with security in mind, adds Jeff Horne, researcher for Internet Security Systems, which makes RealSecure intrusion-detection software.

### How to avoid spyware

Enforcing employee Internet use policy is your first line of defense, Maiffret says. His advice is:

- Configure desktop browsers and Outlook using Microsoft Domain Security Policies.
- Block ActiveX and other executables.
- Manage scripting.
- Filter Web content through an HTTP proxy.
- If necessary, segment certain employees from using the Internet if they don't need it to do their jobs.

Employees also should be taught how to surf the Web safely, says Ian Poynter, chief security officer for Bit9, a security software start-up. Keep user education simple, he says, by sticking to the following points:

- Don't download peer-to-peer programs or anything you're not sure of.
  - Don't click on fun images like dancing bears.
  - Don't download freeware without first checking with IT.
- The bottom line, is if you don't need it to do your job, don't click on it.

### How to detect spyware

Even if you implement all those policies, spyware is likely to get through. Until recently, the only way to detect

## How spyware gets onto your network

Jeff Horne, researcher for Internet Security Systems, lists the five sneakiest ways spyware gets distributed.

- Masquerading as a legitimate plug-in to run a movie or music file.
- Masquerading as a browser helper object such as a Google toolbar (used primarily in home page redirects).
- Hiding out in group directories on peer-to-peer networks such as music-sharing, and then spreading itself by infecting the directories of machines searching those directories for their music selections.
- Tricking people into installing their programs. Instead of saying, "To install this program, click yes," the prompt says, "To install this program, please click no."
- Hijacking Outlook e-mail as if it were a browser (primarily for pop-up ads).



## How to filter Port 80 traffic

Because spyware installs and operates over Port 80, it passes onto computers without notice from the current generation of firewalls, says John Pescatore, vice president of security research for Gartner.

Anti-virus/firewall packages that do sweep http traffic over Port 80 for spyware patterns include Fortinet Fortgate, McAfee Internet Security Suite, Norton Internet Security 2004 and Trend Micro's InterScan Web Security Suite for Windows.

Neither Trend Micro nor Symantec offer spyware detection on an enterprise level. Norton's consumer product contains 313 spyware definitions, and Symantec plans to release the same capability in its enterprise software by end of the first quarter.

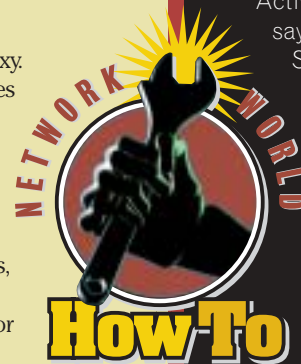
Intrusion detection isn't the correct way to scan for spyware because it relies on attack signatures instead of traffic pattern analysis, users and analysts say.

"It's hard to catch spyware by looking for exploit signatures because it installs on desktops through ActiveX plug-ins and browser helper objects," says Jeff Horne, researcher for Internet Security Systems, which makes RealSecure intrusion-detection software.

"Spyware changes on a day-to-day basis. You'd need a team of researchers writing signatures every day and still you wouldn't be able to keep up the signature files," he says. Instead, he says, you need pattern recognition to capture new forms of spyware. Take, for example, a spyware program called Trickler.

Trickler downloads tiny bits of spyware over hours or a day and gathers itself into a client. "You see this executable going out and trying to grab another executable and so on. Heuristic [pattern recognition] would recognize and put a stop to that," he says.

— Deborah Radcliff



spyware was to wait for a user to call the help desk, says Shane Allen, network engineer for Special Devices, a Moorpark, Calif., maker of pyrotechnic airbag initiators.

"Users would call and say 'I can't open this file. It doesn't print. I can't go to the Web.' So we had to go to the user and re-create what they were doing," Allen says. "You'd start to see all these different errors because something's processing in the background."

Allen moved to a more proactive process in March, when his Web-filtering vendor, Websense, added spyware to a menu of behavioral blocking options in its new product called the Client Application Module (CAM). CAM sells for \$25 per seat for a 1,000-user installation and plugs into Websense's central manager, called Websense Enterprise.

With its daily downloads, Websense Enterprise catches most spyware before it gets on his network's computers, Allen says.

If spyware does get through, CAM prevents it from executing through a kernel-level filter driver that looks for categorized spyware behaviors in the outbound executables.

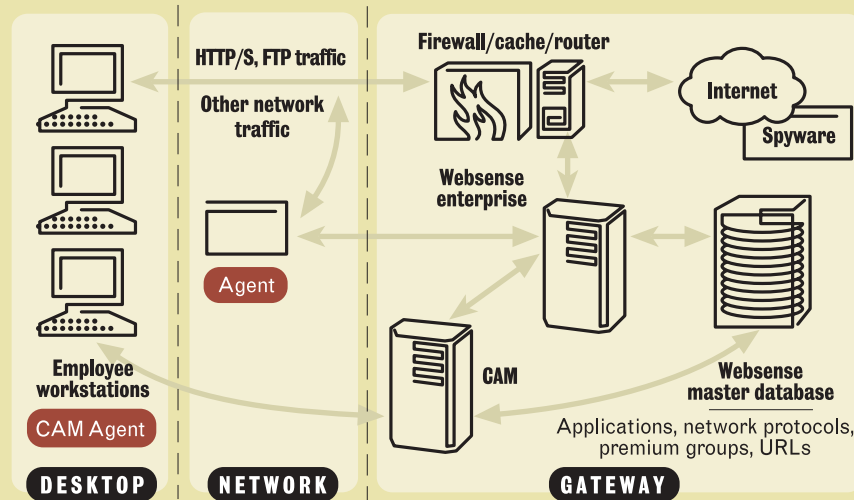
In this way, Websense locates spyware that has snuck past front-line defenses. Nigel Smithson, data security officer for Boston Private Bank, uses Websense reports to determine what computers need disinfecting.

"Spyware is the bane of my existence," Smithson says. He used to deal with spyware reactively. But now he's lowered his incidents of spyware on all but home-use computers through a combination of commercial tools and freeware for a total investment of about \$2,000.

"My way isn't the be-all, end-all," he says. "Anti-virus goes some way towards stopping spyware. And we use a desktop tool to clean it up when we suspect there's spyware on a machine. But certainly, Web filtering prevents most of it."

## Spyware vs. anti-spyware

**Websense's Client Application Module blocks spyware from infecting your network. Websense Internet filter software can block the peer-to-peer connections and the downloading of executables and applets associated with spyware. Agents on the client and the network alert the Websense management tools to a possible spyware download, and the software tells the firewall to block the spyware traffic.**



### How to remove spyware

For spyware that makes it past the Web filter, removal is difficult without an automated spyware removal tool. According to the CDT report on spyware, most spyware is designed to resist un-installation.

"Spyware leaves behind stuff you can't get rid of that's buried in places all over the registry. To clean it means tearing down the registry and knowing what files to look into," says Michael Wood, U.S. representative for Lavasoft, which makes freeware and professional spyware removal software called Ad-Aware. The professional version sells for

\$39.95 per desktop. Allen uses Lavasoft's freeware version for those times he needs to eradicate spyware from an infected machine. Smithson also uses a freeware product called Spybot.

Smithson says he tried Ad-Aware, but Spy Bot caught more spyware without a lot of the custom configuration that he had to do with Ad-Aware.

"Because of Websense, we don't need to put spyware mitigation software companywide. We only use it occasionally when someone has a problem," Smithson says. "But we do recommend that our home users install it on their machines and run it in the background."

Other products on the market include InterMute's SpySubtract, Iolo Technologies' LLC Mechanic, Sygate's SSE firewalls and Tenebril's GhostSurf Pro.

### How to protect teleworkers

Ah yes, the home-user bugaboo. Current management tools, such as those from Websense, don't enforce Web use policy on home-use machines. So only home-use spyware mitigation tools such as Spy Bot and Ad-Aware can protect those machines from spyware.

"Our users take their computers home and browse the Web through an uncontrolled connection. So sometimes they have problems," Allen says. "We had a high-ranking employee call and complain the other day about his browser getting hijacked. He was visiting some Web sites in Thailand, where one of our major suppliers is located. And he got infected."

*Radcliff is a freelance writer in California. She can be reached at deb@radcliff.com.*

# Help! I've been Web-jacked!

Spyware can be a problem for even the most savvy Internet users.

On Dec. 22, an Internet investigator got a tip that child pornography was being housed on an adult Web site. When he visited the site to verify the information, he didn't find any illegal images. But what he did find was a Trojan horse that disabled the ActiveX security controls on his browser and took control of it.

"I heard my hard drive churning and clicked on my task manager and saw three executable programs were installing themselves," says Chris Brandon of Brandon Internet Services. "I knew I was in trouble when I couldn't get my task manager to cancel the programs."

By the time he checked his registry, the Trojan had installed dozens of programs that replaced the default Web page with its own, and loaded its own IP addresses in his favorite places, short cuts and safe zones. When he tried to erase the programs and reboot the machine, the virus reinstalled.

This program is a perfect example of spyware gone amok.

It installed itself by taking advantage of a vulnerability in Internet Explorer 4.x and 5.x that lets an unsigned applet to create and use ActiveX controls. Then it hijacked Brandon's browser, a term called "Web-jacking." But it could have

been worse. Some variants evoke dialers to call up 1-900 numbers if the victim is using telephone dialup for Internet access.

"We're seeing more of this type of virus activity in recent months," says Ken Dunham, director of malicious code for iDefense, a security intelligence firm in Reston, Va. "Trojans promote going to certain pornography sites and other sites they affiliate with because they get money for the clicks from advertisers. They terminate regedit.exe [registry editor], and they can be very difficult to remove."

Anti-spyware vendor PestPatrol reports staggering growth over the past few months of the virus that Symantec dubbed Trojan.Norio. And at least 24 variants of the virus now exist in the wild, according to the anti-spyware site Spywareinfo.com.

Each variant is designed to do something different. One variant changes your customized search settings to allhyperlinks.com, for example. Another variant redirects all searches

through a bogus site called Coolwebsearch.com. Another redirects Verisign's Site Finder to a fraudulent Site Finder site. Another evokes the auto-dialer. And so on.

Expect these types of Trojan viruses to be used for

even more malicious purposes, such as the culling of credit cards and passwords, Dunham says.

"In the case of the Norio Trojan, it changes the registry and the host file," he says. "You type in a name like Microsoft.com, it will redirect you to a site they want you to go to. You could make it redirect you to a fake Citibank.com Web site and get you to fill in sensitive information."

Brandon removed the malicious code by using Spywareinfo's remediation kit called CWSweep. (PestPatrol also provides a removal kit.) He's since been tracking down the IP addresses and domain names that the virus loaded into his registry. Many of the domain names are a variation of Coolwebsearch.com.

"I want to find the people responsible for this, the affiliates in collusion with this, and turn them into Microsoft for that bounty it promises on virus writers," he says.

With the IP addresses and Web site names so easy to find, you'd think tracking the virus writers would be easy for someone with Internet tracking skills. But most of the IP addresses Brandon's investigated led to bogus hosting providers and anonymized administrative contacts. Meanwhile, the PestPatrol report on the virus lists an address for Coolwebsearch.com, the originator of the virus, to be in Natick, Mass.

— Deborah Radcliff

