# Spyware Essentials

TechRepublic®
Real World. Real Time. Real IT.

# Spyware Essentials

TechRepublic®
Real World. Real Time. Real IT.

**Spyware Essentials**

**Published by TechRepublic**
ISBN 1-932509-90-9
Printed November 2005

## Disclaimer

The information contained herein has been obtained from sources believed to be reliable. CNET Networks, Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CNET Networks, Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

TechRepublic
1630 Lyndon Farm Court
Louisville, KY 40223
Tel.: 1.800.217.4339
Online Customer Support:
http://techrepublic.custhelp.com/

November 2005
B082

**Credits**

**Director, TechRepublic Press**
Carmen Barrett

**Executive Editor, Premium Products**
Erik Eckel

**Senior Editor**
John Sheesley

**Operations Manager**
Marilyn Bryan

**Graphic Artist**
Kimberly Wright

**Copy Editor**
Julie Tonini

**Promotions Manager**
Megan Hancock

**Customer Support Manager**
Elisa Suiter

# Foreword

Spyware is among the most prevalent risks facing computer users. Although viruses occasionally wreak more havoc, spyware has quickly become a bigger headache and can cause even greater damage.

Regardless of how well you police your network's systems, spyware program—and their resident adware, stalking horse, Trojan horse, backdoor Santa, malware, and other malicious components—are finding their way in. Once inside your organization, these heinous programs collect sensitive username and password information, harvest keystroke data, redirect search software, and slow system performance. Worse, a recent *Webroot Software State of Spyware* report found that enterprise desktops exceeded 80-percent infection rates; each enterprise system averaged 27 instances of infection.

There's more to combating spyware than just loading a free antispyware application and walking away. Much more. TechRepublic's *Spyware Essentials* collects proven guidance and best practices for diagnosing, troubleshooting, and blocking spyware infestations. You'll find expert information and advice to help you:

- Understand how spyware works.
- Recognize spyware infections.
- Learn how antispyware programs operate.
- Administer and configure leading antispyware products.
- Troubleshoot spyware problems.
- Compare leading antispyware programs.
- Prevent users from becoming phishing and pharming victims.
- Educate users to avoid spyware traps.

Learn to identify, remove, and prevent spyware. Trust TechRepublic to help. Developed by IT professionals for IT professionals, *Spyware Essentials* delivers the tips and solutions you need to overcome spyware challenges, whether you're administering a small office or global enterprise network.

TechRepublic®
Real World. Real Time. Real IT.

# Spyware Essentials

## Recognizing Spyware

## Battling Spyware

## Anti-Spyware Tools

## Category Report: Anti-Spyware

## Phishing and Pharming

## User Education

# 1

# Recognizing Spyware

# Spyware:
# The ultimate uninvited guest

*By Steven Pittsley, CNE*

Spyware. This sinister-sounding word conjures up an assortment of images, from tiny CIA espionage cameras to those annoying pop-up ads that infest computer systems. Techies adopted the term *spyware* as their own in 1999, using it to describe software that is installed on a computer to record information about the computer user. In the last four years, spyware, like viruses, has grown into a plague that affects almost everyone who uses a computer. Regardless of how well you police against them, spyware installations still manage to find their way onto computer systems. Let's look at the purpose of spyware, some examples of how these applications are propagated, and ways in which these programs work.

## Defining spyware

Spyware describes software that is installed on a computer and covertly gathers information through the user's Internet connection without his or her knowledge. Often benign in nature, spyware is most commonly used to collect information for advertising purposes. As with viruses, many types of spyware exist. These categories tend to overlap, and the terms that describe them are often used interchangeably. The following list defines several types of spyware and illustrates the differences between them.

- **Adware—**Adware network applications are the most common type of spyware programs. An advertising company pays the makers of popular games, utilities, and other software programs a small fee to bundle its adware software with legitimate applications. The software vendor is paid whenever the adware application is downloaded with the legitimate program. Adware is designed to display advertising banners through pop-up windows or toolbars. Some adware applications also include code to track a person's Internet usage and personal information, often passing this data to third parties without the user's authorization or knowledge. The Claria Corporation (formerly the Gator Corporation) is one of the largest adware organizations; others include DoubleClick, WhenU.com, Radiate, and Web3000 Ad Network.
- **Stalking horses—**This type of program enables adware networks to function on a user's desktop to obtain the user's demographic and personal information. Like adware, these applications are often bundled and installed with legitimate programs. Usually, stalking horses are described as a desirable add-on during the installation routine. These spyware applications are not always used to display pop-up ads, differentiating them from adware programs. The most common stalking horse programs are eZula's TopText, Cydoor, OnFlow, and webHancer.

- **Trojan horses—**These applications are bundled with popular Internet applications used for file sharing, such as KaZaa, Grokster, and Morpheus. They are similar to stalking horses, but their installation is not disclosed during the program setup.
- **Backdoor Santas—**These programs have no obvious purpose other than to collect information about surfing or shopping habits. Unlike other spyware applications, Backdoor Santas do not work in conjunction with an adware network. A few examples of this type of application are Hotbar, CuteFTP, and the ever-popular BonziBUDDY.
- **Cookies—**These spyware tools are not applications but rather small files that are stored on the user's computer. They are used to build a user profile without notifying the user of the information being stored and are eventually forwarded to an organization. Although cookies are used for many purposes by most Web sites, they are also considered a form of spyware.
- **Malware—**Malware is malicious software designed to disrupt a computer, often rendering the system unusable unless the application is removed. Many malware applications reinstall themselves when you try to remove them, making it extremely difficult to completely uninstall them. Malware includes not only spyware applications, but also viruses, worms, Trojans, and similar nefarious-minded code.

These definitions illustrate the variety of spyware applications in existence today. Generally speaking, the majority of these programs are used for advertising purposes, with malware being the glaring exception. All of them collect demographic and usage information, frequently without the user's knowledge. Although all the software companies that publish spyware applications claim that the programs are benign, most people object to their personal information being collected and sent to an organization without their consent, regardless of the purpose.

Most spyware, with the exception of malware, has a legitimate purpose: to gather marketing data with the intent of providing you with advertisements that appeal to your interests. The advertisers hope to provide you with tantalizing offers that are tailored to your tastes instead of having you see a random assortment of ads. Although somewhat annoying in this form, the concept of demographic marketing has been used by advertisers for decades in the print and broadcast media. But in this case, rather than display regional ads intended for various markets, advertisers display ads based on the user's Web-surfing history.

## The inner workings of spyware

The most common indication that a spyware application is installed on a computer is an increase in the number of pop-up ads that display when a user is surfing the Internet. Many Web sites display pop-up ads as part of their own normal activities, but users should not see pop-ups display every time they view a Web page. In addition, many spyware applications display multiple pop-up ads, sometimes opening three, four, or even five new windows at a time. This is not only annoying, but it also consumes bandwidth and time, which are in short supply for people still using a dial-up connection.

Spyware organizations use a number of methods to get their software installed. Although some spyware, such as malware, is secretly installed, most spyware applications are legally installed when the user installs legitimate freeware, shareware, instant messaging, or file-sharing software. For example, Google's useful toolbar has an option to collect demographic user data. Sometimes the user is presented with an option to deselect the secondary program, as with the Google toolbar. A more commonly used method is disclosing the spyware application in the licensing agreement. Since few people read the end-user licensing agreement (EULA) when they install software, they unwittingly authorize the installation of the spyware application.

Another common method of spyware distribution is through e-mail. In this case, the spyware application is disguised as an e-mail attachment or a Web page link. Again, the user may have a legitimate reason for opening the attachment or link. However, when the user does this, the spyware installation launches. Some popular methods of disguising spyware installers are e-mailed greeting cards or links that claim to install anti-spyware programs.

Spyware applications gather their data using a variety of methods. Many programs track a user's Web-surfing habits by collecting the history of pages he or she views. This information is then transmitted to the adware network, which uses it to customize the advertisements the user views in the pop-up windows that the spyware application opens. Other programs collect demographic information using HTTP cookies. When the Web site opens the cookie, the user's information is transmitted back to the organization, which once again uses it to customize the ads that the user views. Some of the more invasive spyware applications are programmed to redirect the user's Web browser home page. In addition, some programs even go as far as redirecting the browser from a requested page to a different organization's home page, preventing the user from viewing the competitor's page. These types of applications can also slow down computer systems, overload them with pop-up windows, and even cause them to cease working altogether.

Malware applications can do much more damage than merely transferring history data. For instance, some applications are designed to capture the user's keystrokes. This can result in the capture of confidential information such as passwords, credit card numbers, Social Security numbers, and other types of personal data. Spyware can also be used to scan files on users' hard drives or access their applications. Some malware is designed to read, write, and delete specific files on the user's hard drive—or even reformat it.

## The growth of spyware

As most people can attest, spyware use is growing rapidly. An EarthLink survey discovered 83 million instances of spyware installed on three million computers over a nine-month period (**http://news.com.com/EarthLink+finds+spyware+running+amok/2100-1032_3-5397333.html?tag=nl**). Many industry experts suggest that spyware applications are installed on as many as 90 percent of computers that are connected to the Internet. The lucrative nature of the business encourages organizations to have their applications installed on as many computers as possible. For instance Claria, one of the largest adware firms, had revenues of $90.5 million in 2003 and recently announced plans for an initial public offering. With advertising revenue constantly growing, it's no surprise that spyware organizations are so numerous.

In an effort to control the amount of spyware being deployed, the U.S. House of Representatives recently approved legislation prohibiting an organization from taking control of a computer, modifying a Web browser's home page, or disabling antivirus software without the user's authorization. The Spy Act (**http://news.com.com/House+approves+spyware+legislation/2100-1028_3-5397822.html?tag=st.ref.goo**), as it is called, creates a complicated set of rules to govern software that transmits user information across the Internet. This legislation enables the Federal Trade Commission to monitor violators and levy fines of up to $3 million. Although this legislation is not yet a law, representatives on both sides of the aisle and in both houses support the bill. The 399-to-1 vote illustrates the broad support for the Spy Act, which should easily pass through the Senate and be signed into law in the near future.

## Wrap-up

In the last few years, spyware applications have become as prevalent as viruses, if not more so. Although viruses are designed to damage computer systems, spyware is meant to provide consumer advertising. However, the aggressive nature of some spyware organizations and the multiple installations of various spyware applications on a computer system can have the same devastating effect on a computer system as a virus. Spyware is, for the most part, legal. Even so, efforts are being made by the U.S. government to curtail the pervasive ways that spyware companies distribute, install, and use their applications and the collected demographic information. ❖

# Group delivers definition of spyware

*By Joris Evers, CNET News*

The nascent Anti-Spyware Coalition, made up of makers of anti-spyware software, will release a proposed definition of spyware and a common lexicon, said Ari Schwartz, an associate director at the Center for Democracy and Technology, which has led the work of the group. Various consumer and industry organizations helped in the effort, he said.

"Any unified approach to the spyware problem is going to require a common definition of what the problem is," Schwartz said. "One of the biggest challenges we have had with spyware has been agreeing on what it is."

The creation of the Anti-Spyware Coalition was first reported by CNET News.com in June 2005.

Spyware and adware have become a major headache for computer users over the past years. Still, purveyors of the software defend the programs as legitimate marketing tools and take issue with anti-spyware makers when their product is flagged and removed. The coalition's goal is to draw clear lines, ultimately to help consumers keep their PCs clean.

The coalition defines spyware narrowly as software that gathers information about the user and is installed without adequate user notice, consent, or control. The definition would mark as spyware any programs that are downloaded and installed surreptitiously or that track what Web sites people visit, for example.

An expanded definition also includes other potentially malicious programs, such as software that provides backdoors for hackers or serves up ads on the user's screen.

In that definition, spyware and other potentially unwanted technologies are described as those that "impair users' control over: material changes that affect their user experience, privacy, or system security; use of their system resources, including what programs are installed on their computers; or collection, use, and distribution of their personal or otherwise sensitive information."

The group has also drafted procedures for dealing with software makers who believe their product has been unfairly flagged as spyware.

## Could it backfire?

Critics fear that spyware makers stand to gain most from the coalition's work. It may give them the tools to prevent their software from being flagged and removed by anti-spyware products, said Ben Edelman, a Harvard law student and an adware and spyware researcher.

"The entities most urgently calling for uniform standards are those who make applications often labeled as spyware or adware," he said. "They hope to get a single definition that they can then manage to escape."

Internet users know what software they don't like, and anti-spyware makers should build their products based on that, Edelman said. "There's substantial benefit to letting anti-spyware vendors compete to best match users' desires and preferences," he said.

Both spyware and adware can sap computing power. They're often surreptitiously installed on computers to gather information about people that is used for advertising or provided to other interested parties. The market for tools to remove the unwanted software is booming.

There have been cases where a definition of spyware and dispute policies could have helped anti-spyware software makers set up a stable blacklist. Computer Associates International earlier this year temporarily removed the Gator adware program from the spyware detected by its PestPatrol program after the maker of the software complained. The program has since been put back on CA's list of spyware.

In another example, Microsoft is facing heat over its recent decision to downgrade the threat level for the same adware, now known as Claria. The beta version of Microsoft AntiSpyware previously recommended that users quarantine several products from Claria. The Microsoft product still detects the Claria software, but no longer recommends removal.

The public can comment on the Anti-Spyware Coalition's draft definition until Aug. 12, after which the group plans to incorporate the best recommendations in the final version. Members have said they will incorporate the work in their products, Schwartz said.

The efforts by the Anti-Spyware Coalition come months after the collapse of the Consortium of Anti-Spyware Technology vendors, or Coast, which had many of the same goals. Coast fell apart after it admitted a company suspected of making adware, prompting the departure of several key anti-spyware members.

Anti-Spyware Coalition members who make spyware-fighting software include: Aluria, America Online, Computer Associates, EarthLink, Lavasoft, McAfee, Microsoft, PC Tools, Symantec, Tenebril, Trend Micro, and Webroot Software. The coalition is supported by the Canadian Internet Policy and Public Interest Clinic, Consumer's Union, and other organizations. ❖

# Information resources for fighting spyware

*By Steven Pittsley, CNE*

Information about spyware is becoming almost as prevalent as the scourge itself. But not all of the information is reliable, and finding accurate, useful details about the many varieties of spyware is difficult even for technology professionals. To help you zero in on the best information available, we've compiled this list of Web sites. All of these sites contain up-to-date spyware information. The majority of them are geared toward both IT professionals and users. If you have a question about spyware, at least one of these sites is almost guaranteed to have the answer.

## Computer Associates

Computer Associates is one of the largest companies in the industry. Its PestPatrol anti-spyware product is very good, and its Spyware Information Center provides a wealth of excellent spyware information.

Directed at technology professionals, the Spyware Information Center offers the latest spyware news and a large collection of spyware-related articles. The site also contains a list of recent spyware discoveries and a comprehensive and easy-to-use spyware encyclopedia that describes known spyware programs. Even novice computer users will benefit from the many offerings found on this site.

## Counterexploitation

Counterexploitation, or CEXX.org, is a Web site dedicated to preventing the exploitation of computer users. Part of its service is an Adware/Spyware page that contains a wide variety of links to explanations of the various forms of spyware.

This site is extremely useful for advanced users, but novices might find it a bit intimidating. If you're having trouble ridding your system of a particular spyware program, CEXX.org is one of the first places you should consider looking for help. The vast resources provided by this Web site are impressive, but you'll have to dig for the information you need.

## Download.com Spyware Center

Download.com is known for providing download links to nearly every type of software imaginable. However, this site also boasts a good spyware information center. Not only can you download reputable anti-spyware applications, but you can also read reviews of those products and learn how to use them.

The Download.com Spyware Center offers links to a host of spyware-related articles that are applicable for every level of user (**http://www.download.com/Spyware-Center/2001-2023_4-0.html?tag=dir**). Although you may have to click through a number of links to get the information you're looking for, if you're patient, you can find well-written articles on almost any topic you're interested in.

## Sunbelt Spyware Research Center

Sunbelt Software produces one of the most comprehensive spyware resources on the Web: the Sunbelt Spyware Research Center (**http://research.sunbelt-software.com/index.cfm**). Much of the material is geared toward promoting its CounterSpy product, but there's a good bit of other information that's up to date and highly useful.

The Sunbelt Spyware Research Center contains a wealth of spyware-related information on topics such as spyware prevention, organized cybercrime, spyware education, corporate spyware infections, and spyware removal costs. The site is organized well and easy to navigate. Users of any level will benefit from the information provided by Sunbelt Software.

## PC Pitstop

PC Pitstop provides many useful spyware articles for average computer users. IT pros may scoff at some of the titles, such as "Kids and Spyware," but the average computer user will appreciate the straightforward, informative articles.

PC Pitstop also has a spyware forum and free e-mail-based technical help. Although the ultimate goal of the site is to generate members—and revenue—for PC Pitstop, the amount of free, basic information makes this an attractive site for end users.

## SpyChecker

The SpyChecker Web site offers links for downloading a wide assortment of anti-spyware applications and utilities. The site doesn't contain much educational material, but the utilities and other links make this a useful site to visit when you're looking for software to rid your system of forms of spyware that other anti-spyware programs can't remove.

This is definitely a site for advanced users who understand spyware and Microsoft operating systems very well. Many of the tools offered at SpyChecker are written for specific spyware applications or involve highly technical operations such as cleaning the system registry of spyware-related keys.

## Spyware Guide

Another Web site dedicated completely to spyware is Spyware Guide. This helpful site offers a great deal of spyware education, as well as many useful links and resources.

Spyware Guide enables you to look up any known form of spyware and receive an explanation of what it does and directions on how to remove it from your system. The list can be sorted alphabetically by program name, or you can search by spyware category or by company name. If you already know the name of the pesky program, you can simply type it in to retrieve the information. If you want an accurate description of the spyware that's infesting your system, spywareguide.com is definitely the place to go.

## SpywareInfo

The SpywareInfo Web site contains quite a bit of technical information related to spyware. Aimed at advanced users, SpywareInfo also publishes a weekly spyware newsletter. You can read the *Spyware Weekly* online or get the latest spyware news delivered via e-mail.

SpywareInfo also hosts a user forum and a chat room. These resources are handy when you're having a spyware problem. The SpywareInfo members are knowledgeable and provide excellent troubleshooting advice.

## Spyware Warrior

The Spyware Warrior Web site offers tons of information about anti-spyware programs, including a list of rogue anti-spyware sites (**http://www.spywarewarrior.com/rogue_anti-spyware.htm**). Just because a tool or Web site claims to remove spyware doesn't mean that it actually does what it says. The Spyware Warrior site lets you ensure that a particular anti-spyware tool will do the job it says it will do.

## Webroot Spyware Information Center

Webroot Software Inc. produces Spy Sweeper anti-spyware software. As part of its strategy to combat spyware, Webroot has developed the Spyware Information Center. The material contained in the center educates users about basic spyware topics, such as defining, removing, and protecting against spyware.

The Webroot Spyware Information Center is geared toward novice users. Technology professionals will probably find the information at this site very rudimentary. But for those average computer users who want a solid understanding of spyware basics, this site provides a good foundation to build upon.

## Wrap-up

The Web sites listed here are excellent resources for all computer users to become familiar with. Although many are directed toward technology professionals or advanced users, novices will find enough information at some of these sites to help them learn how to recognize and eliminate spyware.

Each of these sites offers something unique. Once you become familiar with their offerings, you'll have a good idea of where to turn when you need to remove a rogue spyware application from your computer or network. ❖

# 2

# Battling Spyware

# The end of spyware? Fat chance

*By Charles Cooper, CNET News*

Call it the unexpected outgrowth of entrepreneurial capitalism. Or if you're wont to take a more cynical view of our affairs, chalk it up to the seamier side of human nature.

In the late 1990s, advertisers wanted more accurate ways to track click-through rates on their Internet advertisements. Cookies weren't doing the trick, and a cottage industry subsequently grew up that helped companies better monitor Web surfing patterns. Among other things, these companies discovered ways to download code onto computers, code that then popped up relevant advertisements when people opened Web pages.

Fair enough as far as that sort of thing goes. Unfortunately, greed quickly overcame common sense and an epidemic was unleashed that my CNET colleague Esther Dyson characterizes as "the scourge of the year."

She's got that right. At stake is a multibillion-dollar advertising industry that doesn't quite know what to do with the third-party shysters it inadvertently helped spawn.

Though the two often get lumped together, a fuzzy line separates adware from spyware. In the case of adware, an ad-generating program gets bundled with a free application, and people who want the app agree to download the whole package (at least theoretically; they're not always aware of the adware component). With spyware, code gets surreptitiously dumped onto people's computers, and there's not even the pretense of soliciting informed consent.

"If you want to be a publisher long term, you can't allow this to continue," says Ralph Terkowitz, a partner with ABS Capital Partners and the founder of *The Washington Post*'s electronic publishing subsidiary.

So what is to be done?

The last thing the technology industry may want is an imposed solution. But when phony pop-ups disguise themselves as legitimate Web pages, few politicians will be able to resist going after so inviting a piñata. New York Attorney General Elliot Spitzer was first to file a lawsuit charging a company with being a source of adware and spyware programs that hinder online commerce and security. Unless adware companies find a way to better police themselves, other politicians inevitably will follow Spitzer's lead.

The adware guys can read the writing on the wall as easily as anyone, and they understand that their not-exactly-vigorous efforts to gain a potential downloader's consent contributed to the current mess. At a workshop sponsored by CNET's Download.com site, executives from four big adware companies—WhenU, Claria, DirectRevenue and 180solutions—acknowledged their critics and even extended an olive branch.

But they have a credibility problem that is going to be hard to shake. So it was that a guy sitting in front of me was in an unforgiving mood. Listening to their explanations of how the adware industry might clean things up, he shook his head and muttered, “slimeballs, slimeballs.”

I don’t know how fairly he represented the opinion of people in the audience, but this clearly was a “show me” crowd. To their credit, the companies agreed to participate, knowing full well that they faced an unsympathetic gathering. At least there were no fistfights to report.

Maybe it was the start of a fruitful dialogue. But there’s an awfully long way to go, and the public increasingly will demand action, not just words. Meanwhile the clock is ticking, and the Spitzers of the world smell blood. ❖

# Spyware threat escalating, expert warns

*By Will Sturgeon, CNET News*

Spyware is becoming increasingly pernicious and sophisticated, according to security experts who are warning that users are still failing to take basic steps to protect themselves against the threat. It's a problem that should scare big businesses as they face up to the fact that important data could be leaking out of their organizations daily. And yet too many organizations are failing to properly educate or protect their employees, one expert says.

"You'd be surprised at the amount of data these things collect," said Eric Chien, a senior researcher at Symantec.

Chien said techniques such as screen capture, key logging, behavioral analysis, and common word recognition are all methods employed by spyware applications to build a profile of a user. Presenting at the Virus Bulletin conference in Dublin, Ireland, Chien also detailed the ways in which spyware can get onto a machine.

"At their most basic, they will be able to find your name, your gender, your age, the amount of time you spend online, what you search for, what you buy, and what Web sites you visit," he said.

Chien proved this point by showing the detailed data relayed by one piece of common spyware.

Such applications won't discriminate between personal and corporate data, though the latter tends to be of far higher value.

Chien also showed conference delegates a more advanced spyware application that is programmed to kick in when any one of hundreds of Web sites are visited and certain words encountered on the page.

Such an application, for example, was able to take and relay screenshots whenever the user was on particular retailers' Web sites where the word "confirm" appeared.

"If you're hitting 'confirm,' then what information is going to be visible on that Web page? Credit card number, name, expiry date, billing address, shipping address." Chien said.

## Tracking the users

And it gets far more worrying for users. The application is also programmed to start sending screenshots whenever users are on any page of certain banks' Web sites.

Chien said users shouldn't put too much faith in perceptions of security as presented in 'https' style URLs.

"Some of these applications can read all https traffic," said Chien, though the danger exists only when accessing such sites from an infected machine.

In fact, the only way users can be protected against such threats is to ensure spyware doesn't exist on their computers.

That requires a balance of technical and educational approaches.

Companies should all have anti-spyware protection in place on all machines, but users must also realize the threat posed by activities such as installing non-essential software and clicking on pop-ups from unknown or untrustworthy sources.

According to research out today from another security vendor, Trend Micro, around a quarter of employees in the U.S. in both the small business and enterprise sector have fallen victim to spyware while at work.

In total, 87 percent of respondents said they are aware of a threat posed by spyware, while 57 percent said they want more education on the threat and 40 percent believe their IT department could be doing more to protect them. ❖

# Spying on the spyware makers

*By Declan McCullagh, CNET News*

Ben Edelman may be spyware's most dangerous enemy. The 25-year-old researcher has spent years analyzing how spyware and adware programs work and disclosing his findings publicly. That often results in red faces and, occasionally, lawsuit threats from companies like WhenU and Claria, formerly known as Gator.

When testing spyware and adware, Edelman isn't about to sacrifice his own Windows XP computer. So he uses the VMware utility to create a virtual Windows box.

"I infect the hell out of it," he says. "It destroys the infected machine."

A law student at Harvard University, Edelman also is completing a doctoral degree in economics. CNET News.com caught up with him after he spoke at a conference in San Francisco sponsored by News.com's sister site, Download.com.

**Q:** What got you interested in spyware in the first place?

**Edelman:** I took a call from the plaintiffs in the *Washington Post* case against Gator. They thought what Gator was doing was absolutely destructive to the availability of free content on the Web. After all, if advertisers could buy ads from Gator to reach the *Washington Post*'s audience, who would buy ads from the *Washington Post*?

I happened to think they were right. But the case settled out of court on the eve of trial so we didn't find out for sure whether Gator's business was legit.

**Q:** How much time have you spent since then on spyware-related topics?

**Edelman:** It's scary. It's what gets me out of bed in the morning right now, more so than classes, more so than my dissertation research. I probably spend 30 hours a week. It's been nonstop for the past 15 months. Before that, it was quite a bit less intense.

**Q:** What was the most interesting thing you've discovered?

**Edelman:** There's just a huge amount of money changing hands here. The biggest, richest American companies are buying advertising through spyware. The biggest, richest venture capital firms are investing in those who make this kind of unwanted software. That's names like American Express, Sprint PCS, Disney, Expedia, Guy Kawasaki's firm.

**Q:** You're using the word *spyware*. But you also mean the advertising-based networks with pop-up ads, right?

**Edelman:** Absolutely right. My claim is that each of the so-called adware networks has obtained installations and is still obtaining installations in ways that offer such poor notice and obtain such limited consent—sometimes none at all—that users can't fairly be said to have consented. If they didn't consent, and their activities are being monitored or transmitted, then that's spying.

**Q:** Have you ever been threatened by spyware makers or adware makers?

**Edelman:** Yes. Some vendors have challenged the permissibility of my method; for example, Gator was awfully angry when I posted a Web service that let any Web site operator see how Gator was targeting their site with competitors' pop-ups. They sent a series of legal papers, complaints, threats to me and my then-bosses at Harvard's Berkman Center.

**Q:** I seem to remember that you had written some controversial software that tested what one adware program was doing—I think it was WhenU.

**Edelman:** I can't comment about that.

**Q:** Ask Jeeves seems to be an above-the-board company. What's your complaint with them?

**Edelman:** The core problem is Ask Jeeves' installation practices. Sometimes their software gets installed without any notice or consent at all through security hole exploits. When they do ask for permission, they don't always tell users everything they need to know to make an informed choice. For example, when installing a Web browser toolbar, they use euphemisms like "directly accessible from your Web browser" instead of the obvious and natural word "toolbar."

**Q:** You don't have any objection to pop-up applications like WhenU or Claria as long as the user knows what they're getting?

**Edelman:** I have no comment on any matter pertaining to WhenU. As to Claria, their core business seems to me to be troubling because it's so parasitic. They can only show ads thanks to users requesting other sites which get no share of the revenues from those ads.

**Q:** What's the latest in terms of threats to anti-adware companies who label certain software "spyware"?

**Edelman:** The background here is that historically users have been tricked into getting all manner of unwanted software into their computers. Their computers become slow, unreliable. Companies step in to help by offering detection programs.

From the perspective of the spyware makers these detection programs are bandits: they take the spyware off the users' computer after the spyware makers have gone to such lengths to infect the computers in the first place. So the spyware companies have been attempting intimidation tactics to force the removers to omit removal of particular advertising software.

**Q:** Name names. Who's been the most litigious?

**Edelman:** One of the few companies to file suit is Claria, which sued PC Pitstop in 2003 alleging unfair business practices when PC Pitstop told its users its view of Claria's software. And New.net took the novel approach of suing Lavasoft in federal court.

Mostly these threats don't lead to litigation. Either the spyware vendors give up or they succeed in their intimidation tactics without having to go to court. There have been at least half a dozen examples just in the past few months.

It's absolutely fascinating to watch Symantec and McAfee struggle with this. It's a very different problem from what they're used to. Virus writers don't fight back.

**Q:** You've been on the attack against Ask Jeeves recently. Why?

**Edelman:** They're getting installations from kids' sites. I've been trying to figure out how these programs have such a large installed base: Who in their right mind would agree to have their computer become a vehicle for pop-up ads? It turns out that many of these programs target kids. They advertise their software at kids sites. They bundle it with videogames. They use advertisement images like smiley faces.

Ask Jeeves has a search engine that nobody really wants to go to. To get users to come, they push these toolbars. But if the toolbars are installed without proper notice and consent, then the entire business collapses. They have no legitimate business source of any substantial traffic to their Web site.

**Q:** Ask Jeeves just tries to get people to download their toolbar. Does that make it spyware or adware?

**Edelman:** It's not exactly spyware like the others. It doesn't show pop-up ads. As far as I know it doesn't track and transmit to its servers every Web site you visit. Yet it uses equally tricky installation tactics. (Editor's note: This week, CBS MarketWatch calculated that Ask Jeeves is valued at $1.8 billion and receives up to two-thirds of its search traffic from sources that also distribute adware.)

**Q:** How much money have you made by consulting for anti-adware companies so far?

**Edelman:** I've made enough to pay for law school.

**Q:** What next?

**Edelman:** I don't know. I might end up teaching. I can see myself practicing law and potentially serving as some sort of a professional consultant. ❖

# Spyware's adversary is software, policy, and action

*By David Southgate*

Whether you choose Spybot-S&D, SpySweeper, or any of a myriad of products to detect spyware on the computers at your small business, one product alone won't do the job. You'll need a comprehensive approach to rutting out spyware, according to Robert Siciliano, author of *The SafetyMinute :01*.

A true anti-spyware plan of attack must include the following:

- Installation of more than one type of anti-spyware software
- Regular updates to spyware definitions
- Regular scans of desktops
- A security policy
- Training for staff and administrators on the damage spyware does to a business

Siciliano's Boston-based company, ID Theft Security, has been fighting the battle against spyware since 2003, says Siciliano. So far they're winning. But it's been an expensive battle as Siciliano estimates that spyware has cost his small business of only 18 workstations well over $20,000 in lost productivity.

## Spyware infiltrates

Although spyware began attacking his enterprise in 2003, the blow to productivity really began in 2000 with pop-up advertising. The ads were such an annoyance to his sales staff that Siciliano purchased LavaSoft Ad-Ware, a product designed to swat pop-ups.

But then came 2003 and spyware. Business was grinding to a halt, as CPU capacity maxed out when spyware began taking over.

"My employees were wasting a good hour to two hours a day just sitting there with the PC bogged down because the bandwidth was so slow," says Siciliano.

"In addition to the loss of bandwidth, we started to see different things happening to different hubs and servers. We traced it back to what we considered to be spyware," says Siciliano.

Because ID Theft Security's staff was a group of heavy Internet users, the problem compounded rapidly. "More than likely we were just getting [spyware] from surfing the Net. Some of the employees were downloading stupid stuff, like tool bars that would tell you what the temperature was outside. They were downloading screensavers, peer-to-peer programs, ridiculous programs that would be billed as something that would clean out your registry, but in fact weren't."

## Siciliano declares war

Siciliano turned to his IT director and a young IT prodigy to address the issue. In early 2003, before they knew of anti-spyware, the team worked on the problem manually—a painstaking process of looking into the C: drives of every computer to identify and delete programs that shouldn't be there.

"We found malicious programs on our C: drives that were hidden under a variety of different names that looked like they might have been simple programs, but were in effect spyware programs," says Siciliano.  In some machines, it took repeated efforts to rid the machines of spyware, involving a delete, reboot, and delete again process. Still spyware kept on coming back. So Siciliano escalated the anti-spyware campaign.

Siciliano describes his initial approach as very reactive. "It was really a work in progress," he says. "We kept being bombarded by different programs. As proactive as we wanted to be, we were always reactive because new things would pop up."

Among Siciliano's next steps were to clamp down on the Net activities of his workforce. He added a self-written security policy and told the staff they were not to download anything from the Internet. Periodically, he would update the policy and reinforce the changes with more training.

He also added desktop monitoring software to the frontline computers for new hires. The computer monitoring takes snapshots and records keystrokes throughout the day. A wrong move during their first few months, and the new employees didn't stick around for long.

"I didn't want to have that Big Brother-Type atmosphere in my company," says Siciliano. "I explained to them, you're eating up my bandwidth, you're wasting my valuable time. It seemed to work."

In the latter part of 2003 and early 2004, Siciliano installed Spybot-S&D and Norton Security on all the workstations, which took care of most of the remaining issues.

"The programs are low cost and they do the job," says Siciliano. "I run them both and have them scheduled to run late at night, 2 to 3 in the morning. My Norton's Security picks up stuff that the Spybot and Lavasoft does not."

Today, due to regular efforts of his two-person system administrator team, who spend a combined eight hours a week administering the network, ID Theft Security's workstations are free of Spyware. "I do not have pop ups, I do not have spyware, and my bandwidth is, well, I'm flying," he says.

Every small business should have solved their spyware problem by now, says Siciliano. To continue to battle with spyware is to continue to waste valuable staff time and computing power.

"This is 2005, how can you allow that to happen," says Siciliano. "It's a constant battle. If you're not paying attention, then you're going to get bit." ❖

# Identify spyware symptoms and slowdowns

*By Steven Pittsley, CNE*

Nothing is free, especially things that run on your computer. Spyware organizations may try to make it seem otherwise, but every process, application, toolbar, and piece of code uses some amount of your computer system's resources. Even something as innocuous as a cookie consumes a small amount of resources. Although each piece of spyware may not be a resource hog by itself, the combined toll of 30, 40, or more spyware applications will definitely have a negative impact on even the most robust system. In this article, you're going to learn some of the common symptoms that will help you recognize spyware that's installed on a system. You'll also learn how spyware affects a computer system by using valuable system resources, either alone or when combined with other spyware applications.

## Spotting spyware: Browser clues

Recognizing some types of spyware is easy, but other types are good at hiding themselves. The most prevalent and easiest form to recognize is adware, since its purpose is to display ads in pop-up browser windows. When an adware program is installed on a computer, an abundance of pop-up windows will display. Some adware programs generate multiple pop-up windows when users view a Web page, subjecting them to two, three, or even four pop-ups whenever a new Web page is opened. Some adware programs are designed to display pop-up windows even if the computer is offline.

Another favorite implement of the adware networks is the browser toolbar. This is a small program that embeds itself in the browser window and claims to increase functionality by making it easy for the user to shop, surf, or search. The aid that browser toolbars provide is debatable, but they record demographic and surfing habits for the adware organization. Many of these applications also generate pop-up windows. If a new toolbar suddenly appears in a browser window, it's a sure sign that the computer is infected with spyware.

Some adware companies install code that modifies the browser settings and changes the home page. Other spyware applications will redirect the browser from the intended Web site to a competitor's site. For example, a user might direct the browser to Google only to have the spyware application redirect the browser to a competitor's search engine. These types of overt changes are always the direct result of spyware applications.

Another browser-related indication that a spyware installation has occurred is that the [Tab] key doesn't work when the user tries to navigate between fields in the browser, or the [Alt][Tab] key combination doesn't switch to another window. Changing or disabling the key functionality forces the user to view the pages that the spyware programs display. This type of programming is rare and is relegated to the most aggressive of advertisers.

## Systray icons and error messages

Spyware applications affect other parts of the system besides browsers. One obvious sign of a spyware installation is a new icon in the system tray. Once again, the spyware companies claim that starting the background process during system startup and adding the tray icon adds functionality for the user. However, in reality, these programs do little more than collect information and send it to the parent organization. In addition, if several spyware applications are added to the startup folder, the startup process is slowed down.

The random appearance of error messages clearly indicates that something is wrong with a computer system. Because many spyware applications are not written with the stringent development processes used in traditional software organizations, these applications have a tendency to corrupt the operating system environment. As a result, users will begin to see error messages during system startup or shutdown or when they attempt to use other applications. Depending on the types of problems caused by the rogue code, some users may even experience system crashes and blue-screen error messages. Left unresolved, these errors can eventually render the system unusable.

## Dial-up connections

Although broadband Internet access is quickly becoming the norm, many people still use dial-up connections. People using these slow connections will suffer from spyware applications that send data across the dial-up connection. Some spyware applications are even designed to secretly install a dialer program, which covertly makes changes to the system and replaces the user's dial-up settings with a new configuration. Dialers typically place long-distance calls that the user is charged for, although many telephone companies will forgive the amounts if the user can prove that the calls were placed by the dialer application. These types of invasive applications are rare nowadays, but one company notorious for dialer programs is Alyon Technologies.

## Depleting system resources

Perhaps the most common complaint about spyware is that it slows down the computer system. Applications running as background processes or in browser windows can consume a great deal of system resources, especially if several of them are installed on the system. Although this problem is more apparent on older systems that do not have an abundance of resources by today's standards, even new systems with lightning-fast processors and 512 MB or more in RAM can be brought to their knees by resource-hungry spyware applications.

Spyware applications use system resources in a variety of ways. First, the programs use memory and CPU cycles when they are running. If more than one adware application is installed and running, the combined effect can be quite dramatic, especially as they begin to open pop-up windows. Not only does this drain system resources and slow down the computer, but viewing Web pages can be quite difficult because the user is forced to waste time closing the advertising windows.

Spyware programs also use network bandwidth to open the advertising pages and send demographic information to the adware organization. Again, one application may not put a large dent in network bandwidth, but if several are active, they can consume a significant chunk, especially if the user is on a dial-up connection.

One type of system resource that is often overlooked is disk space. All forms of spyware use disk space. Although the amount is often small, as spyware applications accumulate on a computer, space consumption escalates. Even the relatively benign cookies can consume a large amount of disk space if thousands of them are saved on the drive. It's not uncommon for several megabytes of disk space to be used for spyware-related applications. This won't affect users who have a large hard disk, but those who have older systems and are pressed for space could benefit from the additional space freed by removing the spyware files.

In addition to using system resources, spyware applications may make registry modifications. This can have catastrophic consequences on a computer system if the application is poorly written. As we noted earlier, these types of modifications can make your system begin to display random error messages or cause crashes. Left unchecked, these problems can ultimately degrade system performance or make the system unusable.

## Time, effort, money

Perhaps the biggest resource drain is the amount of time and money it takes to combat the presence of spyware applications. Corporate technology departments are seeing a large portion of their resources dedicated to removing spyware and preventing it from infecting the workstations on their corporate networks. But average computer users also suffer. They don't have the technological savvy to understand the problem or resolve it correctly. Instead, they're forced to pay computer professionals to remove the spyware from the system or use a system rescue disk to restore the computer to its original state. Neither of these scenarios is appealing for the typical user.

## Wrap-up

As you can see by the examples in this article, the various forms of spyware can be quite disruptive to computer users on all levels. This new form of advertising is much more invasive than its print and broadcast cousins. Consumers can simply ignore ads delivered by those media, but spyware forces the computer user to interact with the pop-up window, toolbar, background process, or other form of code. Recognizing when spyware is installed on a computer system and removing it promptly is the best method of protecting computers from catastrophic problems caused by spyware. ❖

# Eliminate spyware challenges with these 10 tips

*By Scott Lowe, MCSE*

Spyware continues to plague the IT landscape and will continue to do so for the foreseeable future. While Congress has attempted to begin tackling these kinds of problems, laws just won't be enough to eradicate this menace. Further, in days of old, spyware solutions were decentralized and not always appropriate for reasonable enterprise use. Today, the landscape has changed, and here are some tips for you to consider while you tackle the challenge of instituting a spyware solution in your organization. These tips will help you get a handle on spyware in your enterprise

## Centralized management

Until somewhat recently, spyware eradication at the individual desktop was something of a hit and miss scenario. While there are many products that address the spyware issue, ranging in price from free up to tens of thousands of dollars for site licenses, many of these products lacked a critical component to managing the spyware mess: central management.

Without centralized management, the IT staff is left to deal with a critical service on each individual machine; lack of a centralized management console results in an inability for a CIO to gain critical metrics via reporting that he or she can use to help reinforce staffing and budget requests. Further, lack of central management means that software or definitions on a client workstation could be woefully out-of-date, leaving said workstation wide open.

Fortunately, the usual antivirus players, and some newer, spyware-focused players, have hit the market with enterprise-grade antispyware solutions that include central management, helping keep the job of protecting the corporate network wieldy.

## Protect with a layered approach

If you scan a spyware-infested computer using the client that was bundled with the expensive antispyware solution you just implemented, the software will probably report back that the computer was successfully cleaned, and show you a report proving the point. And, when you manually check one of the data points, you'll be able to verify that the software did exactly what it said it would do. Now, scan the system with a different antispyware product.

The chances are fairly decent that this second product will clean spyware that the first one did not catch. Spyware is notoriously difficult to eradicate and one solution often isn't enough. Obviously, you don't want to deploy two corporate antispyware products to every desktop. Instead, consider a layered approach.

Through the installation of an inline network gateway device that runs a different spyware-scanning engine from the one you use on the desktop, you can begin to eliminate spyware at the entry point to the network… before it even hits the user's desktop. The multilayered approach to the spyware dilemma helps to further protect your PC. Besides, it's easier to handle spyware if it never even gets to a PC.

## When possible, use an active agent solution

There are some different ways that a scanner—whether it is a virus scanner or a spyware scanner—can look for problems. First, it can simply make use of a definition file and look for things on a client that match items in the definition file. When this happens, the matching item is handled in whatever way you specify. Or, you can have a solution that actively monitors and watches all activity to and from a computer.

Often, an active solution will be able to learn about normal behaviors and take action even when it notices something out of the ordinary. A definition file is out-of-date as soon as you download it, and there is always a delta between what it can look for and what kind of spyware has been released since the last update.

## Reduce the success rate of phishing expeditions

You've gotten the e-mail: "Click here, and repair your damaged eBay account now! If you don't, we'll close your account and take away your children. Oh, by the way, to repair your account, we need your name, address, social security number, all of your previous addresses and a few of your credit card numbers… just to verify who you are, of course." Unfortunately, phishing sites have evolved from poorly designed and written pages into impressively complete mimics of Web pages of well-known companies.

Why do these scam e-mails keep coming into your inbox? Answer: Because they work. When you choose your next enterprise-grade antispyware solution, look for one that can help you protect your employees and your company from these kinds of phishing trips.

## Plan for growth

When you're considering and evaluating the various antispyware solutions available on the market, look down the line. Many of the solutions either on, or hitting, the market today are scalable up to tens, and even hundreds, or thousands of machines. Of course, you won't be using a single server to manage spyware for a 100,000 machine network, but you should still be able to manage their entire antispyware service from a single location which, in turn, controls the various down-level distribution servers.

## Antivirus and antispyware go hand-in-hand

Some people see spyware and viruses as different problems that need to be combated in different ways. Some see them as the same kind of problem: an unwanted item on a client workstation that can damage files, leak proprietary information, and sap productivity.

When you're looking for a solution to solve your spyware problem, consider rolling your solution in with your antivirus solution. After all, a single-agent solution is easier to manage and may end up costing less than deploying parallel infrastructures to deal with vermin.

## Participate in vendor information-gathering

Many vendors build in to their products the capability to report back to central command with information regarding new potential threats. Some see this kind of communication as a security breach. However, if it fits in with your organization's privacy policy and you can work with the vendor to make sure such a transmission is secure, try to make an effort to participate in this kind of "community service." You'll be helping your vendor to more quickly identify new spyware, allowing them to release an update more quickly. Of course, this won't work for every organization, but the more that take part, the better the updates will be.

## Consider URL controls

Most spyware is acquired through visits to malicious Web sites and downloads from said sites. If you could block access to sites through which spyware is known to be distributed, you could help to prevent some spyware infections from taking hold in your environment. Whether you use a gateway device and/or a desktop client, look for a product that can help you block, or filter, access to these sites, or that integrates into Internet Explorer to help users avoid these kinds of sites.

## Consider differing scenarios

Even within the same organization, you can't always expect every desktop and user usage pattern to be the same 100% of the time. So, why should you roll out an antispyware solution that locks you into a single policy or that makes it difficult to change a policy—for example: changing the time of day that a full scan is run? If you have shift workers or mobile users, you need to take into account their usage needs and plan accordingly. Many enterprise-grade solutions today allow you to place computers into specific management groups, allowing you to enforce different requirements on different users.

## Get antispyware software

This seems simplistic, but many organizations have been slow to respond to the burgeoning spyware threat, ranked by some to be the number one security problem affecting companies today. It's time now to do an analysis to see how much productivity and how many bottom-line dollars you're losing because of this threat. With the right information and justification, including protecting key corporate information, senior management may start to see the value in acquiring such a service, if they haven't already. ❖

# Use these techniques to fight back against spyware

*By Brien M. Posey, MCSE*

It never ceases to amaze me just how hostile the Internet really is. As if fighting with things like spam, pop-ups, and viruses wasn't enough, keeping spyware off of users' computers has practically turned into a full-time job. The reason why keeping spyware at bay is such an ordeal is because there are so many different types of spyware, and because spyware authors go to great lengths to ensure that you won't be able to get rid of the various spyware modules. Using these techniques, you can get spyware under control in your organization.

## What is spyware?

In case you didn't already know, spyware is a generic term usually applied to what I like to call "browser parasites." In most cases, spyware gets installed onto your computer without your knowledge when you visit a malicious Web site. In a way, spyware is actually sneakier than most viruses because most e-mail viruses get sent to you and don't actually activate unless you open an infected attachment.

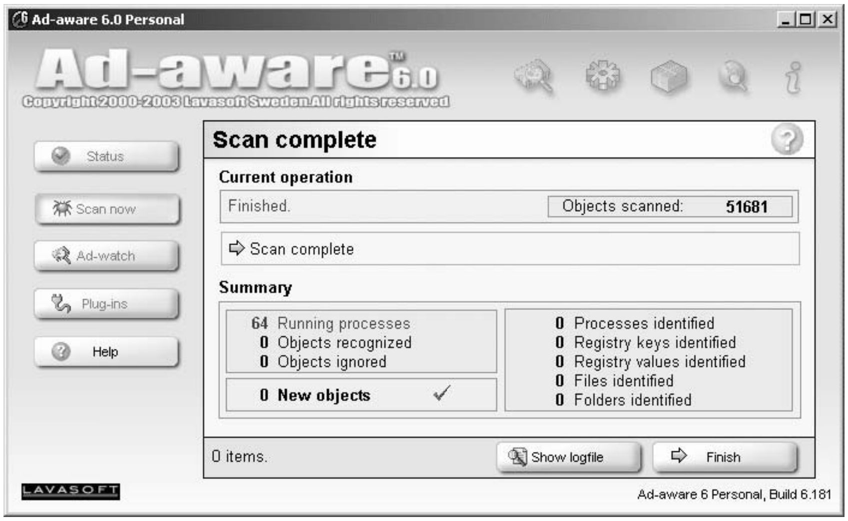
Most spyware modules install without your having to do anything other than visit a malicious Web site. Furthermore, visiting such a site is easier to do than you might realize. How many times have you accidentally mistyped the name of a common site into your browser and unintentionally landed on another site? Often sites that capitalize on common misspellings of popular site names are the most notorious for distributing spyware.

So what does a spyware module do once it's installed onto your system? It varies because there are many different types of spyware. Some spyware modules monitor your browsing habits so that they can flood your computer with pop-up ads based on the types of sites that you visit. Others look for things like credit card numbers and transmit them to some unknown destination across the Internet. Still other spyware modules hijack Internet Explorer, resetting the home page and filling your Favorites list with Web sites of the author's choosing.

## Why is spyware so hard to get rid of?

So far, you have seen that spyware has virus-like qualities, so you might be wondering what makes spyware so much more difficult to get rid of than a virus? Traditionally, controlling spyware just hasn't been as much of an issue as controlling viruses. Think about it for a second. Almost everyone has some sort of antivirus program installed, but how many non-IT people do you know have programs installed for preventing spyware?

**Figure A**



```
Scan complete
Current operation
Finished.                                  Objects scanned:   51681
⇨ Scan complete
Summary
64 Running processes              0 Processes identified
 0 Objects recognized             0 Registry keys identified
 0 Objects ignored                0 Registry values identified
                                  0 Files identified
 0 New objects          ✓         0 Folders identified
0 items.
Ad-aware 6 Personal, Build 6.181
```

Ad-Aware does a good job of getting rid of spyware and is free for personal use.

Although a lot of the antivirus manufacturers are starting to scan for spyware along with viruses, in most cases, the only way to really get rid of spyware is to use an anti-spyware program, such as Lavasoft's Ad-Aware, shown in **Figure A**.

In case you aren't familiar with Ad-Aware, it is, in my opinion, one of the better utilities for cleansing your computer of spyware. One of the best things about it, though, is that it is completely free for personal use. You can download the personal version of Ad-Aware from Lavasoft's Web site. Lavasoft also makes a professional version that will continuously monitor your PC for spyware.

If Ad-Aware works so well, you might be wondering why I don't just end this article right now and save you some reading. It's true that Ad-Aware works very well when it comes to removing spyware. The problem is that, depending on the type of spyware that's infecting your system, your system may not work correctly once the spyware has been removed. This problem is not specific to Ad-Aware, but is common among spyware removal programs.

## When spyware breaks Windows

Typically, when spyware removal breaks Windows, the symptoms look a lot like a DNS error. You might be able to ping a favorite Web site by IP address, but not by DNS name. When you attempt to access the site, Internet Explorer typically displays a message stating that the page cannot be displayed.

To understand why Windows might malfunction once spyware has been removed, you need to understand a little bit about the way that Windows attaches your computer to the Internet. As you probably know, computers communicate across the Internet through the use of the TCP/IP protocol. Windows implements TCP/IP through a mechanism called Winsock.

Winsock, however, is not made up of a single file. Instead, Winsock takes a layered approach to implementing TCP/IP in a chain-like fashion. If you were to remove a file from the chain, Winsock would cease to function properly and Internet communications would be either handicapped or completely disabled.

Some spyware modules exploit Winsock. There are certain benefits to doing this. First of all, the spyware module appears to be part of the operating system and therefore is more difficult to detect than other types of spyware. Second, if the spyware module is hooked into the Winsock chain then it makes it extremely easy for the module to monitor all Internet- (and network-) based communications. Finally, if a spyware module can trick Windows into thinking that the module is a part of the operating system, then the module will not be limited to the permissions granted to the machine's current user. In most situations, the operating system and its subcomponents have full permissions over the machine.

Here's where things get tricky, though. Imagine that a spyware module has infiltrated the operating system and has hooked itself into the Winsock chain. Now imagine that you ran a spyware removal program that was able to detect and remove the module, but now the Winsock chain is broken and Internet access does not work. In a situation like this, it would seem as though you should be able simply to reinstall Windows over the existing copy, and that in doing so, you would replace any missing files, thus relinking the Winsock chain in the process. Unfortunately this technique doesn't work, and here's why.

Microsoft designed Windows to be upgradeable and adaptable. Therefore, the components included in the Winsock chain are not hard-coded into Windows. Instead they are called through the system's registry. Any time that you reinstall Windows over an existing copy, the Setup program will refresh the system files, but it will make every effort to preserve any customizations that have been made to the registry. This means that if a spyware module was designed to sit in between two normal Winsock components, then the registry may still try to call the spyware module even though the spyware module has been removed and Windows has been reinstalled.

The only way to really fix the problem is to rebuild the Winsock chain and correct the Winsock-related entries within the registry. Keep in mind that editing the registry is dangerous because an incorrect modification can destroy Windows and/or your applications. I therefore recommend that you perform a full system backup prior to attempting the procedure that I am about to show you.

To manually rebuild Winsock, locate and delete the following registry keys:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock2
```

After removing these keys, you must close the registry editor and reboot the machine. When you reboot the machine, Windows will look for the registry keys that you have deleted. When it does not find them, it will recreate them from scratch, thus correcting the registry problem.

After the machine reboots, you must reinstall the TCP/IP protocol. To do so, right-click on the machine's network connection and select the Properties command from the resulting shortcut menu. This reveals the connection's Properties sheet. Now, click the Install button, select Protocol, and click Add. Next, click the Have Disk button and when prompted, enter *C:\Windows\inf* (where C:\Windows is the path to your Windows directory). Select the Internet Protocol (TCP/IP) option from the list of available protocols and click OK. Reboot the computer to complete the operation.

Although this procedure will fix the Winsock problem, there is an easier way to get the job done. Someone has created a free utility called Winsock Fix that automates the procedure. Keep in mind, though, that the utility still works by modifying the registry, so it's a good idea to back up your system prior to running it. You can download Winsock Fix from DSLReports (**http://www.dslreports.com/r0/download/544752~62fe0e8dc00fac87e6f0f83c54d283a4/WinsockFix.zip**).

## Software restriction policies

One way that you can fight spyware is to use a little-known Windows XP security feature called a software restriction policy. Software restriction policies were originally designed to help administrators to keep unauthorized software, such as games, off of network workstations. In some cases, though, a software restriction policy can be very effective in the fight against spyware.

The catch with using software restriction policies is that although there are several different ways to set them up, for all practical purposes, you need to know what software it is that you are trying to block. For example, you can't just configure the software restriction policies to keep games off of a workstation, but you can specify which games should be blocked, assuming that you know the name of one or more of the files that make up the games. It works the same way for fighting spyware. You need to know the name of the files used by a spyware module before you can block it.

So, you can't use software restriction policies as a catch-all solution to spyware because new spyware modules come out every day, and many actually use system files (which can't be restricted). The policies are effective, though, against some of the more well-known types of spyware.

A good example of this is Gator Corporation, which recently changed its name to Claria Corporation. I'm not going to outright refer to the Gator software as spyware, because recently Claria has been filing libel suites against anyone who does; however, Claria's software does have that reputation.

In case you aren't familiar with the Gator software, here's how it works. Gator is an electronic wallet. It keeps track of your personal information so that any time you are asked to fill out a form on the Web, Gator automatically fills in as much of the information as it can automatically. It sounds nice in theory, but in exchange for this convenience, Gator requires you to allow Claria to monitor your Web browsing habits and display targeted pop-up ads on your PC through the Gator Advertising Network (sometimes referred to as GAIN).

One thing that separates Gator from other types of spyware is that they actually disclose upfront that they will be monitoring your Web surfing habits and displaying ads on your system. Although they do disclose this information, the Gator installer tends to pester and entice users into installing it. Fortunately, you can block Gator through the use of software restriction policies.

There are several different versions of Gator floating around, but if you create a software restriction policy that blocks the files FSG.EXE, FSG_3202.EXE, and TRICKLER.EXE, you can prevent users from infesting workstations with Gator.

To create a Gator-blocking software restriction policy in Windows XP, open the Control Panel and click the Performance And Maintenance link, followed by the Administrative Tools link. Next, double-click the Local Security policy icon to open the Group Policy Editor.

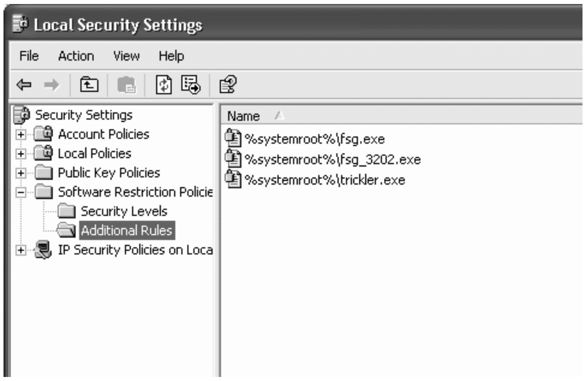
When the editor opens, navigate to Security Settings | Software Restriction Policies | Additional Rules. Right-click on the Additional Rules container and select the New Path Rule option from the resulting shortcut menu. When you do, you will see the New Path Rule dialog box. Enter %SYSTEMROOT%\FSG.EXE into the Path box. Make sure that the Security Level option is set to Disallowed, and enter a description indicating that you are preventing Gator. Click OK and repeat the procedure for the FSG_3202.EXE and TRICKLER.EXE files. The new software restriction policies will look something like what you see in **Figure B**.

## Using a firewall to prevent spyware

During one of my more recent spyware removal endeavors, a user asked me how it was possible for her computer to become infected with spyware when she had a firewall. The truth is that a firewall will do very little to prevent a spyware infection. Keep in mind that most of the time when an infection occurs, it's because you visited a malicious Web site. The malicious code is usually passed through TCP port 80, along with the site's other HTML code. Since Port 80 is the standard port used for browsing the Web, a firewall isn't about to prevent traffic from flowing across this port.

Just because your firewall doesn't usually prevent a spyware infestation doesn't mean that it is useless in the war against spyware though. Think about it for a moment. The main function of spyware is to transmit information about you or your browsing habits to someone else. Even if your firewall can't prevent spyware

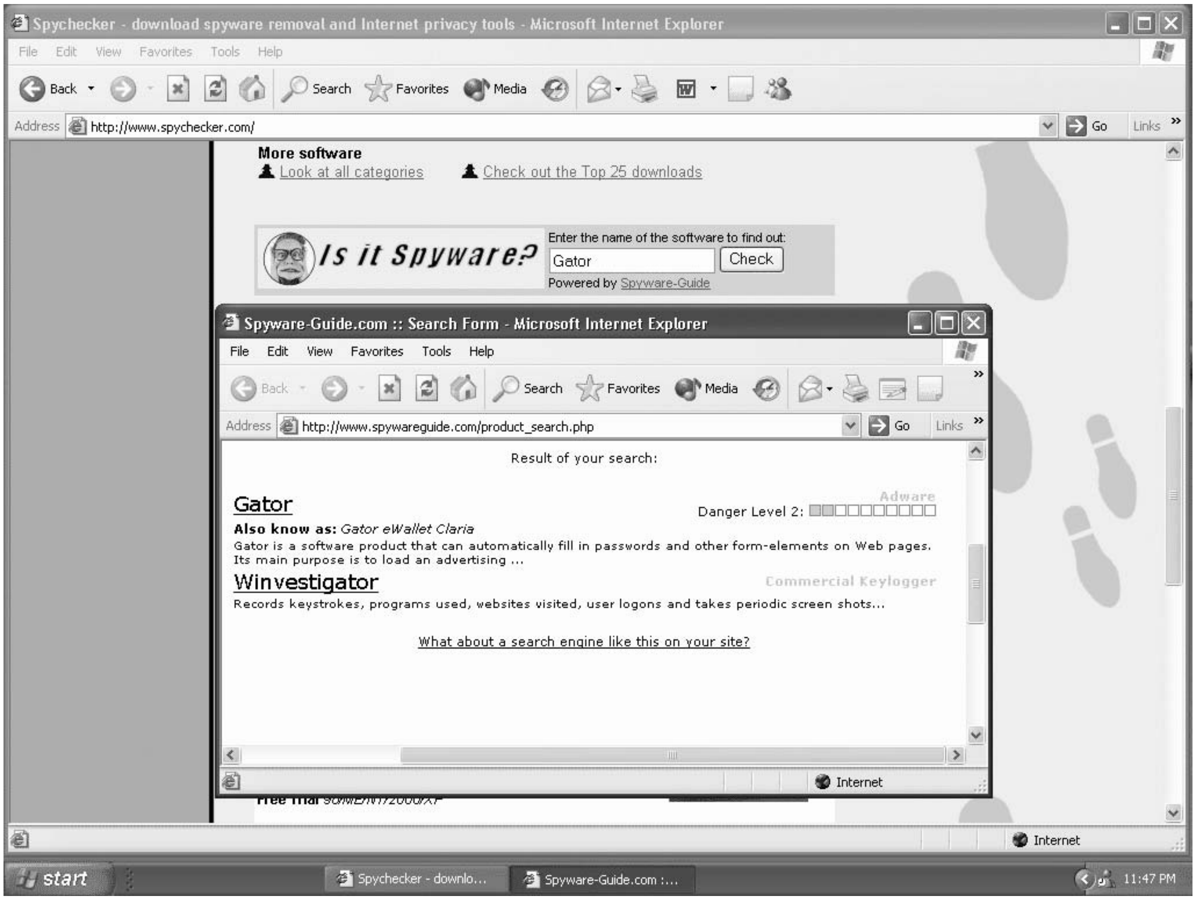
## Figure B



%systemroot%\fsg.exe
%systemroot%\fsg_3202.exe
%systemroot%\trickler.exe

Some spyware can be prevented by using software restriction policies.

## Figure C


Spychecker - download spyware removal and Internet privacy tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.spychecker.com/
Go Links
More software
Look at all categories
Check out the Top 25 downloads
Is it Spyware?
Enter the name of the software to find out:
Check
Powered by Spyware-Guide
Spyware-Guide.com :: Search Form - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.spywareguide.com/product_search.php
Go Links
Internet
start
Spychecker - downlo...
Spyware-Guide.com :...
11:47 PM

Gator

Result of your search:

Gator — Adware — Danger Level 2: ■■□□□□□□□□

**Also know as:** *Gator eWallet Claria*

Gator is a software product that can automatically fill in passwords and other form-elements on Web pages. Its main purpose is to load an advertising ...

Winvestigator — Commercial Keylogger

Records keystrokes, programs used, websites visited, user logons and takes periodic screen shots...

What about a search engine like this on your site?

Spy Checker offers a free database of applications containing spyware.

from getting into your PC, it can prevent potentially sensitive information from being sent back to the person who wrote the spyware module. Just configure your firewall to restrict outbound traffic. Normally, a default firewall configuration will consider all outbound traffic to be safe. I recommend restricting all outbound traffic except for on a few ports. For example, you will probably want to keep the ports used for HTTP, POP3, and SMTP open.

## When all else fails, check the database

Although most of this article has focused on spyware infestations that occur by accidentally stumbling onto a malicious Web site, malicious Web sites are definitely not the only source of spyware. Anyone who has ever visited download.com knows that there are thousands of different applications freely available for download. Although most free applications are exactly what they claim to be, there are applications available for download that will secretly install spyware onto your machine when you install the application.

So how do you know whether or not an application is safe? You could read the application's license agreement or terms of use, but such documents can be tough to understand and not all purveyors of spyware actually disclose their practices. A better solution is to simply ask someone who knows. The Spychecker Web site contains a database of applications known to have spyware attached. If you are considering installing a questionable application, try searching for the application in the Spy Checker database to see if it contains spyware. You can see an example of this in **Figure C**. ❖

# Protect your network from adware and spyware

*By Brien M. Posey, MCSE*

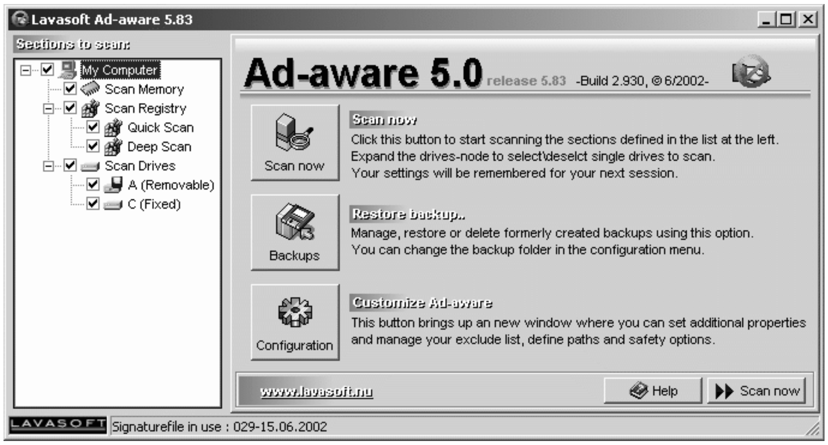
Just as fast as you secure your network, either hackers or legitimate businesses will be trying to find a way to dig into your company's data. One of the latest security threats that network administrators face comes from adware and spyware. Although spyware and adware are not supposed to be malicious, they can allow important data to escape from your network by bypassing security you've placed on your network firewalls. Here's what you can do about this security breach.

## What are adware and spyware?

There are so many different types of spyware and adware that it is difficult to pin down a specific definition. Generally speaking, spyware is software that's designed to transmit information about your network to someone on the outside. Typically, spyware might transmit things like passwords, information about your operating systems, network share information, or even information about your domain structure.

Adware, on the other hand, is typically used to place ads on your computer. For example, suppose you're bombarded with pop-up ads when you visit a particular Web site. If you're visiting a well-known Web site from a legitimate company, there's a good chance that those pop-up ads might not have come from that

**Figure A**



Scan now
Click this button to start scanning the sections defined in the list at the left.
Expand the drives-node to select\deselct single drives to scan.
Your settings will be remembered for your next session.

Restore backup..
Manage, restore or delete formerly created backups using this option.
You can change the backup folder in the configuration menu.

Customize Ad-aware
This button brings up an new window where you can set additional properties and manage your exclude list, define paths and safety options.

Signaturefile in use : 029-15.06.2002

Ad-aware scans your system for various forms of adware.

company at all. It could be that some adware running in the background is generating the ads and displaying them as if they were a part of the company's Web site.

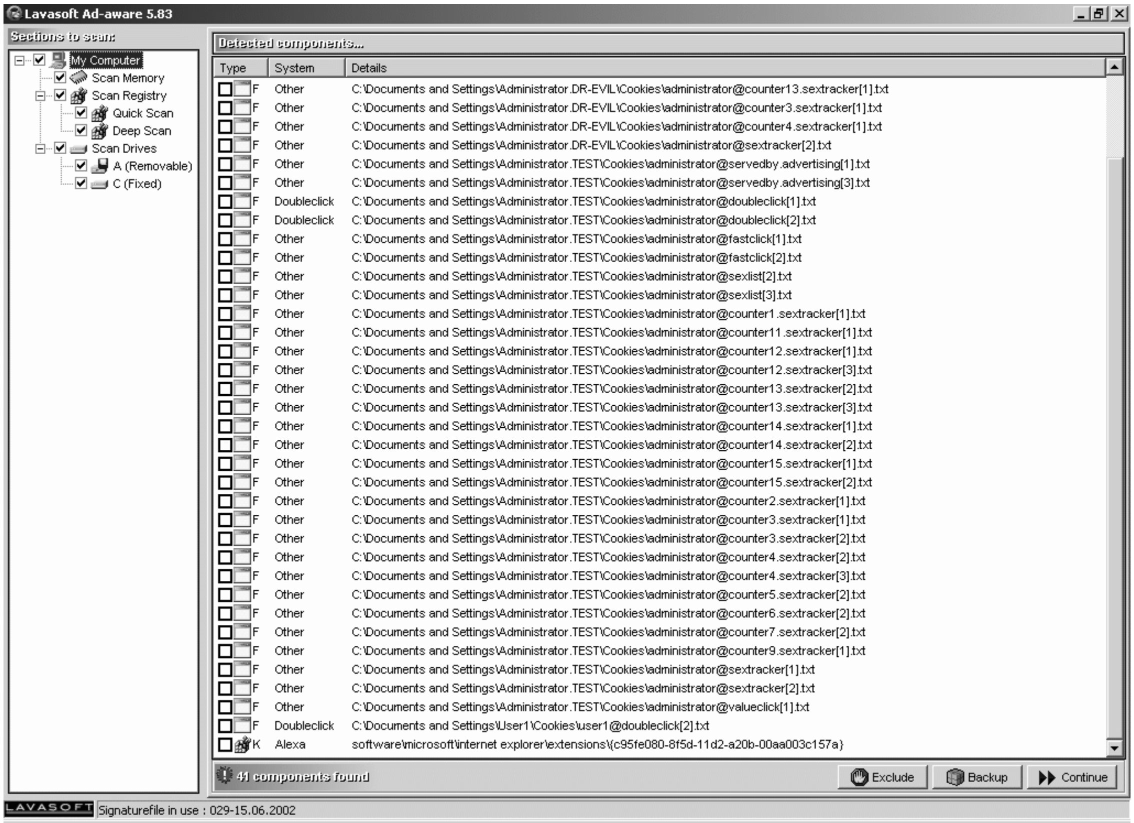
Some adware programs blur the line between adware and spyware by actually collecting information on which Web sites a PC visits, then sending that information to someone who uses it for advertising purposes.

## Spotting adware

There are several utilities you can download that will help you to detect and remove adware from your system. One of the most comprehensive adware removal programs is Lavasoft's Ad-aware. You can download Ad-aware for free through the download section of the Lavasoft Web site (**http://www.lavasoft.de/**).

As you can see in **Figure A**, Ad-aware is similar to an antivirus program, but is designed to spot adware instead of viruses. Like any good antivirus program, Ad-aware can be configured to scan Windows on boot up, and you can custom configure many of the scanning options.

**Figure B**

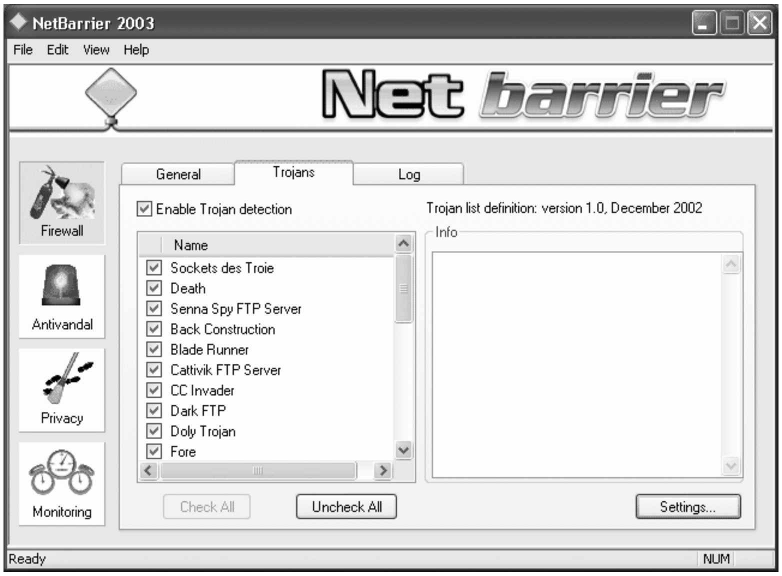


| Type | System | Details |
|---|---|---|
| □ F | Other | C:\Documents and Settings\Administrator.DR-EVIL\Cookies\administrator@counter13.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.DR-EVIL\Cookies\administrator@counter3.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.DR-EVIL\Cookies\administrator@counter4.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.DR-EVIL\Cookies\administrator@sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@servedby.advertising[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@servedby.advertising[3].txt |
| □ F | Doubleclick | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@doubleclick[1].txt |
| □ F | Doubleclick | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@doubleclick[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@fastclick[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@fastclick[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@sexlist[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@sexlist[3].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter1.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter11.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter12.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter12.sextracker[3].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter13.sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter13.sextracker[3].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter14.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter14.sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter15.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter15.sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter2.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter3.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter3.sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter4.sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter4.sextracker[3].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter5.sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter6.sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter7.sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@counter9.sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@sextracker[1].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@sextracker[2].txt |
| □ F | Other | C:\Documents and Settings\Administrator.TEST\Cookies\administrator@valueclick[1].txt |
| □ F | Doubleclick | C:\Documents and Settings\User1\Cookies\user1@doubleclick[2].txt |
| □ K | Alexa | software\microsoft\internet explorer\extensions\{c95fe080-8f5d-11d2-a20b-00aa003c157a} |

Signaturefile in use : 029-15.06.2002

In a week's time, 41 adware components had found their way onto one of my PCs.

Figure C



☑ Enable Trojan detection

Trojan list definition: version 1.0, December 2002

☑ Sockets des Troie
☑ Death
☑ Senna Spy FTP Server
☑ Back Construction
☑ Blade Runner
☑ Cattivik FTP Server
☑ CC Invader
☑ Dark FTP
☑ Doly Trojan
☑ Fore

NetBarrier 2003 from Intego is a personal firewall with built-in Trojan detection.

As you can see in **Figure B**, during a week's time, 41 adware components had found their way onto this machine. Most of these were in the form of cookies, but there were other types of adware present on the system as well. If all of this was on the system after a week of not being scanned, imagine how much adware could potentially exist on machines that have never been scanned.

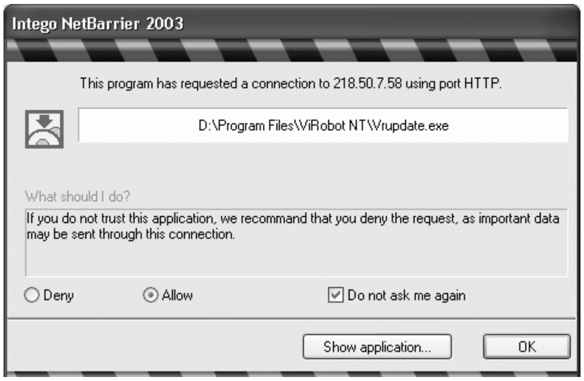
## Spotting spyware

There are lots of utilities that are designed to spot spyware as well as various types of malicious Trojans. One of my favorite utilities for spotting Trojans is a utility called NetBarrier 2003 from Intego (**http://www.intego.com/home.asp**).

NetBarrier 2003 is designed to act as a personal firewall. I'll talk about the product's firewall capabilities in a minute, but first, I want to show you NetBarrier's built-in utility that's designed to detect Trojans. To access this module, simply click the Firewall button, then select the Trojans tab. You'll see a list of known Trojans along with options for enabling Trojan detection, as shown in **Figure C**. What I like about this particular utility is that you can update its list of Trojans.

You probably noticed in Figure C that NetBarrier 2003 has a lot of features, including various privacy and antivandal mechanisms. I've worked with NetBarrier 2003 extensively, and it is truly an excellent product. Even so, using NetBarrier 2003 isn't really enough to completely safeguard your network against all Trojans.

**Figure D**



Intego NetBarrier 2003

This program has requested a connection to 218.50.7.58 using port HTTP.

D:\Program Files\ViRobot NT\Vrupdate.exe

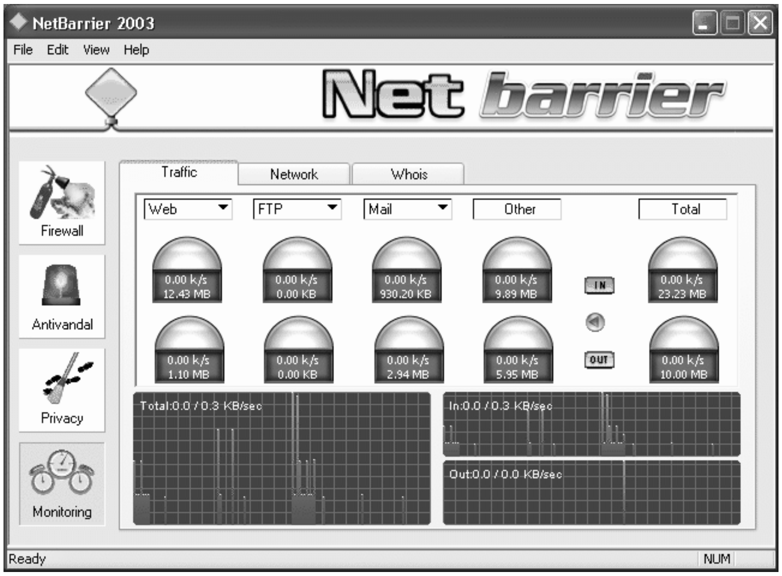
What should I do?

If you do not trust this application, we recommand that you deny the request, as important data may be sent through this connection.

○ Deny ● Allow ☑ Do not ask me again

NetBarrier alerts you to outbound traffic.

**Figure E**



NetBarrier allows you to monitor the specific types of traffic flowing across your network.

I have NetBarrier 2003 running on all of my computers. The program is set up to detect Trojans and act as a personal firewall. Between these features and the antivandal features, it's very difficult for a hacker or a Trojan to exploit an individual PC. However, I also rely heavily on my parameter firewall. The biggest difference between my configuration and the configuration most people use is that, rather than using my firewall as my first line of defense or my only line of defense, my parameter firewall is my last line of defense (from the standpoint of outbound traffic).

I work hard to secure each of my PCs to ensure that they don't become vulnerable in the first place. I also use the NetBarrier firewall to control what types of packets the PCs are allowed to transmit. I then configure my parameter firewall to block outbound traffic on most TCP and UDP ports. The only ports that I've left open were those required for common functions, such as sending e-mail.

If you're wondering why I even bother guarding my perimeter firewall against outbound traffic if I've got NetBarrier 2003 in place, it's because it's always possible that someone could shut down NetBarrier or that NetBarrier could malfunction. I also have devices on my network that aren't capable of running the Windows version of NetBarrier and could potentially be exploited.

## Advanced Trojan detection

If you use NetBarrier to detect spyware, use Ad-aware to detect adware, and use NetBarrier in combination with your parameter firewall, you'll stand a very good chance of winning the war against spyware and adware. However, there is always the chance that a Trojan could exist for which NetBarrier doesn't have a definition. This is similar to what happens when a new virus comes out. Until your antivirus software has its virus definitions updated, you're vulnerable to the virus. Likewise, if your PC gets infected by a Trojan that NetBarrier is unaware of, you're vulnerable until a new Trojan definition update has been received. During that time your PC could have already disclosed a lot of sensitive information.

Fortunately, NetBarrier has a feature that can help you to detect unknown Trojans. NetBarrier displays a pop-up message any time a program tries to send outbound traffic (see **Figure D**).

As you can see, NetBarrier displays the file that was transmitting the data and the port that was being used. You then have the option of blocking the action. When I initially installed NetBarrier, I was flooded with these warnings. You might have noticed in the figure that you have the option of suppressing future warnings about the specific transmission. If you suppress the warning messages related to normal network activity, then you'll only see messages related to unusual activity. This can help you to spot Trojan activity before any sensitive information can be disclosed.

Still another way that you can spot suspicious activity is by monitoring bandwidth consumption. In **Figure E**, you can see NetBarrier's mechanism for monitoring bandwidth. Although the screen is configured to show Web, FTP, and Mail traffic, there are actually dozens of different predefined traffic types that you can monitor. To put it bluntly, NetBarrier 2003 makes it possible to know exactly what your PC is doing with its network connection. ❖

# Multiple tactics can help keep spyware at bay

*By Steven Pittsley, CNE*

Removing spyware from a computer is comparable to a root canal: Both can be painful and time consuming. That's why the best way to combat spyware is to do everything you can to prevent it from being installed in the first place. Although nothing will protect you completely, you can follow some simple steps to reduce the amount of spyware that finds its way into your organization. Just think of these measures as brushing and flossing. They may not always prevent major problems, but if you don't do them, you're guaranteed to have serious issues at some point.

## Use spyware detection tools regularly

Antivirus software is a staple of every enterprise workstation these days. No IT staffer would even dream of deploying a workstation without it. Yet spyware detection tools are still scarce on company networks. A recent Webroot survey indicated that while 70 percent of organizations expressed concern about spyware, fewer than 10 percent of them have installed any spyware detection software.

Spyware detection tools, such as LavaSoft's Ad-Aware, are generally used to remove spyware that is already installed on a workstation. However, removing these programs is also an important part of preventing additional spyware from being installed on a workstation. Once a spyware program is installed on a computer, the author may send updates to the program. For example, a user could be presented with a window announcing an update to a program that's actually spyware. If the user agrees to update the software, the additional spyware is installed. Routinely running spyware detection programs can eliminate this threat.

## Keep operating systems and software updated

Network administrators understand the need for keeping the server and workstation operating systems and applications updated. Managers and small business owners often don't. This can present problems for IT pros, because skimping on updates can lead to problems that ultimately cost more than upgrading a few workstations or applications.

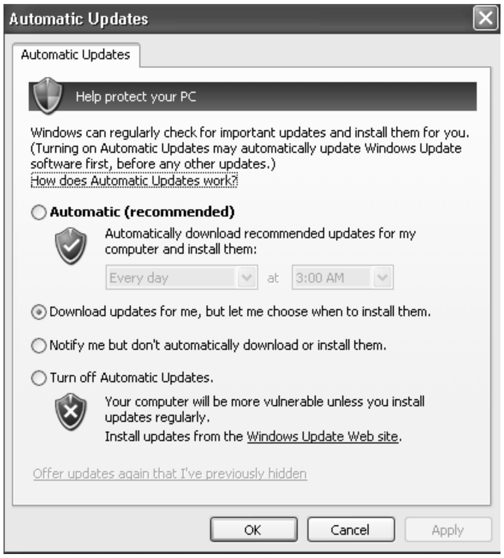
For instance, Windows 95/98 workstations still have a presence in many organizations, despite being outdated and lacking security. The absence of user permissions and restrictions allows anyone to install software on the computer. So, for organizations using Windows 95/98, the first step in reducing the risk of spyware (and avoiding many other issues) should be an upgrade to Windows 2000 or XP.

In addition to updating the workstation operating system, you should also keep application software updated. Software vendors regularly update their applications to patch holes that spyware authors exploit. For example, Microsoft's Windows XP Service Pack 2 includes an update to Internet Explorer that provides a pop-up blocker and an Add-On Manager, which shows a list of browser add-ons that have been installed. Often, these add-ons are actually spyware.

You should also install all service packs and hot fixes. These updates may target holes that virus and malware authors exploit. This is especially true of antivirus and spyware detection software. If the spyware definition file isn't current, the detection tool won't be able to identify the latest spyware. Generally, it's a good idea to check for updates at least once a week.

Microsoft recommends that you configure Windows to download and install operating system updates automatically. This isn't a viable solution in an enterprise, where you need to verify that the changes are compatible with your environment. However, if you work in a small organization or consult for a number of small business clients, you may want to configure Windows to either notify you before installing the updates or to notify you when updates are available. These two options give you control of when (and if) updates are installed. You can configure the Windows XP Automatic Updates settings by clicking Start | Control Panel | Automatic Updates. In the Automatic Updates dialog box, shown in **Figure A**, select the option you want to use and click OK.

**Figure A**



Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)

How does Automatic Updates work?

○ Automatic (recommended)

Automatically download recommended updates for my computer and install them:

Every day at 3:00 AM

● Download updates for me, but let me choose when to install them.

○ Notify me but don't automatically download or install them.

○ Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.
Install updates from the Windows Update Web site.

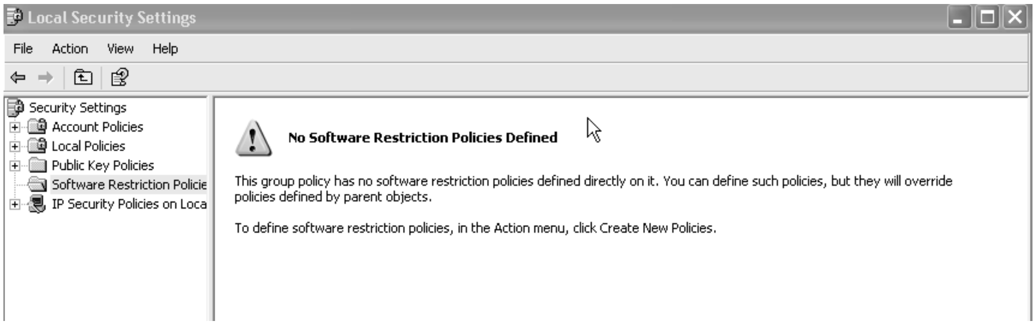
Offer updates again that I've previously hidden

## Limit Web surfing

Every minute that employees spend surfing the Internet costs their employers money in the form of reduced productivity or reduced network availability. Another less obvious consequence of user surfing is the time required for IT support personnel to remove spyware from workstations. This is a significant concern. A recent Dell survey reported that 20 percent of the calls to its help desk were related to spyware. Although the Dell help desk primarily services home customers, that's still an enormous amount of resources dedicated to resolving spyware-related issues.

One solution to this problem is to reduce the amount of external Web surfing users conduct. If particular employees don't need to use the Internet as part of their job, don't give them a browser application, or strictly enforce an Internet

Figure B



**No Software Restriction Policies Defined**

This group policy has no software restriction policies defined directly on it. You can define such policies, but they will override policies defined by parent objects.

To define software restriction policies, in the Action menu, click Create New Policies.

Figure C

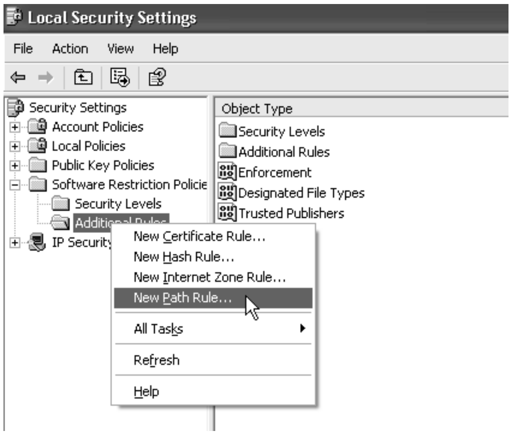
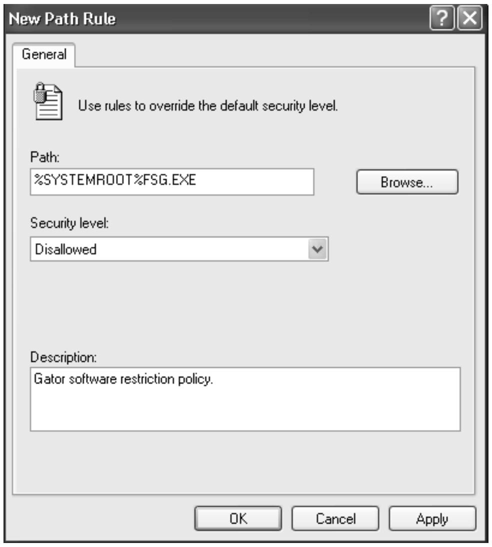


Figure D



Use rules to override the default security level.

Path: %SYSTEMROOT%FSG.EXE

Security level: Disallowed

Description: Gator software restriction policy.

usage policy. This type of policy will reduce technical support calls, free up network bandwidth, and possibly increase productivity.

## Use group policies and software restriction policies

In an enterprise environment, you can employ group policies to prevent software installation on user workstations. This is a good way to keep users from installing tempting applications such as the Google toolbar and WeatherBug, or any other type of software that has not been qualified for your network. To find out more about setting up group policies, download our "Windows Group Policy Quick Guide" (**http://techrepublic.com.com/5138-6355-5379477.html**).

If you work in a smaller organization, software restriction policies can offer a nice solution for preventing installation of specific programs. You must manually create a policy for each program, which makes it a time-consuming method of blocking spyware installation. However, despite this drawback, you may want to consider using a software restriction policy to prevent installation of certain applications, such as software from Gator Corporation (now called Claria Corporation). You might also want to prevent someone from reinstalling an application you just spent an hour removing.

To create a software restriction policy in Windows XP, click Start | Control Panel | Administrative Tools | Local Security Policy. The Local Security Settings dialog box will appear. Click Software Restriction Policies. If no policies are currently defined on the computer, you'll see the message shown in **Figure B**.

Now, click Action | New Policies, and you'll see two new entries under Software Restriction Policies. Right-click on Additional Rules and select New Path Rule, as shown in **Figure C**.

When the New Path Rule dialog box appears, enter *%SYSTEMROOT%\filename* in the Path field. For instance, typing *FSG.EXE* as the filename will block installation of a Gator Trickler file. If the application includes multiple files, you must create a restriction policy for each one.

Verify that the Security Level is set to Disallowed, and type a description in the space provided, as shown in **Figure D**. Once you create the software restriction policy, no one can install the file on that particular computer.

Since you have to know specifically which software installations to block before you can create a policy to block them, you'll need information on what files may be worth restricting. You can find out about known spyware and adware programs by checking a "parasite" list such as the ones offered by DoxDesk, Kephyr, and Pest Patrol.

## Use a firewall

Firewalls do a good job of preventing others from accessing your computer. Unfortunately, they do little to prevent spyware from being installed because most spyware applications come bundled with legitimate applications that you yourself install. Spyware is also usually passed through TCP port 80, which is the standard port used for browsing the Web. That means you can't block port 80 unless you also want to block all of your legitimate Web traffic. However, you *can* use a firewall to prevent information from being sent back to the adware company.

Most default firewall configurations consider all outbound traffic to be safe. But you might consider restricting outbound traffic on all ports except those used for HTTP, POP3, and SMTP. Although this won't prevent spyware applications from sending data through those ports, it will prevent applications from sending your personal information through any other outbound port.

## Wrap-up

Even if you follow every precaution we've considered here, chances are good that spyware will still end up on your users' machines. However, these steps will at least help reduce the amount of spyware that infests your organization. Regularly running anti-spyware tools, keeping operating systems and applications up to date, controlling employee surfing habits, restricting software installation, and using a firewall to help prevent information from being sent to adware companies will lessen the number of spyware root canals you have to undertake. ❖

# Block and remove spyware from your network

*By Mike Mullins*

Spyware (a.k.a., adware) is typically bundled with shareware and includes a mechanism for tracking your online behavior and reporting it to a centralized server. The centralized server builds a profile of your browsing characteristics and serves advertising and pop-ups that suit your online habits.

It isn't a bad concept: Instead of bombarding you with random advertisements, someone somewhere decided to let you develop your own advertising profile and then feed you ads that are targeted to your online behavior. However, bad idea or good, spyware has no place on the company's LAN.

## Block spyware

The best way to remove spyware is to not allow it in the first place. Don't load shareware or freeware on production machines. Also, instruct your users to avoid Web advertisements. Some spyware can be loaded simply by clicking on a Web advertisement in a browser. Since your company's LAN is for company business, block known advertisement sites. Blocking these sites has the added benefit of increasing available bandwidth to the Internet for your users.

The best way to block ad sites is to send the ad request from your Web browser to the host machine's loop-back address. To do this, add a *127.0.0.1 bad_ad_site.com* entry in the host file of every machine on your network. Then, when a Web page contains a reference to an ad located on the *bad_ad_site.com* server, your browser will first consult the host file to locate the IP address before sending a DNS request for the ad site content. The request for content will appear blank in the browser, so no cookies or spyware will be loaded or accessed.

Rather than spending months developing your own list of ad servers to enter into your host file, you can use Gorilla Design Studio's list, which contains over 17,000 entries.

## Remove spyware

What do you do if your machines are already infected with spyware? Check your clients and servers regularly for spyware entries, and regain control over network security by deleting all traces of the rogue programs.

You'll need a tool to remove the programs, cookies, and harmful registry entries on spyware-infected machines. I prefer Ad-aware Professional from LavaSoft. This tool removes spyware and provides real-time protection from an impressive list of spyware programs.

Removing spyware programs is essential to regaining control over your network security.

## Final thoughts

Spyware and adware-blocking programs have really matured. Take advantage of them for removing spyware and adware. However, if you find either spyware or adware on your company network, you have a much larger problem. Users should not be able to download and install programs containing these in the first place.

Before purchasing software to stop or block spyware or adware, take a look at the policy that allowed it to land on your machines. Software add-ons aren't a cure for poor or lax security. Improve security by crafting a comprehensive group policy on software installation and Internet Explorer policy settings.

Stop providing valuable information about your LAN and your users, and regain control of your network. Block all advertisements and don't dilute the administrative right to install programs. Users aren't responsible for network security; we are. ❖

# Anti-spyware apps use a variety of detection methods

*By Steven Pittsley, CNE*

Spyware applications are installed and working their clandestine trade. You know it because pop-up ads appear every time you open a Web page, and your system is slower than a car running uphill on ice. Now what? First, you have to find a good spyware detection and removal tool. However, all detection applications are not created equal. Aside from interface differences, the particular methods that these programs use can greatly affect how well they identify rogue applications. In this article, we'll look at the differences in the detection methods employed by the most common spyware-detection applications. We'll also explain how spyware is different from viruses and why antivirus applications generally can't detect spyware.

## Filename matching

The simplest form of spyware detection is filename matching. As the name suggests, this method scans the drive for specific filenames of known spyware. The files are then flagged for removal.

This form of detection works, but there is a considerable flaw in the theory. In an effort to subvert the detection software, spyware companies either change the filenames or employ a random naming strategy. Once the filenames are changed, the detection software is unable to recognize the spyware. Another problem with filename matching is that the detection software is unable to differentiate between a valid file and one associated with a spyware application. For example, suppose a popular adware program has a file named samplefile.dll associated with it. If a legitimate application also has an associated file named samplefile.dll, the detection software will flag the file for removal regardless of which application it is used for.

## File properties

Another method of spyware detection compares the properties of the file with those of known spyware. This type of detection is usually combined with filename matching, making it a little more reliable than simply comparing filenames. When the detection software matches a filename, file properties such as the size, publisher, and version are compared to the known values in the spyware definition database. If one or more of the properties match the defined parameters, the file is flagged for removal.

Combining filename and file property matching makes the detection software more robust. However, spyware authors are able to get around this form of detection easily by renaming the files, changing the publisher, slightly modifying the file size, or updating the revision. But the chances of erroneously removing a valid file are lessened with this form of spyware detection.

## File signatures

Filename and file property detection methods basically look at the wrapper around the program code. While this may be helpful in separating a Snickers from a Milky Way, the only way to know exactly what you're getting is to look inside the wrapper. In the spyware-detection world, this is done using file signatures to detect rogue files.

When searching for spyware, the detection software actually looks inside files for certain signatures, or patterns. When a matching signature is found, the file is flagged for removal. Although spyware authors may be able to easily change the filename or properties, modifying the program is a much more involved process. File-signature detection is a reliable method, and many popular detection software applications use it.

## Heuristics

Heuristic detection is similar to file-signature scanning, except that the detection software searches for certain instructions or commands that are not part of normal applications—such as a command to delete everything on the hard drive. Heuristic methods are generally used to detect malware and other malicious types of applications.

Heuristic detection is a good method for identifying spyware, but a purely heuristic system detects only malicious code, not things like cookies or adware. More effective spyware-detection applications usually combine heuristics with other methods, such as file sharing and filename matching.

## Registry scanning

Like all applications, spyware modifies the system registry during installation. Over time, these values can clutter the registry and slow down the computer. The registry may also become corrupted. Virtually all detection applications scan the system registry for traces of spyware by matching values for known spyware applications with those in the application's definition database.

## Comparing spyware and viruses

Spyware and viruses are completely different threats. Spyware is designed to collect demographic and personal information, display pop-up advertisements, or track shopping and surfing habits. Viruses rarely have any real purpose other than to annoy users or carry out malicious instructions.

Virus code is designed to propagate itself as often as possible. Although the program may try to hide itself inside another application, the virulent code is responsible for its own replication. Spyware also hides itself inside other applications, but it's not designed to propagate itself. Instead, it relies on the computer user to install the legitimate application. This is the fundamental difference between spyware and viruses.

Spyware- and virus-detection programs are also completely different, even though they use similar techniques to ferret out the offending code. Like some spyware-detection programs, antivirus packages use file signature and heuristic techniques, but the approach is different. Instead of searching only for known viruses, antivirus software uses heuristics to analyze code sequences in an effort to detect unknown viruses. This doesn't always work, but the attempt occasionally thwarts a virus outbreak before it becomes an epidemic.

Another difference between viruses and spyware is the size of the code. Virus code is usually quite small and easy to detect once the virulent code has been defined. Spyware is often quite large in comparison. Many spyware applications bring with them hundreds of files and additional traces, making it extremely difficult for the spyware-detection software to clean everything off the system. In addition, spyware authors are constantly changing their applications to avoid detection. In fact, many spyware authors use spyware-detection software to help them determine whether their changes are going to be caught. They work with the various detection packages to tweak the code until their application is no longer found. Thus, spyware-detection software must have a thorough understanding of each spyware application for successful detection and removal to take place. The detection application must know where all of the various folders, files, and registry entries are located and also know the dependencies between spyware elements and other associated applications.

Because virus- and spyware-detection applications are so different, you won't typically find a single application performing both tasks. This is due partly to the complex nature of the applications and partly so that vendors can generate multiple revenue streams. However, this trend is changing, as vendors such as Norton, Symantec, and McAfee enter the spyware-detection field. In the next few months, several new software packages will have antivirus and spyware-detection modules combined into a single package.

## Wrap-up

Spyware detection and removal is a complex procedure. As the big-name vendors begin to focus their sights on spyware, integrated virus- and spyware-detection packages will become available. Combining the two functions into one package should bring even more technological advances to the spyware battle and make it easier to remove both types of offensive code from your machines. ❖

# Ways to centralize your anti-spyware defense

*By Scott Lowe, MCSE*

Depending on your network environment, it's probable that spyware has become a bigger problem for your organization than viruses. There are a lot of reasons that this could be so. First, more and more people use the Web every day, and many don't take basic precautions such as reading before clicking "I agree" to an onerous license for a Web download. Second, since viruses have been recognized for many years as a serious problem, most companies have taken the appropriate step of installing antivirus software on all computers, often tied back to a centralized distribution and management system.

In my situation, I'm the IT Director for a small college with students that bring anything and everything to campus, including, in the past, a multitude of viruses. As such, we've installed Symantec Antivirus which is distributed to students from a central location. Through this central distribution center, we can make sure that antivirus software is installed the way we want for best protection, and that updates are regularly applied.

Now, spyware rears its ugly head. With its deliberate system-debilitating properties, spyware can be more of a productivity stopper than viruses ever have been. While there have been a number of spyware solutions, including SpyBot and AdAware, available for quite some time, many of the original spyware-busting applications lacked centralized distribution and update capabilities. Some of the solutions available now, however, solve one or both of these dilemmas.

## Software solutions

Software solutions provide a traditional means by which to detect and eradicate nefarious spyware. Centralized anti-spyware solutions work basically as you would expect. Generally, the software includes a server component from which anti-spyware client software is pushed to each organization's desktop. Further, there is usually some kind of administrative console from which you can easily and centrally configure clients and run reports.

I'll provide a view into some potential solutions for the rest of this section. This is by no means intended to be a comprehensive guide to every product available. Instead, I will go over a couple of solutions in the software space and a couple hardware solutions that you might consider.

### Sunbelt CounterSpy Enterprise

With client support for all versions of Windows back to Windows 98 Second Edition, Sunbelt's CounterSpy Enterprise has the features that you'd likely want in a centralized anti-spyware installation. Among its features is the ability to deploy client software in a number of different ways both completely and automatically.

The currently shipping version of the CounterSpy client uses Microsoft's (formerly Giant's) AntiSpyware engine. However, Sunbelt does not use the same scoring values that Microsoft's tool does, so, even though they share the same engine and definitions, each product rates spyware a little differently. This sharing agreement is only in place until July of 2007, so look for Sunbelt to switch engines and definitions in the next release.

CounterSpy Enterprise provides a number of reports to help you identify where you are most vulnerable and to, perhaps, mitigate problems in other ways. One report, an executive summary, provides a quick view of how many desktops have infestations, shows you the top ten pieces of spyware found, as well as the severity level of the various infestations and most infested machines on your network. Further, it breaks down the threats by categories such as "Adware," "cookie," "toolbar," and so on.

CounterSpy Enterprise also easily (and affordably!) protects Citrix and Terminal Server installation. According to Sunbelt, the company charges you for just a single agent for the entire server, even if a number of users with Windows terminals connect. For mobile users, CounterSpy allows them to be away from the management server for a period of time before they have to update their spyware definitions. Of course, you can always configure these machines to update over a VPN connection as well, so the window of updates can be pretty short.

Speaking of price, CounterSpy Enterprise runs between $10 and $24 per seat. CounterSpy also comes bundled for consumers, without a server component, and costs about $20 per seat when used in this configuration.

For more information about Sunbelt's CounterSpy Enterprise, visit **http://www.sunbeltsoftware.com/CounterSpyEnterprise.cfm**.

### Webroot Spy Sweeper Enterprise

Like CounterSpy Enterprise, Spy Sweeper Enterprise, as its name suggests, is an enterprise-level product with automatic deployment capabilities, a central management console, and reporting. Spy Sweeper Enterprise also includes the ability to keep mobile clients current by connecting them to webroot's update servers when these clients can't be easily connected to the corporate Spy Sweeper server. As with virus definitions, keeping your spyware definition file current is critical to successfully combating this problem.

On the client side, Spy Sweeper supports Windows versions back to Windows 98. The server, however, needs to be an operating system in the NT family—one of NT 4.0 SP5+, 2000, XP, or 2003. However, unlike CounterSpy, Spy Sweeper does not support Citrix and Terminal Services, although some reports indicate that it might work.

### New (and old) kid on the block: Microsoft AntiSpyware

While it lacks centralized deployment and reporting features, I should mention Microsoft's foray into the anti-spyware market. In late 2004, Microsoft acquired Giant Corporation, a company that developed an impressive, real-time spyware scanner, akin to a real-time virus scanner in that it actively monitors system activity against a spyware signature database to make sure the system stays free and clear of spyware. While the product does not yet have a centralized deployment server, you can use Active Directory for the initial deployment. Even though it lacks central management capability Microsoft's version of this product, currently available in beta, does keep itself current with new spyware definitions and regularly checks for new versions of the product itself.

As for cost, Microsoft has committed to providing the product to legal Windows users at no additional charge. While some might say Microsoft owes it to their customers to provide this service because of the various flaws in Windows, it's actually a very good product.

Beyond just using a definition file, users of Microsoft's AntiSpyware can opt to join SpyNet, which helps the software more quickly detect programs that should be considered spyware. SpyNet is an opt-in program whereby users of the product help to determine what programs should and should not be considered spyware.

Microsoft's AntiSpyware runs on Windows 2000, XP, and 2003. The current beta expires December 31, 2005. To download and install the software, visit Microsoft AntiSpyware Web page (**http://www.microsoft.com/athome/security/spyware/software/default.mspx**).

Again, while Microsoft's product doesn't provide for centralized deployment, it does keep itself current once it's on your user's desktops, and you can't beat the price! Of course, without the centralized management capabilities found in other products, Microsoft's product is incapable of providing statistics reporting regarding infection, which can be useful if you're trying to track down a particular problem.

Look for this consumer-oriented product, however, to turn into a paid product with centralized management for the enterprise.

## Hardware solutions

Like most things in IT, appliances have hit the spyware market. The appliance approach has the advantage that its only purpose in life is that for which it was designed—nothing more. Of course, regardless of whether you go with a software or a hardware solution, you probably want something full-featured, so I'll also go over a couple of appliance-based alternatives for the rest of this section.

### Barracuda Spyware Firewall

Barracuda has done well with its spam firewall appliance and recently released another similar-looking appliance that helps organizations prevent spyware infestations. Dubbed the Spyware Firewall, Barracuda's device is installed inline between a LAN segment and the organization's firewall.

What this means is that the Barracuda solution does not require a client installation in order to function. This can be good, or bad, depending on your situation. At my college, I might use this as a second-level measure, but would also have a solution that requires a client to be installed on each PC. Why? I have a large mobile population that includes hundreds of student laptops and a couple dozen administrative laptops. I have complete control over the administrative systems, but no admin rights to the student laptops. Therefore, a two-phased approach is our best bet. Use (and require) the client for all campus systems and, for those student's who ignore our requests, they'll still be partially protected by the inline solution, at least when they're on campus. It's not perfect, but it's a solution.

The Barracuda device is priced based on the throughput you want to achieve as well as feature set. The 5Mbps unit (the 210), for example, does not include the ability to block malicious IMs. On the other side, the premier unit achieves 200Mbps of throughput and includes the entire enterprise feature set, including IM blocking, caching, syslog support, and more.

The Barracuda 210 runs around $2,000 with Energizer Updates (definitions) running around $500 per year. The top-line 810 unit can run as much as $28,000 with Energizer Updates costing an additional few thousand dollars per year. The middle of the road Barracuda 410, which features up to 20Mbps of throughput and, with the exception of this slower speed and a smaller cache, includes all of the features of the 810, runs around $6,000 with Energizer Updates running a little under $1,500 per year.

For more information about Barracuda's foray into the anti-spyware market, visit **http://www.barracudanetworks.com/ns/products/spyware_overview.php**.

### Tangent Packet Hawk 2.0

Tanget's Pack Hawk 2.0 is a relatively new product in the market, but includes enterprise-level features, including centralized management and reporting, Quick Start assisted installation to get the device up and running quickly, and, like the Barracuda product, protection against instant message spyware, pop ups, adware, and the general nasties that wreak havoc on your network. Packet Hawk can also help protect your desktops from problems related to removable media, too.

With prices ranging from $1,495 for up to 100 desktops ($495 per year for updated spyware definitions) up to just under $9,000 for up to 5,000 desktops (plus $2,995 per year for definition updates), the Tangent Packet Hawk is about in line with other products on the market. The company does make available a device that scans more than 5,000 desktops, too. For more information about the Packet Hawk, visit **http://www.packethawk.com**.

## Antivirus vendors

Not to miss out, antivirus software vendors have recently started to jump on the antispyware bandwagon by adding spyware scanning capabilities to their products. This year, major antivirus vendors, including Sophos, Symantec, and McAfee, have updated, or are updating, their products to cope with the spyware threat, which has become a serious security problem for many companies.

If you're already running an enterprise antivirus product, check with your vendor to see what their plans are in the antispyware space. You may be able to save a lot of money by doing so.

## What to look for

Now that you have seen a little of what is available on the market, what should you look for as you try to make the best decision for your organization? Here are a few tips to help you make the best choice:

- **Central administration:** For an enterprise-level product, this is a must as it would be prohibitive to manually install a client on thousands of desktops.
- **Regular updates:** Like a virus scanner, a spyware scanner needs to be updated regularly with new definitions. Whether your clients are updated from a central server on your network or from the vendor's servers, it doesn't matter as long as the clients are kept current.
- **No conflict of interests:** Microsoft made news recently when it was revealed that their antispyware product has lowered the alert status for Claria, a purported adware provider. Whether or not this is fair is still up for debate, but try to choose a solution that is free from these kinds of conflicts of interests, when possible.
- **Antivirus and antispyware in one:** If you already have antivirus software for your enterprise, consider contacting that vendor before you start a search for a separate antispyware solution.

Spyware is just going to get worse as we move forward in the Internet Age, so be prepared! ❖

# Dealing with "spyware residue"

*By Steven Pittsley, CNE*

All the hype surrounding spyware concerns recognizing it when it's installed on a computer and then removing it. But what happens after you remove those invasive programs? Spyware removal programs don't always eliminate every trace of spyware. They usually get the heart and soul of the spyware programs, but slight remnants of the offending application are often left behind. Sometimes, the fragments go unnoticed, but other times, they can cause serious problems. Let's take a look at what you can do to remove traces of spyware that remain on a computer after the removal tool has finished its job.

## Looking for remnants

A good spyware removal tool, such as LavaSoft's AdAware or Spybot Search & Destroy, can take care of most spyware-related files and registry entries. However, spyware removal tools must have a thorough understanding of each application to eliminate everything associated with it. And since spyware authors continually modify their programs to avoid detection, the spyware removal companies may sometimes lag behind in their definition file updates. This is why stray files, registry entries, and other spyware residue may remain on the computer even after the application is removed.

The first thing you can do to locate spyware residue is open Add Or Remove Programs and look for applications you didn't install. If you find any, click the Change Or Remove Programs button and uninstall the program. This sounds like a basic step—and it is—but it's still an effective starting point.

The next step is to open Windows Explorer and look for any strange or unknown files and folders. Sometimes, spyware removal tools will delete the files in a folder but leave the folder on the drive. For instance, if you see a file named GMT in Common Folders, you can probably delete it because it's part of the Gator spyware application. Of course, you should be careful when deleting files and folders to make sure you don't inadvertently remove something that one of your legitimate applications needs. If you're not sure about a particular item, either leave it alone or move it to a different location for a few weeks until you're certain it can be safely deleted.

Finally, look in the Startup folder for applications that don't belong. Many spyware applications put themselves in this folder so they launch when you start the computer. This folder is located in different places depending on the version of Windows that is on the computer. In older versions, the Startup folder is located at C:\Windows\Start Menu\Programs\Startup. In Windows XP, it's located in the user profile at C:\Documents and Settings*userid*\Start Menu\Programs\Startup. Be sure to check the Startup folder in the All Users profile too.

## Taming registry problems

One of the most common areas for spyware remnants to hide is in the system registry. These stray values can cause the computer to run slow, generate system errors, or, in extreme cases, make the system unusable. Eliminating these problems may require you to edit the registry, but be very careful. If you're unsure of whether to remove an entry, leave it alone. Don't remove anything unless you are certain you can do so without harming the system. If you mistakenly delete a registry entry for a critical system function, you can corrupt the registry and make the system unusable. Searching the registry for stray values is difficult, even for experienced technicians.

### Back up the registry

Before you make any registry changes, you should back up the registry. That way, you can restore it if you accidentally remove a critical entry. Use the following steps to create a backup of the system registry:

1. Click Start | Run, type *Regedit*, and press [Enter] to open the Registry Editor.
2. Click File | Export and navigate to the location where you want to save the file.
3. Enter a filename, such as *Backup_Reg*, and click Save.

The current registry will be exported to the location you specified. Note this information in case you need to use the backup file.

### Finding spyware residue in the registry

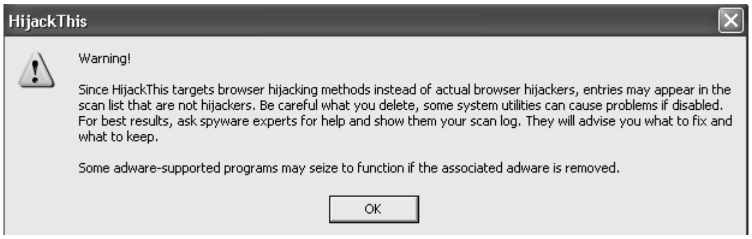
Instead of manually searching through the registry for spyware-related entries, you might consider using a tool such as HijackThis. This program identifies possible spyware entries in the registry. However, it is not a spyware removal tool, and some of the entries it flags may be legitimate. You're ultimately going to make the choice of which entries are deleted. Once again, use extreme caution when doing this. HijackThis is available as a free download. Here's a brief rundown on how to use it.

After you download HijackThis, double-click the icon to launch the program. HijackThis will present the warning message shown in **Figure A**.

When you click OK, the HijackThis main screen displays, as shown in **Figure B**. To begin a registry scan, click the Scan button.

The registry scan takes just a few moments. As **Figure C** shows, the results will be displayed in the HijackThis window. Select any entries that you want to remove and click Fix Checked. Click Yes when the warning message appears. HijackThis will then remove the selected entries.

**Figure A**

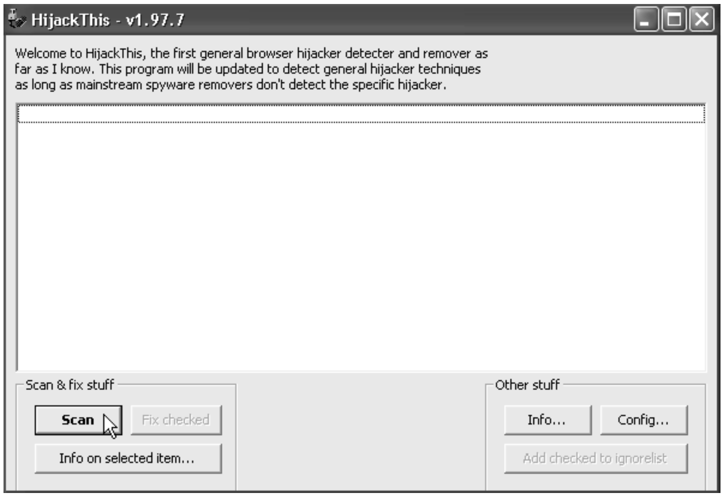


Warning!

Since HijackThis targets browser hijacking methods instead of actual browser hijackers, entries may appear in the scan list that are not hijackers. Be careful what you delete, some system utilities can cause problems if disabled. For best results, ask spyware experts for help and show them your scan log. They will advise you what to fix and what to keep.

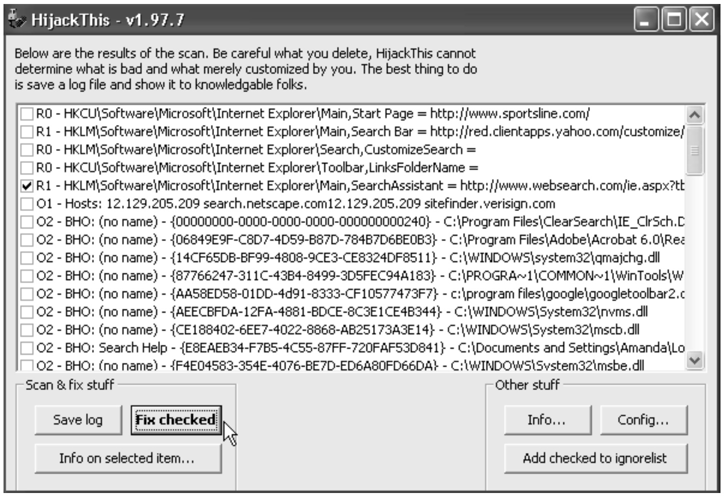
Some adware-supported programs may seize to function if the associated adware is removed.

**Figure B**



Welcome to HijackThis, the first general browser hijacker detecter and remover as far as I know. This program will be updated to detect general hijacker techniques as long as mainstream spyware removers don't detect the specific hijacker.

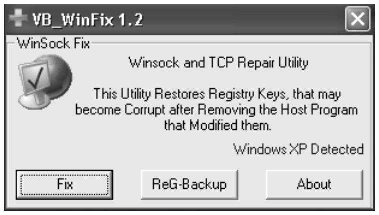
**Figure C**



Below are the results of the scan. Be careful what you delete, HijackThis cannot determine what is bad and what merely customized by you. The best thing to do is save a log file and show it to knowledgable folks.

```
☐ R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.sportsline.com/
☐ R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Bar = http://red.clientapps.yahoo.com/customize/
☐ R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
☐ R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =
☑ R1 - HKLM\Software\Microsoft\Internet Explorer\Main,SearchAssistant = http://www.websearch.com/ie.aspx?tb
☐ O1 - Hosts: 12.129.205.209 search.netscape.com12.129.205.209 sitefinder.verisign.com
☐ O2 - BHO: (no name) - {00000000-0000-0000-0000-000000000240} - C:\Program Files\ClearSearch\IE_ClrSch.D
☐ O2 - BHO: (no name) - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} - C:\Program Files\Adobe\Acrobat 6.0\Rea
☐ O2 - BHO: (no name) - {14CF65DB-BF99-4808-9CE3-CE8324DF8511} - C:\WINDOWS\system32\qmajchg.dll
☐ O2 - BHO: (no name) - {87766247-311C-43B4-8499-3D5FEC94A183} - C:\PROGRA~1\COMMON~1\WinTools\W
☐ O2 - BHO: (no name) - {AA58ED58-01DD-4d91-8333-CF10577473F7} - c:\program files\google\googletoolbar2.c
☐ O2 - BHO: (no name) - {AEECBFDA-12FA-4881-BDCE-8C3E1CE4B344} - C:\WINDOWS\System32\nvms.dll
☐ O2 - BHO: (no name) - {CE188402-6EE7-4022-8868-AB25173A3E14} - C:\WINDOWS\System32\mscb.dll
☐ O2 - BHO: Search Help - {E8EAEB34-F7B5-4C55-87FF-720FAF53D841} - C:\Documents and Settings\Amanda\Lo
☐ O2 - BHO: (no name) - {F4E04583-354E-4076-BE7D-ED6A80FD66DA} - C:\WINDOWS\System32\msbe.dll
```

Figure D

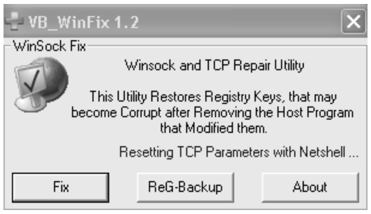


Winsock and TCP Repair Utility

This Utility Restores Registry Keys, that may become Corrupt after Removing the Host Program that Modified them.

Windows XP Detected

Figure E



Winsock and TCP Repair Utility

This Utility Restores Registry Keys, that may become Corrupt after Removing the Host Program that Modified them.

Resetting TCP Parameters with Netshell ...

## Restoring Winsock and TCP/IP settings

Another troublesome problem that can occur after running a spyware removal program involves the computer's network configuration. The TCP/IP settings on the computer are controlled by the Winsock.dll file. Spyware removal tools can sometimes delete registry entries or values in Winsock that are used for network connectivity. One indication of this problem is that when you try to view a Web page and receive a Page Cannot Be Displayed error, you can still ping the Web site.

In pre-XP versions of Windows, you could reinstall the TCP/IP protocol to resolve this problem. However, in Windows XP, TCP/IP is a core component of the operating system. There are, however, tools that will help you restore the TCP/IP protocol to the state it was in when you first installed Windows XP. One of these tools is WinSock XP Fix, which you can download free from Spychecker.com. Let's look at how it works.

After downloading WinSock XP Fix, double-click the executable file. When the utility launches, you'll see the main window shown in **Figure D**.

The first thing you should do is create a backup of the registry. You can either follow the procedure described earlier or use the ReG-Backup feature in WinSock XP Fix. The next step is to restore the corrupted registry keys. Click the Fix button and then click Yes to apply the WinSock XP Fix settings.

WinSock XP Fix will restore the file and fix the network configuration. The progress will be displayed in the main program window, as shown in **Figure E**.

Once WinSock XP Fix has finished restoring the registry settings, click OK to reboot. The network configuration should then work normally again.

## Wrap-up

Spyware applications can slow down a computer, use disk space, and, when removed, may leave behind remnants that can disable certain system functions, such as the network configuration. Programs like HijackThis and WinSock XP Fix help make locating these remnants and removing them a much easier process. ❖

# Take back control after Internet Explorer is hijacked

*By Brien M. Posey, MCSE*

My father-in-law—a computer novice—recently telephoned me for help changing his Internet Explorer home page. After I walked him through the usual technique, he explained that a Windows Permission Error was preventing him from making the change. I asked him a few more questions and soon realized that, at some point in the past, a pornographic Web site had hijacked his IE. Every time he opened IE, the browser went straight to this pornographic site. Worse yet, the modification prevented him from changing the home page.

A three-hour battle ensued during which we tackled some serious registry edits and a malicious group policy. Eventually we were able to return control of IE to my father-in-law and remove the offending application. Here's how we did it.

## One size doesn't fit all

It's a sad truth that malicious individuals can hijack a Web browser in a variety of ways. And since there is no standard hijacking technique, there is no standard repair technique. If your browser is hijacked, a significant chance exists that the repairs that worked for my father-in-law will not work for you. I will therefore cover several repair techniques.

## Begin with a thorough scan

When faced with an IE hijacking, you should first scan the computer for viruses, Trojans, adware, and spyware. It's highly likely that one of these items is the hijacker. Until you ensure that your computer is free from these parasites, you'll only be treating the symptoms rather than the actual problem.

Unfortunately, I have yet to discover a single program that effectively scans for every potential form of spyware, adware, virus, and Trojan. I therefore recommend using several different programs. I know it's time consuming to download all these utilities and perform a separate full-system scan with each, but this is a critical step in the troubleshooting process.

Scan for viruses first. My antivirus program of choice is ViRobot Expert from Hauri. Although Hauri is a relative unknown in the United States, it has been a leading antivirus program in Asia for many years. ViRobot Expert will completely repair the damage from many viruses that Norton and McAfee will only quarantine or delete. In fact, my father-in-law was running McAfee—with the latest updates. I asked him to uninstall McAfee and install the free trial version of ViRobot Expert. ViRobot Expert instantly caught four viruses that McAfee had missed. Another reason I recommend using ViRobot for this particular problem is that ViRobot Expert not only scans for viruses, but also scans for common hacker tools.

Now that the system is virus free, it's time to scan for adware with a utility such as PestPatrol (which also removes spyware) or my personal favorite, which is Ad-aware from Lavasoft. After you have scanned for adware, I recommend scanning the system for spyware with a spyware removal tool, such as SpyBot-Search & Destroy from PepiMK Software or, my favorite, BPS SpyWare/Adware Remover from Bullet Proof Soft.

After you have scanned the system for virus, adware, and spyware, reboot and try to change IE's home page. If you're still unable to do so, then it's likely the hijacker has modified the Windows registry or configured a malicious group policy.

### BEFORE WE BEGIN

Warning: The following section involves editing your system registry. Using the Windows Registry Editor incorrectly can cause serious problems requiring the reinstallation of your operating system and may lead to the loss of data. TechRepublic does not and will not support problems that arise from editing your registry. Use the Registry Editor and the following directions at your own risk.

## Clean the registry

When a program hijacks IE by modifying the registry on a Windows NT/2000/XP system, the change often impacts only the current user. This is because many users don't have local administrative privileges and can only modify the HKEY_CURRENT_USER portion of the registry, not the HKEY_LOCAL_MACHINE portion. If the user has local administrative privileges or the machine is running Windows 9x/Me (which won't protect the registry), the change could be applied to all of the users on the system, depending on hijacker's level of sophistication.

With this in mind, log on as the person who's having the problem and open the Registry Editor. Then, navigate through the registry tree to:

```
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\
    Control Panel
```

Check for the existence of keys named ResetWebSettings or HomePage. If such keys exist, delete them. Next, navigate to:

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
```

Verify that the information stored in the Default_Page_URL key and Start Page key is correct. If these keys contain values that reflect an undesirable startup page, double-click on the key to open its dialog box and then replace the existing value with an appropriate one.

There are two more registry entries you should check, but you'll need to ensure you have the proper permissions before doing so. As I mentioned before, if you're using Windows 9x/Me, any user can modify the registry, but if you're using Windows NT/2000/XP you'll need local administrative privileges.

Navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main
```

As before, check the Default_Page_URL and the Start Page keys for inappropriate values and change the values if necessary. Next, navigate to:

```
HKEY_USERS\Default\Software\Microsoft\Internet Explorer\Main
```

Once again, check the Default_Page_URL and the Start Page keys for inappropriate values, and change them as necessary.

## Check for malicious policies

Another method IE hijackers can use to prevent you from fixing their handiwork is to change the system's policies. Normally, you shouldn't have to worry about this with Windows NT, 2000, or XP. With those systems, I've never heard of a browser hijacking that involved a modification of a group policy. If you're running Windows 9x/Me, however, it's very possible that an unauthorized policy may have been placed on your system.

To determine if this is the case, search the hard drive for files with a POL extension. If such files exist, they may or may not be malicious. I recommend booting the system into MS-DOS mode and renaming the policy file with an extension of PCY instead of POL. This will disable the policy without deleting it.

Now, boot Windows normally and play around to see what effect, if any, disabling the policy has. If you're suddenly able to edit IE's home page, then it's probably safe to assume that the policy was malicious and didn't belong on the system. If this is the case, go ahead and delete the policy file.

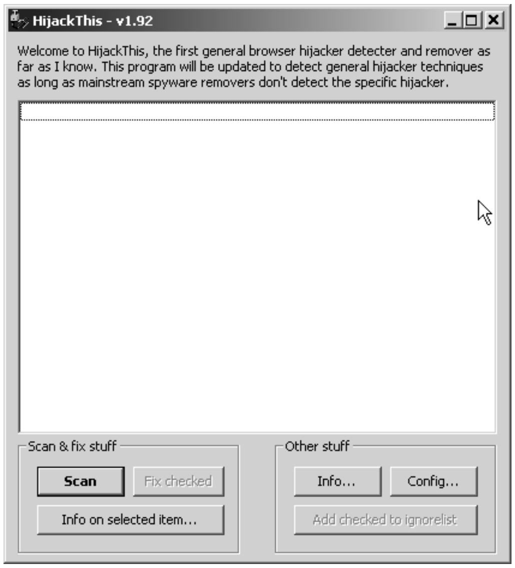
On the other hand, if you're still unable to edit IE's home page and unable to perform some normal tasks, the policy is probably legitimate and you should reenable it. You can do this by booting the system into MS-DOS mode again and renaming the policy file so that it once again has the POL extension.

## Hijack This!

By now, you're probably wondering which technique I used to fix my father-in-law's problem. I used a really cool freeware utility called HijackThis, shown in **Figure A**, which you can download at **http://www.spywareinfo.com/~merijn/index.html**. This utility scans the Windows registry and hard drive for IE settings that have been modified. If modifications are found, each modification is listed, and you may then choose which modifications to keep and which to remove.

Once HijackThis is open, click the Scan button to start a new scan. Once the scan is complete, a list of modifications will be displayed, as shown in **Figure B**.

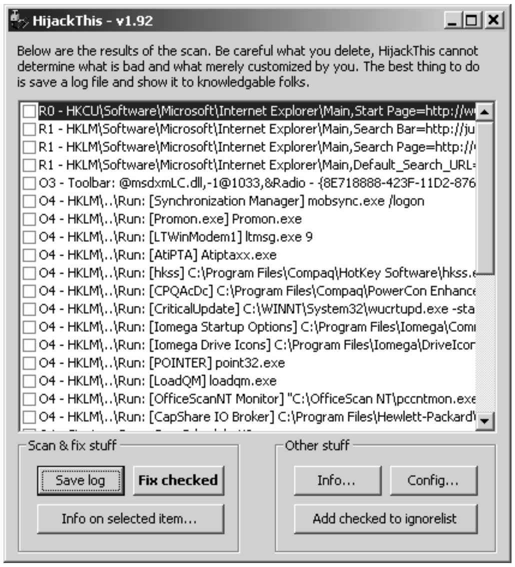
**Figure A**



Welcome to HijackThis, the first general browser hijacker detecter and remover as far as I know. This program will be updated to detect general hijacker techniques as long as mainstream spyware removers don't detect the specific hijacker.

Here is the HijackThis main window before a scan has been run.

**Figure B**

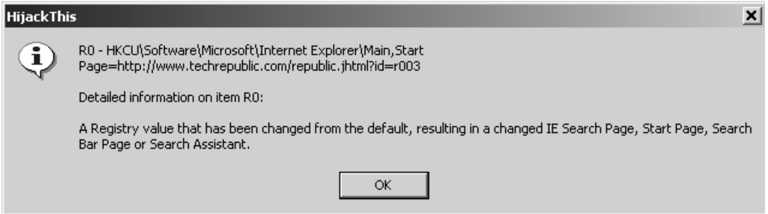


Below are the results of the scan. Be careful what you delete, HijackThis cannot determine what is bad and what merely customized by you. The best thing to do is save a log file and show it to knowledgable folks.

```
□ R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page=http://w
□ R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Bar=http://ju
□ R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page=http://
□ R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL=
□ O3 - Toolbar: @msdxmLC.dll,-1@1033,&Radio - {8E718888-423F-11D2-876
□ O4 - HKLM\..\Run: [Synchronization Manager] mobsync.exe /logon
□ O4 - HKLM\..\Run: [Promon.exe] Promon.exe
□ O4 - HKLM\..\Run: [LTWinModem1] ltmsg.exe 9
□ O4 - HKLM\..\Run: [AtiPTA] Atiptaxx.exe
□ O4 - HKLM\..\Run: [hkss] C:\Program Files\Compaq\HotKey Software\hkss.e
□ O4 - HKLM\..\Run: [CPQAcDc] C:\Program Files\Compaq\PowerCon Enhance
□ O4 - HKLM\..\Run: [CriticalUpdate] C:\WINNT\System32\wucrtupd.exe -sta
□ O4 - HKLM\..\Run: [Iomega Startup Options] C:\Program Files\Iomega\Com
□ O4 - HKLM\..\Run: [Iomega Drive Icons] C:\Program Files\Iomega\DriveIcor
□ O4 - HKLM\..\Run: [POINTER] point32.exe
□ O4 - HKLM\..\Run: [LoadQM] loadqm.exe
□ O4 - HKLM\..\Run: [OfficeScanNT Monitor] "C:\OfficeScan NT\pccntmon.exe
□ O4 - HKLM\..\Run: [CapShare IO Broker] C:\Program Files\Hewlett-Packard\
```

Here are the HijackThis scan results.

**Figure C**



R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page=http://www.techrepublic.com/republic.jhtml?id=r003

Detailed information on item R0:

A Registry value that has been changed from the default, resulting in a changed IE Search Page, Start Page, Search Bar Page or Search Assistant.

This entry shows the current IE start page.

When the scan is complete, you can select the suspicious entries and click the Fix Checked button to remove them or highlight each entry individually and click the Info On Selected Item button to learn more about each one, as shown in **Figure C**.

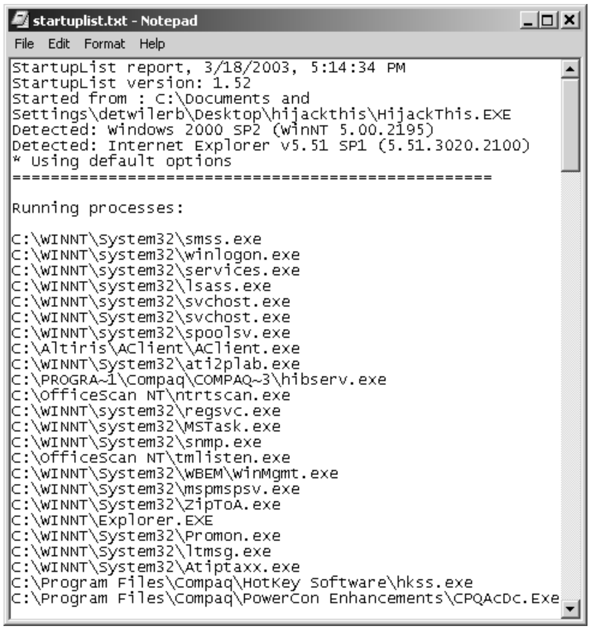
I found using HijackThis to be extremely effective, but it's not for the novice. I strongly recommend backing up your Windows installation before running HijackThis because it's easy to accidentally damage Internet Explorer. For example, ViRobot Expert, the antivirus product I mentioned earlier, integrates itself into Internet Explorer and Outlook. If you had ViRobot Expert installed and then used HijackThis to remove all IE modifications, you would be removing ViRobot Expert's IE component, thus weakening your security.

### StartupList: Another handy HijackThis tool

Integrated into HijackThis, StartupList generates a list of every application that starts automatically when Windows boots. This list is more in-depth than the one provided by Msconfig, but doesn't provide a GUI or a means to control whether programs start or not.

To run StartupList, click the Config button from the HijackThis main window. Then click the Misc Tools button. Click the Generate StartupList log button, then click Yes. The list is saved as a text file with the name, startuplist.txt, in the directory where HijackThis is located. HijackThis automatically opens the text file with Notepad, as shown in **Figure D**.

**Figure D**



```
StartupList report, 3/18/2003, 5:14:34 PM
StartupList version: 1.52
Started from : C:\Documents and
Settings\detwilerb\Desktop\hijackthis\HijackThis.EXE
Detected: Windows 2000 SP2 (WinNT 5.00.2195)
Detected: Internet Explorer v5.51 SP1 (5.51.3020.2100)
* Using default options
==================================================

Running processes:

C:\WINNT\System32\smss.exe
C:\WINNT\system32\winlogon.exe
C:\WINNT\system32\services.exe
C:\WINNT\system32\lsass.exe
C:\WINNT\system32\svchost.exe
C:\WINNT\System32\svchost.exe
C:\WINNT\system32\spoolsv.exe
C:\Altiris\AClient\AClient.exe
C:\WINNT\System32\ati2plab.exe
C:\PROGRA~1\Compaq\COMPAQ~3\hibserv.exe
C:\OfficeScan NT\ntrtscan.exe
C:\WINNT\system32\regsvc.exe
C:\WINNT\system32\MSTask.exe
C:\WINNT\System32\snmp.exe
C:\OfficeScan NT\tmlisten.exe
C:\WINNT\System32\WBEM\WinMgmt.exe
C:\WINNT\System32\mspmspsv.exe
C:\WINNT\System32\ZipToA.exe
C:\WINNT\Explorer.EXE
C:\WINNT\System32\Promon.exe
C:\WINNT\System32\ltmsg.exe
C:\WINNT\System32\Atiptaxx.exe
C:\Program Files\Compaq\HotKey Software\hkss.exe
C:\Program Files\Compaq\PowerCon Enhancements\CPQAcDc.Exe
```

StartupList displays the applications that are automatically started when Windows boots.

## Preventing reinfection

If all goes well, by now you've been able to reclaim your Web browser. If not, you may have to reinstall Windows. Simply reinstalling Internet Explorer or upgrading it to a newer version doesn't usually get rid of the problem (believe me, I've tried). Once you do get Internet Explorer back under your control, there are several basic steps that you can take toward preventing this problem from occurring in the future.

If you're using an always-on connection, such as through a DSL or cable modem, use a good personal firewall. Use reputable antivirus software and keep it current. Do not run, save, or download programs that you don't trust.

Regularly delete all temporary Internet files and cookies from your browser's cache. It's possible that IE cached the malicious code, so you'll want to make certain that it's gone for good from your system. Make sure that you have all of the latest security patches in place, especially for Windows, IE, and Outlook.

Still another way to prevent the problem from happening again is to use a freeware utility called Browser Hijack Blaster. This program constantly monitors Internet Explorer for modifications. If a modification is attempted, Browser Hijack Blaster alerts you to the impending modification and asks if you want to allow it or prevent it from happening. Browser Hijack Blaster is compatible with Windows 9x/Me/NT/2000/XP. ❖

# Recover from an Internet Explorer hijacking with these tips

*By Brien M. Posey, MCSE*

In the Technical Q&A, I found an interesting post from member Sfath. "I have a client that every time he opens IE, it defaults to a porn site," Sfath wrote. To troubleshoot this problem our troubled tech has already tried deleting all temp files, downloaded program files, and mysterious links. Sfath has also tried editing the registry to no avail. "When the page opens it continually generates different porn pages and basically locks up the computer," Sfath wrote. "It also removes Norton AntiVirus." Let's examine what could be causing Sfath's problems.

Assuming that Sfath has already checked IE's home page setting, the problem Sfath describes is often related to either hidden software that's manipulating Internet Explorer or a registry entry. Let's review some of the advice other members and myself offer on troubleshooting both potential problems.

## The usual suspects

If hidden software is the culprit, the machine is most likely infected with a virus, Trojan, spyware, or adware. I don't want to waste space getting into a discussion of the differences between these mechanisms, but I will say that I have seen malicious Web sites use all four, and sometimes combinations of the four, to push their Web content onto your system. The scary thing is that depending on which mechanisms are being used, the infected computer could be transmitting sensitive, personal information to the owner of the porn site.

I recommend starting with a full virus scan using a quality antivirus product such as Norton AntiVirus, McAfee VirusScan, Trend Micro's OfficeScan, Grisoft Inc's AVG AntiVirus, or my current favorite, ViRobot from Hauri. ViRobot will remove viruses, Trojans, spyware, and some adware. A good freeware utility for removing adware recommended by TechRepublic members Soulrider and DKlippert is Ad-aware from Lavasoft. TheChas, who also believes spyware may be the culprit, recommends Sfath check out Start Page Guard from Piotr J. Walczak. Member Cglrcng suggests that Sfath "also check the connections tab in Internet

### WORD OF WARNING

The following section explains techniques for editing your system registry. Using the Windows Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system and could cause you to lose data. TechRepublic does not and will not support problems that arise from editing your registry. Use the Registry Editor and the following directions at your own risk.

Options for an 'XXX Auto Dialer,' remove the connection if present or he [Sfath's client] could be in for a real shock when the telephone bill arrives."

## Check the registry

If the problem persists after scanning for malicious code or hidden software, the Windows registry should be your next target. Initially, I recommend navigating through the registry to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft. Look at the Internet Account Manager\Import folder and its subkeys. The existing subkeys will differ from machine to machine. Normally, they will link to various Internet components, such as IE, Eudora, and Netscape. Look for and delete anything suspicious.

Next, check out the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Account Manager\Preconfigured key. Again, what exists will differ from machine to machine. Some of the more common (and harmless) subkeys are Active Directory GC, Bigfoot, Verisign, and WhoWhere. Look for anything suspicious and delete it. You can identify a suspicious entry because beneath the subkey you'll find a link to a malicious Web site in the LDAP URL key.

Then, check the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Domains key. In a default Windows XP installation, there will be an entry for Hotmail.com, but nothing else. Delete anything that links to a potentially malicious Web site.

Finally, go to a healthy machine that's running the same operating system and the same version of Internet Explorer (including service packs). Navigate to the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer registry key. Right-click on the key and select the Export command from the shortcut menu. This will export the various Internet Explorer registry entries to a text file. Copy this text file to the infected machine, open the Registry Editor, and navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer. At this point, select the Import command from the Registry Editor's File menu. Follow the prompts to import your text file. This will reset all of the Internet Explorer related registry entries, and should return Internet Explorer to working order.

## Reinstall Internet Explorer

The tips I've listed should solve Sfath's problem. If they don't, it could be that the malicious software has overwritten a DLL file somewhere in the system. In such a case, reinstalling IE will probably be the only hope. Check out Microsoft Knowledge Base article 318378 for information on reinstalling IE (**http://support.microsoft.com/default.aspx?scid=kb;en-us;318378**). ❖

# Notes:

# 3 Anti-Spyware Tools

# Combine and conquer using anti-spyware tools

*By Steven Pittsley, CNE*

Anti-spyware applications vary in terms of features and functionality, and some are better than others at rooting out spyware. Instead of putting all of your eggs in one basket, it may be better to leverage the strength of several programs in your fight against spyware.

In this article, you'll learn about some of the more prominent anti-spyware products on the market today. Since there isn't one all-inclusive anti-spyware program that handles every type of spyware threat, it's a good idea to learn about the strengths of each application so that you can take advantage of the features you need to handle your particular spyware challenges.

## Comparison criteria

Many anti-spyware tools are on the market today. We chose five of the more comprehensive packages currently available to see how they stack up:

- Ad-Aware
- CounterSpy
- PestPatrol
- Spybot S&D
- Spy Sweeper

All of these applications have similar feature sets and do an excellent job of detecting and removing spyware. Any of these programs would be a good choice. However, none of them can detect and protect you from all forms of spyware, and each offers something that one or more of the other packages don't. So using at least two anti-spyware packages will build a better defense around your network than using one product by itself.

**Table A** offers a side-by-side comparison of the five anti-spyware packages based on 14 criteria.

## Lavasoft's Ad-Aware

The most popular product in the anti-spyware fight is currently Lavasoft's Ad-Aware. This application protects computers from various forms of spyware, including parasites, selected Trojan horse programs, dialers, malware, and tracking components. Although Ad-Aware does a good job against most spyware, it can't detect spyware in RAM, recognize when spyware is attempting to install itself, or detect key loggers. Despite these omissions, Ad-Aware is still a solid product. It has

**Table A:** ***Anti-spyware tool of comparision***

| | Ad-Aware | CounterSpy | PestPatrol | Spybot S&D | Spy Sweeper |
|---|---|---|---|---|---|
| Detection of spyware running in RAM | | x | x | x | x |
| Detection of unwanted home page changes | x | x | x | | x |
| Scanning open Internet ports | | | | x | |
| Scanning the system startup settings for spyware | x | x | x | x | x |
| Detection of tracking cookies | x | x | x | x | x |
| Detection of key logger programs | | x | x | x | x |
| Detection of attempted spyware installation | | x | | | x |
| Detection of spyware-related registry entries | | x | x | x | x |
| Removal of spyware programs during system startup | x | x | | x | x |
| A detailed report of the system scan | x | x | x | x | x |
| The option to roll back changes made by the anti-spyware application | x | x | x | | x |
| The ability to update spyware definition files | x | x | x | x | x |
| Length of updates provided with the purchase of the program | 1 year | 1 year | 1 year | Forever | 1 year |
| Cost | Personal use is free; corporate use is $39.95 | $19.95 | $39.95 for the first year; $19.95 yearly renewal | Donation | $29.95 |

an easy-to-use interface and performs system scans quickly. Not only does Ad-Aware do a good job of protecting your computer, but it's also free for personal use. Ad-Aware Professional is available for $39.95 for corporate use.

## Sunbelt Software's CounterSpy

The newest member to join the anti-spyware game is Sunbelt Software's CounterSpy. Aiming to become a major player in the battle against spyware, CounterSpy offers a full range of defenses and advanced features, such as the ability to detect spyware that's in memory, to remove programs during system startup, to detect key logging programs, and to recognize when spyware programs are attempting to install themselves. CounterSpy appears to be a solid product with an above-average feature set. It has a friendly interface, a comprehensive list of defenses, and excellent technical support. Its $19.95 price tag is the lowest of all the non-freeware products we reviewed.

## Computer Associates' PestPatrol

PestPatrol is a comprehensive anti-spyware tool that can detect active spyware running in RAM and locate spyware during system startup. The functional interface and above-average frequency of definition file updates make this program a good choice for any anti-spyware campaign. The only weaknesses in the application are its inability to detect spyware during system startup and to identify spyware when it attempts to install itself. Backed by the vast resources available at Computer Associates, PestPatrol appears poised to become a major player in the anti-spyware game. However, the $39.95 price tag is a bit steep considering some of the shortcomings.

## PepiMK Software's Spybot Search & Destroy

PepiMK Software's Spybot S&D was an early entry in the anti-spyware market and is one of the most widely used anti-spyware programs. Offering a full variety of anti-spyware features, Spybot S&D can handle just about everything except browser hijackers, spyware installation detection, and application removal during startup. Its most unusual feature is the ability to scan open ports for spyware-related activity. This is a valuable function if you believe your computer is sending personal information back to the spyware companies. Among the products we reviewed, only Spybot S&D supported port scanning.

Like Ad-Aware, Spybot S&D is a free utility that includes unlimited updates. In default mode, Spybot can easily be used by the average computer user. However, only more experienced users will be able to take advantage of Spybot's advanced features, such as the more sophisticated reporting options and automatic scanning.

The feature set and price tag make Spybot S&D an attractive choice for any anti-spyware arsenal, especially as a second tool to supplement another application's limitations.

## Webroot's Spy Sweeper

Webroot's Spy Sweeper is a popular anti-spyware product. This feature-rich package boasts every type of anti-spyware function, except port scanning. The simple interface and powerful features make Spy Sweeper a good addition to your anti-spyware lineup. The $29.95 price tag is moderate, although CounterSpy offers similar features for $10 less.

## Wrap-up

Used individually, the anti-spyware tools featured in this article will provide an excellent defense against all current forms of spyware applications. However, using two or more packages in conjunction will increase your power to root out even the most invasive forms of spyware. ❖

# Introducing CounterSpy Enterprise

*By Steven Pittsley, CNE*

Sunbelt Software's CounterSpy Enterprise product is designed to help administrators combat spyware that threatens the corporate network. Although this is only the first version of the product, CounterSpy's ease of management and powerful features make it a strong candidate for you to consider as you design your spyware defenses. You can obtain a preview edition of the product by visiting the Sunbelt Software site at **http://www.sunbelt-software.com/product.cfm?id=400**. Here's a look at what the product offers.

## CounterSpy components

CounterSpy consists of three components:

- The **Admin Console** provides a broad range of configuration and management options, which we'll discuss in depth in the next section.
- The **Server Module** contains the workstation database, spyware definition database for download to the Agents, and other management-related data. The Server Module communicates with the Admin Console and the Agents using short XML bursts. This HTTP traffic, which utilizes SOAP, can pass through firewalls that are configured to allow such traffic.
- The **Agent** software is installed on each network workstation. After installation, the program scans for spyware that is resident in memory, in the system registry, or on the computer's hard disk. The Agent can be configured to display a System Tray icon, or it can be hidden from the user's view.

## Centralized management

CounterSpy Enterprise was developed independently from Sunbelt Software's CounterSpy personal edition. As a result, CounterSpy Enterprise contains an extremely well-conceived centralized management scheme. The CounterSpy Enterprise Management Console lets you perform a multitude of tasks. For instance, you can:

- Install the CounterSpy client Agent on workstations located throughout the enterprise network. You can deploy CounterSpy using a silent push. Because the client Agent is available as an MSI file (in addition to being available as an .exe file), you can also deploy CounterSpy by using the user's login script, SMS, or an Active Directory Group Policy, or by allowing the user to install the application from a Web page.
- Schedule spyware scans on individual workstations, several computers, or all of the computers on the network. You can scan for threats by using the Scan Now button or by scheduling either a quick or deep scan.

- Configure e-mail alerts that notify designated people when spyware is detected on a client workstation.
- Set the security level for various categories of spyware. For example, certain types of spyware, such as malware, constitute an immediate threat. CounterSpy lets you determine what action to take against a category of spyware.
- Automatically deploy new spyware definition files to Agent workstations.
- Create a variety of reports. Crystal Reports is bundled with CounterSpy, providing you with a full array of reporting options. You can select from the seven preconfigured reports or create your own.
- Remove items that are quarantined on workstations. In fact, the items can be removed only by the centralized admin. Although this might appear to be an administrative headache, the configuration options in CounterSpy allow you to control what types of spyware are quarantined. This reduces the amount of quarantined programs to a manageable number.
- Roll back items that were quarantined on just one machine, an entire policy, or the entire network. There is no rollback option for deleted items.

Using these powerful features, you can customize CounterSpy to meet your organizational requirements. CounterSpy doesn't scan for spyware when someone logs on to a PC, and it can't repair Winsock DLL files, but it does offer a wide assortment of configuration options that should meet most administrators' needs.

## CounterSpy requirements

The CounterSpy Admin Console and Server Module components have the following hardware and software requirements:

- A 1Ghz P3 or higher
- At least 512 MB of RAM
- 150 MB of free disk space
- MDAC 2.6 or greater, as required by the server
- One of the following operating systems:
  - Windows Server 2003
  - Windows XP Professional
  - Windows 2000 Server with Service Pack 3
  - Windows 2000 Professional with Service Pack 2
  - Microsoft .NET Framework 1.1 or higher

The CounterSpy Agent has the following hardware and software requirements:

- A Pentium 200 workstation
- At least 20 MB of free disk space
- One of the following operating systems:
  - Windows XP Professional or Home edition
  - Windows 2000 Professional with Service Pack 2

**Table A:** ***Anti-spyware tool comparison***

| Description | Price |
|---|---|
| Small Business Network Kit: 10 machines<br>Includes the Management Console | $255.00 |
| Small Business Network Kit: 15 machines<br>Includes the Management Console | $359.00 |
| Small Business Network Kit: 25 machines<br>Includes the Management Console | $559.00 |
| 30 - 99 machines (priced per license) | $20.00 |
| 100 - 199 machines (priced per license) | $18.00 |
| 200 - 499 machines (priced per license) | $16.00 |
| 500 - 999 machines (priced per license) | $13.00 |
| 1,000 - 1,999 machines (priced per license) | $11.00 |
| 2,000 - 3,499 machines (priced per license) | $9.00 |
| 3,500 - 4,999 machines (priced per license) | $8.00 |
| 5,000 - 9,999 machines (priced per license) | $7.00 |
| 10,000 - 19,999 machines (priced per license) | $6.00 |
| 20,000 - 50,000 machines (priced per machine) | $5.00 |

- Windows NT 4.0 Workstation Service Pack 6
- Windows 98
- Window 98 Second Edition
- Windows Me

CounterSpy requires all servers and workstations to have Internet Explorer version 5 or later installed.

## CounterSpy pricing

**Table A** summarizes Sunbelt Software's comprehensive pricing scheme for CounterSpy. Spyware definition file updates are free for one year, which is standard for the industry.

## Wrap-up

Although CounterSpy Enterprise is a brand-new product, it appears to be feature-rich and well written, and it does an excellent job of removing spyware from client workstations. CounterSpy Enterprise is a competitive product that should be considered for all corporate spyware defense plans. ❖

# Configuring and administering CounterSpy Enterprise

*By Steven Pittsley, CNE*

CounterSpy Enterprise is a recent entrant in the battle against spyware. It provides a solid defense of your corporate network with powerful tools such as policy-based group management, remote agent installation, and scheduled scanning. Let's take a look at some of the features and configuration options CounterSpy Enterprise includes.

## Configuring database updates

Updating the spyware definition files is among the most important tasks you'll perform in the fight against spyware. You can deploy the client agent to every machine on the network, configure stringent policies, and perform spyware scans twice a day, but none of this will defend against a brand-new spyware application. The only way to prevent a new strain of spyware from invading your network is to regularly update the spyware definition database. The CounterSpy Enterprise interface makes the update process easy.

Managing the frequency of client and database updates is one of CounterSpy's system configuration options. To work with these settings, expand the System list and click Updates.

The Updates screen lets you specify how often CounterSpy should check for new updates to the client Agents and to the spyware definition, or threat, database. Because your defenses are only as good as the software you've deployed, you should consider checking for updates every two or three hours. The inquiries and subsequent downloads are relatively small and shouldn't put a strain on your network. Even if you elect to check for updates less frequently, you should, at a minimum, check for threat database updates at least twice per day.

The System Configuration screen contains optional settings for configuring how CounterSpy Enterprise communicates with Sunbelt Software to obtain updates. This screen consists of two sections.

The Proxy Server Settings section allows you to configure the Address and Port settings to use when communicating with Sunbelt Software. The Email Server Settings section provides various e-mail configuration options that CounterSpy will use to notify you about spyware/adware that is detected on your network.

## Working with policies

The strength of any centrally managed product is the ability for administrators to easily configure and manage clients. CounterSpy Enterprise excels in this regard by simplifying configuration of group policies for maximum control and flexibility.

The CounterSpy Enterprise Admin Console provides an easy-to-use policy configuration interface. The Policies folder expands to list all of the group policies that have been created. To work with a policy configuration, simply highlight the policy to display the available options.

The toolbar at the top of the screen lets you force a scan on a single machine or all of the machines assigned to the policy. You can also manage the machines in the policy using the Add, Remove, and Reassign buttons.

The middle portion of the policy configuration screen lists all the machines assigned to the policy. The Last Scan column provides the date and time each machine was last scanned for spyware. The Defs Version and Agent Version columns display the client version that's installed on each workstation. Occasionally reviewing this information can help you make sure each machine is being scanned regularly with the latest agent software and spyware definition database information.

The Schedule tab provides a variety of options for both a quick scan and a deep scan of the machines assigned to this policy. You can enable either or both types of scans. You can also schedule the start time, days of the week, and run frequency of the scan. The CounterSpy client Agent runs as a background process that doesn't affect workstation performance. You should consider running a quick scan at least once per day and a deep scan once a week. If the workstations have heavy Internet use, you should consider scheduling more frequent scans.

The policy configuration window also allows you to configure what gets scanned during a quick or deep scan. You can select from these options:

- Scan Known Locations
- Scan Cookies
- Scan Memory And Running Processes
- Thorough Scan

You should probably select all of these options for the deep scan, and possibly select Scan Known Locations and Scan Memory And Running Processes for the quick scan. The selections you make should be based on the amount of Internet use the machines encounter. For heavy use, you might consider selecting all of the options for both types of scans or possibly selecting Thorough Scan during a quick scan.

The CounterSpy threat database contains all the known spyware that the software looks for when it scans a workstation. However, just because a program is listed in this database doesn't mean that it isn't legitimate software. For example, the DameWare remote control tool could potentially be used for spyware-type purposes. That doesn't mean that it shouldn't be installed—it's a popular and useful tool for network administrators. In this case, you wouldn't want CounterSpy to remove the program from certain machines when it performs the system scan.

The Allowed Threats tab lets you allow certain programs to be installed on the workstations that are assigned to the policy. This prevents CounterSpy from removing them. It also enables you to customize the policy for the person who is using the workstation. For example, you'd want only network administrators to have the DameWare remote control tool. The Allowed Threats tab gives you the flexibility of allowing certain users to have the program, while preventing others from installing it.

The Notifications tab allows you to specify who is notified of certain types of warnings generated by CounterSpy. For example, you could configure CounterSpy to notify you of all the threats found during a system scan or just the very critical ones. These notifications provide you with information about the threats that were found on the network.

The Agent tab provides several options for configuring the CounterSpy Agent software on the client workstations. You can display the CounterSpy taskbar icon and elect to update the threats database or Agent software whenever updates are available. You can also manually force an update of the threats database or Agent software for all workstations assigned to the policy, and you can change the reboot message per policy.

The Action tab enables you to specify the type of action taken for certain types of spyware. For example, you could elect to quarantine programs deemed to be adware or delete spyware considered to be an AOL Exploit. Generally speaking, the default settings are appropriate for most environments. However, each network and environment is different, so you may need to fine-tune the actions to meet the needs of your organization.

## Management tasks

CounterSpy provides many configuration options that allow you to manage agents, quarantined threats, and all spyware-related threats. These features give you even more centralized control over how spyware is handled on the network workstations.

The Agents screen, under Management in the CounterSpy interface, provides information about the Agents that are deployed on the network. You can check the status of the Agent software, determine when the last scan was performed, and verify the threat database and Agent version. In addition, you can assign a policy to the Agent. Although you can handle these tasks in other places within the CounterSpy application, it's much easier to view all of the Agents in one location, rather than having to view them within each policy.

The Quarantine and Threats management options are similar. The Quarantine screen provides information about spyware that was found by client Agents. The Threats screen provides a list of all the threats in the database. You can use this information to determine the name of the program, the organization that produced the application, and the threat level of the spyware.

## Wrap-up

The easy-to-use interface and powerful tools available in CounterSpy Enterprise make it an appealing choice for spyware defense. The centralized management features simplify the job of configuring and managing client Agents, updating the threat database, and leveraging other CounterSpy Enterprise options for effective protection and flexibility.

Most enterprise anti-spyware tools on the market were adapted from standalone products rather than designed specifically for an enterprise situation. CounterSpy Enterprise benefits from being designed from the ground up as an enterprise tool. It's one of the more comprehensive anti-spyware programs available and should provide a solid defense against spyware for virtually any size organization. ❖

# Survive and recover from malware with Spybot and Ad-aware

*By Mark Kaelin*

According to the *Webopedia*, malware is defined as "a noun, short for malicious software; software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse."

According to *Wikipedia*, malware (a contraction of "malicious software") is software developed for the purpose of doing harm.

The key words in those definitions are damage, disrupt, and harm. Malware is an example of the worst the Internet and World Wide Web can offer. Detecting, destroying, and removing spyware has been the subject of many TechRepublic articles, but the plague remains.

## Now, it's personal

Once upon a time, I blew off any concerns about malware as a problem for the novice users of the world who didn't follow the most basic rules of security—don't open attachments and don't agree to install unsolicited software from Web sites. My blissful ignorance was shattered on July 20, 2004, when I became a victim of a malware hijacking.

The fact that I could be hijacked by merely clicking a link on a Google search page seems, even now, to be the surreal reality of someone else. How could such a thing be allowed to happen?

The whole concept of malware is lost on me. Are we supposed to believe that hijacking someone's system to install unasked for and unwanted software is somehow going to induce that victim to become enamored with the products that are featured in the subsequent force-fed advertising? Does that ever really happen? I don't believe it.

It is much more likely that the person violated in this unwelcome scenario will have a reaction much more like mine, in which one is motivated to stop this from happening to anyone else ever again. I defy any malware purveyor to jump in the article discussion and justify malware as a good business practice. And I don't mean the usual rationalization that it makes them money. I'm talking about justifying it ethically. I say there is no justification—prove me wrong!

## Removal

Fortunately for all of us, the combination of malware, spam, and spyware has caught the attention of more than just a few inspired and talented individuals and application developers. Over the past few years, TechRepublic has written several articles describing how to remove spyware and malware from infected systems.

Many of those articles have mentioned the remarkable cleansing power you can bring to bear with the combination of Spybot Search & Destroy and Ad-aware. In my case, those two were extremely effective in removing the infestation.

For those TechRepublic members looking for a refresher on the general implementation of these applications, here is how the combination worked for me.

### Firefox to the rescue

First, I borrowed a utility CD-ROM from a colleague. The utility CD had a copy of the latest version of Mozilla Firefox, which I quickly installed. Because most of the malware was tuned to the start of Microsoft Internet Explorer, I was able to access Download.com using Firefox—a normally simple thing made nearly impossible by the vindictive software I was trying to remove.

From Download.com, I acquired the latest versions of Spybot Search & Destroy and Ad-aware 6.0, which I quickly installed on the infected system. The initial Spybot routine found 79 questionable objects. After removing those offensive tidbits, I updated the reference file for Spybot and ran it again. This updated cleansing operation found another 25 objects to remove.

So far so good—but I still had problems with pop-up advertisements and frustratingly slow Web browsing, so I knew that I had not eliminated the entire infection. Like heeding your doctor's warning about taking the entire series of an antibiotic treatment, I needed to continue to fight the infection by running Ad-aware 6.0 with an up-to-date reference file, which netted an additional 171 objects. While most were innocuous advertising trackers, several were nasty bits of code and registry key combinations that begged to be destroyed.

Running the latest versions of Spybot and Ad-aware, including the latest reference files available, completely removed the offending malware and gave control of my computer back to me. The key to this success was the use of a Web browser other than Internet Explorer. That's when I began to ponder the larger meaning of this unpleasant experience.

## Recovery kit

Trying to find a silver lining in this incident, I decided I should create a recovery kit and burn it on a CD-ROM. On this CD are the installation files for Firefox, Spybot Search & Destroy, Ad-aware 6.0, and a copy of the AVG Anti-Virus software. These applications would have been good enough to fix my problems, but I'm wondering if there should be more applications saved to this disk. For example, I'm thinking perhaps I should make the CD bootable for those occasions when I need to at least get to a command prompt.

In the past, many of us tech-types have created recovery disks—first it was 5.25-inch floppies with DOS and command-line utilities, then 3.5-inch diskettes with perhaps an antivirus application, and now it is CD-ROMs or thumb drives with the capacity for all kinds of applications.

## Legislation and regulation

When I started to research how I came to have this little misadventure, I came across the Web site of U.S. Representative Jay Inslee and noted his efforts to pass the Computer Software Privacy and Control Act, H.R. 4255. My immediate response is to support any legislation that will criminalize the hijacking of computer systems and the unapproved installation of unsolicited software. However, the cynical part of me also wants to make sure the legislation is properly written and does not place an extraordinary burden on Web sites.

That may seem paranoid to some, but when Orrin Hatch is trying to ramrod legislation (**http://news.com.com/Senator+wants+to+ban+P2P+networks/2100-1027_3-5280384.html**) through the U.S. Congress that would make it illegal to participate in a P2P network, I think some paranoia is justified.

Another excellent source of information is the United States Computer Emergency Readiness Team (US-CERT), which contains a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported. To underscore the seriousness of the problems caused by malware, it is interesting to note that the US-CERT is governed by the Department of Homeland Security's National Cyber Security Division (NCSD) and the National Strategy to Secure Cyberspace.

If you or your users suffer the misfortune of a malware hijacking, I encourage you to notify the US-CERT about the offending Web site. However, the unfortunate reality of the current situation is that the offending Web site itself is probably a victim of a hijacking, and the Webmasters are likely unaware of the infection they are spreading. This trickery means that most malware pushers are escaping the long-arm of the law—at least for now.

## The future is now

The prevalence of malware is a problem that we must address. And by "we," I mean IT professionals. The current situation, where a user's system can be compromised simply by visiting a Web site, is intolerable. Network administrators, Webmasters, system designers, application developers, and the numerous other IT professionals responsible for Internet security and infrastructure should tackle this malware problem head on and now.

Perhaps it is time to make Spybot and Ad-aware, or similar applications, an integral part of normal network security. Of course, that would mean that we would have to pay for these tools, which are now generally free to use. But I think that small bit of investment is well worth the cost, especially when you consider the time spent trying to remove malware.

Perhaps your company has already adopted a network policy on those applications. Help your colleagues here at TechRepublic establish their own policy by explaining how your policy regarding malware-prevention software is working. What problems have you had to overcome, and what benefits have you derived from this policy?

## Technology is key

Malware is more than a nuisance; it is an epidemic that costs us all time and resources. While criminalizing the hijacking of PCs and browsers will prevent some of this activity, we cannot count on that legislation to actually become law. Instead, it will ultimately be technology itself that will find a way to prevent this insidious behavior. But until the technology of prevention catches up to the technology of infliction, we will have to pay a price for access to the World Wide Web. It's a shame that that price is constantly being raised by the darker side of human nature and the scourge of malware. ❖

# Protect against spyware and adware with Spybot

*By Jim McIntyre*

By simply visiting a Web site or installing shareware, you may be installing software, cookies, or applications that are able to monitor and log your Internet activity. This category of software is generally referred to as *spyware*. *Adware* is normally associated with shareware that generates pop-up ads or displays banner ads.

Spybot is a freeware tool to detect and remove spyware and adware from your system, and it performs this job remarkably well. Here's how you can install and configure Spybot to protect your privacy.

## Installing Spybot

Spybot is donation-ware from Spybot S&D. That means you don't have to pay for it, but the organization does take donations to support future development. You can obtain the latest version of Spybot from the Spybot Web site. Download the installation file, currently Spybotsd12.exe, to a temporary directory on your hard drive, and you're ready to go.

To install Spybot, double-click on the self-extracting archive and follow the prompts in the Setup Wizard. Spybot installs like every other Windows program you've ever used, with no confusing prompts or gotchas during the wizard. Once the installation is complete, you're ready to start running Spybot.

## Running Spybot

To start Spybot, double-click on the desktop icon. The first action to take when Spybot runs is to check for updates by clicking the Search For Updates button. This will ensure that the spyware signatures used by Spybot and the program itself are up to date. If there are any updates, click the Download Updates button and let them download and install.

The default for Spybot is to run in Easy Mode. In this mode, Spybot searches for problems using a predefined configuration. Easy Mode is a good way to run Spybot if you want to run a quick check for cookies and other items that can identify you and report your Internet activity to a third party. Running Spybot in Advanced Mode, however, provides more configuration options. To run Spybot in Advanced Mode, use the following procedure:

1. Right-click the desktop icon for Spybot.
2. In the menu, click on Properties.

3. Change the executable target from:
   C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe /easymode
   to:
   C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe
4. Double-click the icon to run Spybot in Advanced Mode.

### Main settings

All configuration changes are made through the menus contained in the Settings tab: On this tab, you'll see several options that allow you to adjust Spybot to suit your preferences. Here are the main options you'll want to take note of:

- **Save All Settings:** This allows Spybot to be used with the same configuration for every scan.
- **Create Backups Of Fixed Spyware Problems:** Some programs associated with Spyware will not function after the spyware component is removed. If you must use a program with a spyware component, the ability to recover the spyware will eliminate the need to reinstall the entire program.
- **Create Backups Of Removed Usage Tracks:** Creating a backup of usage trackers allows you to view these trackers and examine which Web sites are trying to monitor your activity.
- **Create Backups Of Fixed System Internals:** Any registry inconsistencies fixed by Spybot may cause problems for your system. Using this option allows the registry to be restored to the state it was in before the Spybot scan.
- **Ignore If Single Detections In Include Files Need A New Program Version:** Activate this option.
- **Display Confirmation Changes Before Doing Critical Changes:** Using this option will ensure you are aware that changes are about to be made; you'll be prompted for confirmation.
- **Scan Priority:** Most users will use normal scan priority.

### Automation settings

Spybot has the ability to run whenever the system is booted and to detect and fix any problems automatically. Enable the following settings under the Automation section of the Settings tab:

- Run Check On Program Start
- Fix All Programs On Program Start
- Rerun Checks After Fixing Problems
- Immunize On Program If Program Has Been Updated
- Search The Web For New Versions At Each Program Start

- Download Updated Included Files If Available Online
- Expert Settings

The Expert Settings menu activates the Secure Shredder to run automatically when Spybot removes files. Because the Secure Shredder permanently deletes removed files, this tool should not be used automatically.

### Selecting file sets

To make it easier to select file sets, go to the Settings tab. Under the Expert Settings menu, enable the following settings:

- Show Expert Buttons In Results List
- Show Expert Buttons In Recovery List

These settings activate a drop-down list in the Search & Destroy screen. This list contains an easy-to-understand description of the types of scans available.

### The Directories tab

The Directories tab is used to specify where downloaded files are stored. Spybot will scan this directory whenever a check is run. The software in the specified directory will be scanned to see if any spyware or Trojans will be installed with the downloaded software.

To add a directory to the list, right-click in the blank under the Download Directory heading and select Add A Directory To This List. Browse for the folder you want to add to the list. At the bottom of the screen, select the Check Also Subdirectories Of The Above check box. Repeat the procedure for any additional folders you want checked by Spybot.

## Running a Spybot scan

After configuring Spybot with the options you want, the next step is to run the scan of your system. Click on the Spybot-S&D tab and click Search And Destroy. Next, click on the File Sets button and select the type of scan to run. For this example, a Minimal Spyware Check was run. Click Check For Problems.

When the scan is complete, Spybot will display the results. Problems are divided into three categories. Red entries indicate spyware. Spyware problems are always selected to be fixed by Spybot. Green entries indicate usage trackers. You probably won’t cause any problems by removing these from your system. Black entries are system internals. Make sure you know exactly what areas of your system will be affected before removing any of these entries.

Spybot automatically selects spyware problems to be fixed, so the next step is to click on the Fix Selected Problems button. If there are any problems that cannot be fixed because a program is in use, Spybot will attempt to correct the program automatically the next time the system is rebooted, before the spyware program is started.

Now, click on the File Sets button and select Usage Tracks Check Only for the next scan. Click on Check For Problems, and Spybot will run a check for Internet usage trackers. To remove individual trackers from your system, click on the check box next to the tracker in the results, and then click on the Fix Selected Problems button. Spybot will remove the selected trackers from your system. To remove all usage trackers, click Select All Items and then click on Fix Selected Problems.

The same procedure applies when Spybot runs a check on your system internals. This check is looking for registry inconsistencies, broken desktop links, and bad paths to executables. When a check on system internals is run, make sure you understand the output. Removing reported registry problems, and other entries related to system performance, can cause problems for your system.

## Other Spybot tools

The Tools menu controls several tools associated with Internet Explorer and services run at startup. One of the programs you'll notice here is the Resident tool, a continuously running security program. Presently, the Resident tool section provides a browser application for Internet Explorer that prevents downloads of known malicious software, such as spyware installers. To activate the Resident tool program, click on the Install button at the top of the screen.

The Active X menu displays a list of Active X controls currently installed on your system. Active X controls are categorized by color. Green entries are legitimate Active X controls. Red entries mark controls related to spyware. Black entries are not known to the Spybot database.

The BHOs tab displays information about Browser Helper Objects (BHOs). BHOs are small programs—often Active X controls—that extend Internet Explorer's capabilities. Because they are integrated with your browser, BHOs have access to each Web site you visit. Green entries are legitimate BHOs; red entries are associated with spyware; black entries are unknown to Spybot.

If you have any concerns about a BHO in this list, you can easily disable it. Click on the BHO to be disabled. At the top of the BHO window, click on the toggle button. Disabled BHOs will then appear grayed out in the BHO list.

On the Browser Pages tab, Spybot also provides protection against browser-hijacking agents that can reset the start or search page in Internet Explorer. If your browser start page or search page is changed and cannot be reset through IE, the new URL will probably show up in this list.

To reset the offending URL and ensure the URL is added to the next Spybot update, click on the URL your browser has been redirected to. At the top of the screen, click on the Change button and enter the new URL. Mail the offending address to detections@spybot.info, and the URL will be added to the list of known bad URLs.

Spybotcomes with its own hosts file, which contains an extensive list of Web sites known for spyware; you can view this list on the Hosts File tab. When this file is installed, no content from any of the sites in it will be displayed. To install the Spybot hosts file, click on the Hosts File tab.

At the top of the Hosts File screen, click on Add Spybot-S&D Hosts List. The Spybot hosts file will now be used instead of your default hosts file. To remove the Spybot hosts file, click on Remove Spybot-S&D Hosts List.

**AUTHOR'S NOTE**

Using the Spybot hosts file can cause decreased performance. Read the FAQ included with Spybot to correct these problems for your version of Windows.

The Process List tab displays all processes running on your system. Although any process may be killed (stopped) through this tab, it is intended primarily as information for technical support. To kill a process in this list, select the process and click on the Kill button at the top of the window.

## System Startup

The System Startup menu lists all programs that are started when Windows is launched. This menu allows the user to change the path to a Startup program or change the command used to execute the program. You can also delete any program from Startup or insert a program to be started with Windows.

To view any item in the System Startup list, select the item and click on the Info button at the top of the System Startup screen. To disable a program run at startup or to allow a disabled program in this list to start with Windows, select the program and click on the Toggle button at the top of the screen. To change the path to a program run at startup or to change the command options run with the program, select the program from the System Startup list and click on the Change button at the top of the screen.

One good feature of this menu is that it gives you the ability to add and configure new startup programs. To add a new program to the Startup list, click on the Insert button at the top of the screen. Make the program available to All Users On Startup or only to the Present User. Select how the program will be run. There are three selections available:

- Run The Program As A Normal Program
- Run The Program As A Service
- Create An Autostart Group Link

Provide a name for the registry entry and select the path to the executable file. A new entry with the value you enter will be added to the list of programs run at system startup.

## View Report

The View Report menu is used to generate a report of your system configuration, including the configuration used for Spybot. The results from a Spybot scan can also be included with this report.

## Using Spybot Immunization

The Spybot Immunization function is controlled through the Spybot-S&D tab. It provides four very useful functions:

- Permanently immunizing Internet Explorer from spyware
- Preventing Internet Explorer from downloading known spyware installers
- Preventing spyware from making changes to Internet Explorer configuration
- Locking the hosts file

To provide immunity for your browser and hosts file, click on the Immunize icon under the Spybot-S&D tab. In the first configuration panel, titled Permanent Internet Explorer Immunity, click on the Immunize button to immunize Internet Explorer. The next panel is labeled Percent Running Bad Download Blocker For Internet Explorer. In the drop-down list, select Block All Bad Pages Silently. Click on Install.

In the third panel, Recommended Miscellaneous Protections, click in each of the three check boxes available to lock the hosts file and to prevent spyware from reconfiguring Internet Explorer when immunization is activated. Spybot blocks all entries that are in its database.

## Stop spyware in its tracks

The growth of spyware, adware, and other methods of tracking and reporting your Internet habits makes privacy and security more of a problem than most Internet users are aware. Spybot is a great tool to start using if you're concerned about your privacy. In this article, I covered the basics of using Spybot to remove software that can intrude on your privacy and affect your system performance. Spybot should be one of the first programs you install on any computer connected to the Internet. ❖

# Knock out Network Essentials adware with PestPatrol

*By James Detwiler*

Pop-ups, spyware, and adware are the banes of Internet browsers. Why can't surfing the Web be more like watching TV? At least you know when someone's trying to sell you something then; there's a clear line between program and advertisement. Also, TV commercials don't just appear out of thin air and hijack the upper half of your TV screen. And they don't install renegade programs on your set without permission. Why should the Internet be any different? TechRepublic member Grey_Woolf would definitely like to know.

This member turned to the Technical Q&A seeking advice on how to uninstall a mysterious program named NE. The app started loading itself automatically whenever Internet Explorer 5.5 was started. In Grey_Woolf's words, "This app causes pop-ups... Also, I have noticed the unit gradually slows down."

In an attempt to fix the problem, Grey searched the registry and System.ini for any occurrences of NE. His hunt turned up absolutely nothing. What did TechRepublic members have to say about the nefarious NE?

"Pop-ups, spam, and spyware—and all the other nasty names they all go by—that we do not want on our computers are not always as easy to find just by searching our registries. They are in the registry most likely, but usually under a different name, or nonobvious name," said Paul (a.k.a. XpertDragon). He asked, "Have you already downloaded Ad-aware? It is shaping up to be like the program of the year I think, and it is free...it works well, and will remove most, if not all, unwanted junk off of your PC." He also suggests investing in a good pop-up stopper like AdSubtract Pro.

Ashnaidu offered this advice: "[To prevent pop-ups] you can disable active scripting in Internet Explorer. You might not want to use this method, because it prevents other scripts from running which might cause many Web sites to be displayed incorrectly."

Disable active scripting by changing the Security settings under Internet Options in the IE Tools menu. Paul saw this solution as a bit too drastic, not wishing to "cut my nose off to spite my face."

BeerMonster pointed Paul in the direction of the PestPatrol Web site where a full explanation of the application NE is given. The program Network Essentials appears to be a pop-up loader that gathers information on browsing habits. This gathered data is then used to generate pop-up advertisements based on targeted key words. The adware installs three files on your machine: NE.EXE, NE.DAT, and NE.DLL. Distributed by SmartPops, the application is installed by the Trojan DownloadWare and can be removed by using Add/Remove Programs. PestPatrol suggests first removing DownloadWare from the machine before Network Essentials in order to prevent an unauthorized reinstallation. Further instructions on removing the files from the system registry are also given.

Hitting the mark perfectly, BeerMonster received many kudos from Paul, whose future Web browsing will hopefully be pop-up free. With many thanks, Paul proclaimed, “Excellent! [BeerMonster] You are the man!” ❖

# Stop spyware with Microsoft's AntiSpyware Beta

*By Luke Swagger*

Poll just about any IT professional and ask them what their biggest headache is, and the answer will be the same: spyware. Viruses and hackers can do damage, but spyware is much more widespread, and even thought it's not deadly, it can slow down users and be annoying. Many companies have tried to solve this problem, and now Microsoft has put its foot down too. Here's a look at Microsoft AntiSpyware and how it can help reduce the threat of spyware in your organization.

## A beta? Who cares?!

We don't often talk about Beta software as being used in a production environment. Microsoft has worked pretty hard in making AntiSpyware solid, and it has some compelling features that make it worth a look even as a beta.

First, you can configure Microsoft AntiSpyware to automatically update itself. Other popular anti-spyware applications like Spybot and AdAware require you to manually update them before they run. This is important because much like antivirus software, if your anti-spyware signatures are out of date, your software is useless.

Second, Microsoft AntiSpyware will scan for spyware activity on a real-time basis. Most anti-spyware software requires you start them and run them to find spyware. If you don't scan often enough, your computer can become infected and cause damage until you remove the spyware. Microsoft AntiSpyware takes a page from virus scanners and runs in the background, looking for spyware activity. When it detects something fishy, it will display a warning box in the lower left-hand corner of your screen.

Microsoft AntiSpyware runs on Windows 2000 Professional computers or later, including Windows XP and Windows Server 2003. If you're still running Windows 9x, you're out of luck.

## Obtaining Microsoft AntiSpyware

You can obtain Microsoft AntiSpyware by downloading it directly from Microsoft's Web site (**http://www.microsoft.com/downloads/details.aspx?FamilyId=321CD7A2-6A57-4C57-A8BD-DBF62EDA9671&displaylang=en**). Microsoft AntiSpyware is offered as part of the Genuine Windows program, which means that before you can download it, you must first validate that your copy of Windows XP is genuine. You do that by clicking the Continue button next to the Validation Required title on the Web page.

### AUTHOR'S NOTE

Microsoft created the Genuine Windows Program in an effort to encourage people not to pirate Windows. By offering Microsoft AntiSpyware for free, as well as other programs and updates, Microsoft hopes to bypass the sharing of Windows XP and security keys over the Internet. Windows Product Activation (WPA) was supposed to stop Windows piracy, but it hasn't completely.

You then must download and run an ActiveX Control from Microsoft that checks to make sure you have a legitimate copy of Windows before allowing you to

download the program. Once your copy has been validated, you can download Microsoft AntiSpyware freely. It's only 6.5Mb, so it won't take too long to download.

## Installing and configuring Microsoft AntiSpyware

To install Microsoft AntiSpyware, run AntiSpywareInstall.exe. This will begin the Installation Wizard. This wizard runs like just about every other Windows installation you've ever done. You can just accept all of the defaults. At the end of the Wizard select Launch Microsoft AntiSpyware.

When Microsoft AntiSpyware starts, you'll see the Microsoft AntiSpyware Setup Assistant appear. Here you'll configure Microsoft AntiSpyware before you can use it.

Start by downloading the available updates. Remember, unless you keep Microsoft AntiSpyware updated, it won't be effective. It may actually be worse than running no anti-spyware software at all, because outdated software lulls you into a false sense of security. To that end, as part of downloading updates during this step, you should make sure you enable the AutoUpdater.

Next, you can enable Microsoft AntiSpyware's Real-Time Security Agent protection. This will protect your computer as it runs, but be aware that it can also impact system performance. If you have a workstation with low resources, you may not want to enable real-time security. Select Yes and click Next.

You're then asked if you want to join the SpyNet Community. This is supposed to inform other computers in the network when spyware has been encountered. Microsoft encourages you to do so, but it's purely optional.

The last step of the configuration is to run a scan. Click Run Quick Scan Now. You'll want to do this to remove any spyware that's already on your system.

## Running Microsoft AntiSpyware

Microsoft AntiSpyware runs very similarly to an anti-virus program, scanning memory first, then programs on your hard drive and the system registry.

When the scan completes, you'll see how many pieces of spyware the program has found and how long it took to find it. When you close this screen you can then treat the spyware that's been found.

For each piece of spyware found, you have four choices:

1. **Ignore:** Ignore the scan results for this scan and take no action.
2. **Quarantine:** Move the spyware to a safe place but don't delete it.
3. **Remove:** Remove the spyware from your system.
4. **Always Ignore:** Ignore the scan results and don't report this item as spyware in the future.

Select the choice from the dropdown list box and click Continue. If you use System Restore, you can create a Restore Point by selecting the Create Restore Point checkbox. Doing so may help you recover in case you accidentally remove something important. After Microsoft AntiSpyware finishes, your system should be spyware-free. ❖

# Stopping spyware with Trend Micro Anti-Spyware Enterprise Edition 3.0

*By Scott Lowe, MCSE*

Recently, Trend Micro released a new version of their antispyware product, which includes a powerful Web-based administration console, automatic client deployment, frequent updates, and real-time protection from spyware.

In this article, I will go over the installation and configuration for this product on both the server and a client. I will also demonstrate how Trend Micro's automatic deployment works and will show you how to manually install the client on problem or non-domain machines you want to protect.

## System requirements

As you would expect from an enterprise-level spyware product, Trend Micro Anti-Spyware Enterprise Edition 3.0 has multiple components, including a server component and a desktop client. The server side of the equation is managed via a Web console, and the desktop portion can be installed either automatically, if you have the right privileges, or by using an MSI file.

Your servers and workstations should meet some minimum specifications to use this product. While the workstation's specifications remain constant, server requirements may change depending on how many workstations you plan to support.

### Workstation

The basic thing to keep in mind with Trend Micro's enterprise antispyware solution is "older operating systems need not apply." By this point, though, if you're still running Windows 95, 98, or ME in your organization, you're getting used to hearing this, so Trend Micro's choice not to support these operating systems is really not a surprise. Here's a list of what Trend Micro *does* support:

- Windows 2003 Standard, Enterprise, and Web with no service pack, or with SP1
- Windows XP Home and Professional with no service pack, or with SP1 or SP2
- Windows 2000 Professional, Server and Advanced Server with SP3 or SP4

As for system requirements, Trend Micro doesn't require a whole lot and asks only that your system have at least 128MB of RAM and 10MB of available disk space.

If you want to be able to install the software without using an MSI file, your workstation should be a member of your corporate domain, or you should know the local administrator password for each client. Further, if the client is running Windows XP Service Pack 2, you must either disable the internal firewall or configure it so it does not block the ports required by Trend Micro Anti-Spyware.

Specifically, allow these ports:

- 137
- 138
- 139
- 445 (NetBIOS)
- 8088 (Apache management)
- 54447
- 54448
- 54449

If you don't want to allow these firewall exceptions, you will need to use the MSI file and manually install (or deploy using your typical method) the client software. If you use client firewall software that requires you to provide a list of allowed executables, make sure to allow cwshredder.dll, imclntinst.exe, ssengine.dll, tmasca.exe, and tmasea.exe.

### Server

The server requirements are significantly heftier than the workstation list, and change depending on how many clients you plan to support. First, make sure the server you select is not currently running MySQL, since Trend Micro will install this software for its own use. Trend Micro also recommends the following minimal requirements for your server:

- Processor: 2.4GHz for up to 12,500 clients; dual 3GHz for up to 25,000; and Quad 3.4GHz for up to 60,000 clients
- RAM: 512MB for up to 12,500 clients; 1GB for up to 25,000; and 2GB for up to 60,000 clients
- Disk space: 5GB
- A static IP address
- Windows 2003 Standard or Enterprise
- Windows 2000 Server or Advanced Server with SP4
- If you plan to use IIS, make sure to install the IIS components, or the IIS role, depending on your version of Windows. You can also choose to use the Apache Web server, if you like. I'm using IIS in my examples.
- Internet Explorer 5.5 or better (to access the management console; if you prefer not to do this from the server, you can access the management console from a workstation)
- Sun Microsystems' Java Virtual Machine (for viewing reports)

If you need to allow specific access to certain applications on a software-based server firewall, make sure that the executables tmassa.exe and reminst.exe are allowed. They support the automatic client installation. If you use the MSI installer, you don't need to worry about this.

## Server installation

Before beginning your server installation, make sure it meets the requirements noted above. Next, from whatever location that is appropriate (either an installation CD or an expanded ZIP file), execute the TMAS-EE.exe file to begin the installation of the product.

I'll take you step-by-step through a typical installation that uses IIS as the Web server.

The first screen is a typical software license screen. You should read the contents to make sure there are no surprises. When you're done, click the I Accept button to move on.

The next couple of screens ask you for registration information gathered when you either purchased or registered the product. If you have not registered your product, you need to. At the end of the registration process, you will be provided an activation code, required to complete the installation. Click the Register Online button if you have not yet registered. If you have, just click Next.

If you completed the registration portion of the installer, you should have the activation code requested on this next step. You can either type the code manually, or copy and paste it from your browser window. Click Next when you're done.

The third screen of the installation asks you to provide, and to verify, your e-mail address.

Now, you're getting to real product installation options. First, decide to what location you would like to install the antispyware product. The default location is C:\Program Files\Trend Micro\Antispyware. Click the Browse button to choose a different location. Once you've chosen, click the Next button.

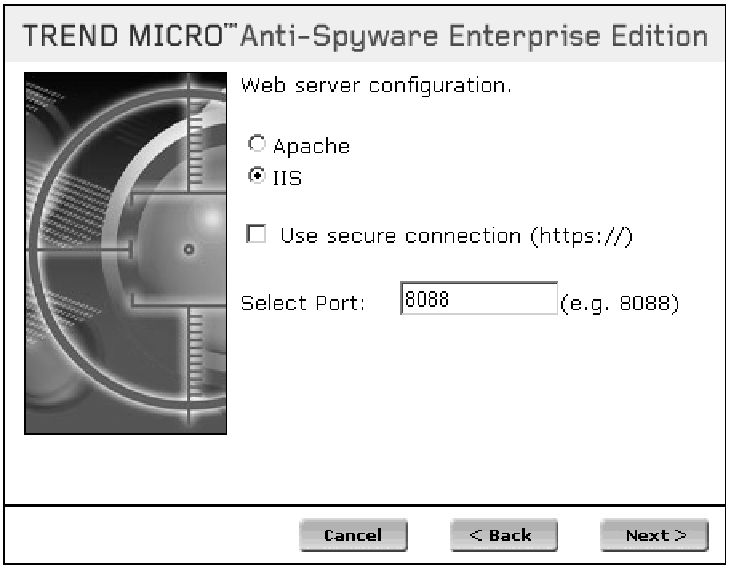
Next, provide a domain account that you will use to administer the client software process. I've created an account using Active Directory Users and Computer named 'tmadmin' and added it to the Domain Administrators group for this purpose. Click the Next button when you're done.

Likewise, you need to specify an account to use to access the Web console on the server. Check the box next to Use Domain Administrator Settings From Previous Screen if you want to use the same account you previously specified. Otherwise, uncheck this box and provide appropriate credentials. Click Next when you're done.

The Web administration portion of the installation is important since you'll use it for all administrative activity. On this next screen, you need to decide which Web server—IIS or Apache—you want to use, and on which port it will run. You can also indicate that you want a secure connection using an SSL certificate, by selecting the Use Secure Connection option.

For this installation, I'm using IIS. If you opt for Apache, version 2.0 of Apache shipped with Trend Micro's product. In **Figure A**, I've shown you the

**Figure A**



TREND MICRO™ Anti-Spyware Enterprise Edition

Web server configuration.

○ Apache
● IIS

□ Use secure connection (https://)

Select Port: 8088 (e.g. 8088)

Choose your web server and port, and decide if you want SSL enabled.

Web server configuration. Note that, when you start Internet Services Manager now, you'll see an AntiSpyware site. The installer adds and configures it automatically. The default port for administration is 8088, and I have maintained this default in this example.

Next, you can optionally choose to install the Control Manager Agent, which is useful for larger installations. I will not be going over the Control Manager in this article, but will be using the Web-based administration console.

Once you make these selections, the software installer completes the installation and configuration of the product, after which you are provided with a summary screen on which you can opt to launch the Web console.

## Administration

With the server-side installation completed, you can move on to administering the product and getting it deployed to workstations in your organization. During this part, I will go over both the automatic and manual installation of the antispyware product onto your client computers.

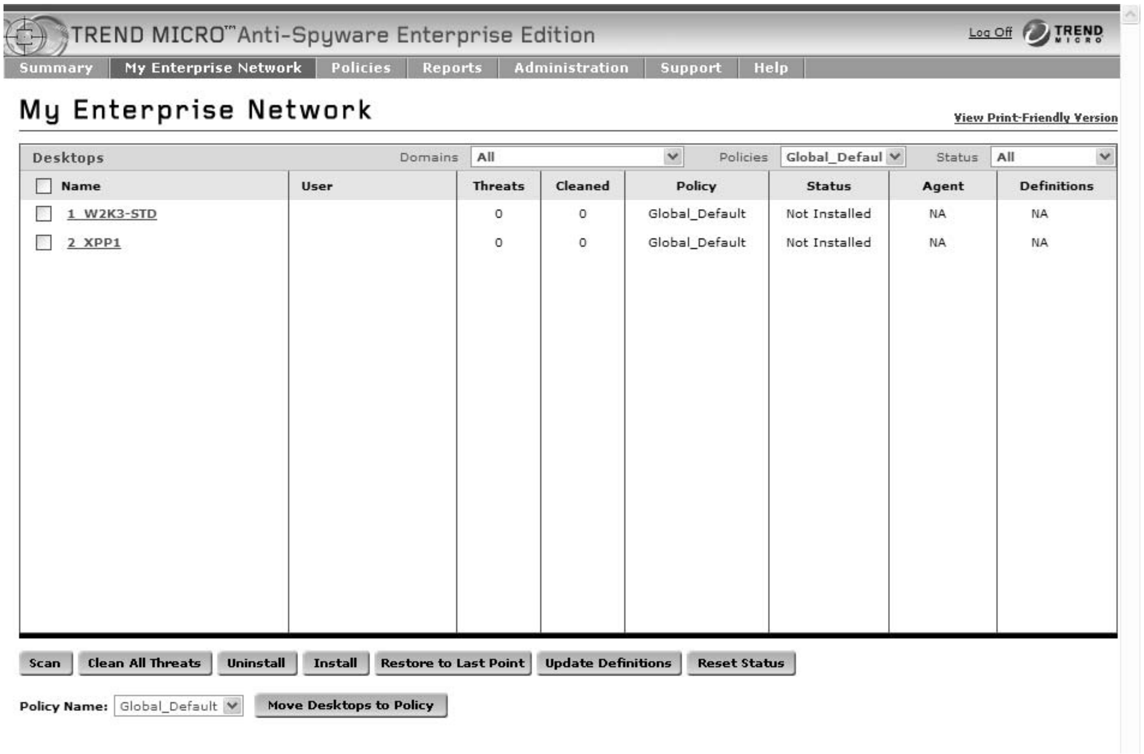
The first step is to log into the Web administrator using either the account you created during the installation or any domain administrator account.

There is really only one step you're required to take in the administration tool before you get started. That is to identify which domain, or domains, you will be administering with this tool. Keep in mind that, if you administer multiple domains, you should add your administrative account to the Enterprise Admins group instead. To add a domain to Trend Micro Antispyware, select it in the Discovered Domains column and click the Add button, placing it into Active Domains. In this example, I've moved the domain named 'example' to this area.

Now, click on the My Enterprise Network tab at the top of the screen. Clicking on this tab brings up a list of machines that have been discovered in your managed domain. Note in **Figure B** that my server has discovered two clients with a status of "not installed," meaning that the client software has not yet been deployed. One of these machines, W2K3-STD, is my Trend Micro Antispyware server, while the other, XPP1, is a Windows XP desktop machine.

In order to demonstrate both installation methods, I will automatically deploy the client software to the Windows Server machine and install the client from the MSI file on the XP machine. Both methods are discussed later in this article.

**Figure B**



Domains: All · Policies: Global_Defaul · Status: All

| ☐ Name | User | Threats | Cleaned | Policy | Status | Agent | Definitions |
|---|---|---|---|---|---|---|---|
| ☐ 1 W2K3-STD | | 0 | 0 | Global_Default | Not Installed | NA | NA |
| ☐ 2 XPP1 | | 0 | 0 | Global_Default | Not Installed | NA | NA |

Policy Name: Global_Default

You can get at-a-glance facts from the My Enterprise Network tab.

## Policies

You can create multiple policies that allow the antispyware software to work differently on different machines in your organization. For example, if you choose to run a daily scan of each machine a la antivirus software, you can create different schedules for different work shifts.

Trend Micro Antispyware comes with a default policy that enables a quick machine scan every night at 11:00 P.M., along with a startup scan. Other options, including automatic product and definition updates, are not enabled. Trend Micro's Active Application Monitoring, a process that proactively prevents spyware from infecting your system, is also disabled by default.

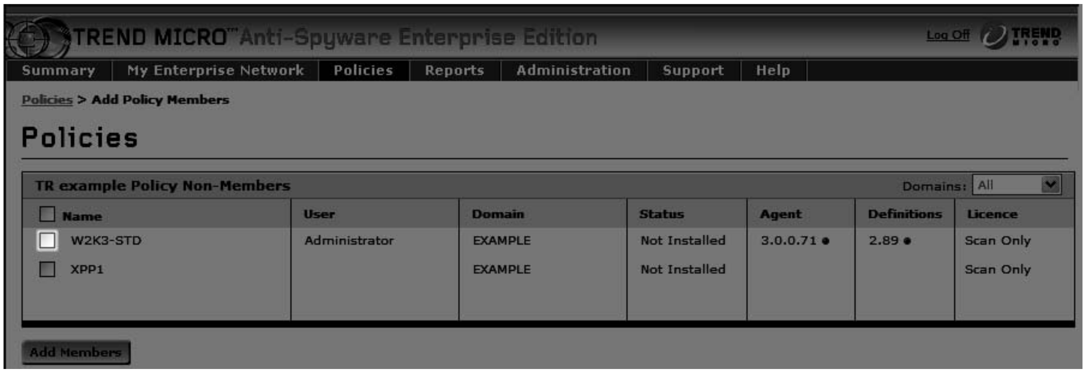
For this article, I'm going to create a new, stricter policy. To create a new policy, click the Policies option at the top of the administration screen and click the New Policy button at the bottom.

Each policy requires a name and selection of the various options you want to include in the policy. For this example, I have created a policy named 'TR example' and enabled automatic installation of the antispyware client, automatic updates of both the product and spyware definitions, strict active application monitoring, and a full scan of machines included in this policy every night at 11:00, except Sundays. Once you create and configure a new policy, click the Save button. Your new policy now shows up in the list of available policies.

If you want specific machines to be included under a certain policy, you need to add machines to it by adding said machines to the policy's member list. From the Policies window, open the policy and choose the Policy Members tab. This tab shows you a list of computers associated with a particular policy. By default, all new computers are associated with the Global Default policy.

If you open up a new policy, you won't see any computers in the list. Click the Add Members button to add a computer to the Policy Members list. The screen shown in **Figure C** shows the two machines I have in my example.com domain in

**Figure C**



Policies

TR example Policy Non-Members

| □ Name | User | Domain | Status | Agent | Definitions | Licence |
|---|---|---|---|---|---|---|
| □ W2K3-STD | Administrator | EXAMPLE | Not Installed | 3.0.0.71 ● | 2.89 ● | Scan Only |
| □ XPP1 | | EXAMPLE | Not Installed | | | Scan Only |

Select the check box and click Add Members.

my lab. To add the W2K3-STD machine to the 'TR example' policy I created, I would select the highlighted check box and click the Add Members button.

Now, you can deploy client software to your desktop machines with the right policy.

### Deploy client software from the administration console

If you place a client into a policy for which you have enabled Automatic Installation, Trend Micro Antispyware will automatically install the client, assuming you have provided an appropriate user name and password for the client. In fact, after waiting a couple of minutes after adding W2K3-STD to the 'TR example' policy, the client was installed with no intervention required on my part. The W2K3-STD machine now has the client installed and is actively cleaning.

If, for whatever reason, Trend Micro Antispyware can't automatically deploy the client (perhaps you did not enable automatic client installation in your policy, for example), you can still manually deploy the client without having to use the MSI installer file. To do so, from the My Enterprise Network window, click the check box next to the computer to which you want to deploy the software and click the Install button at the bottom of the window.

If you have machines that are not a part of your domain, you can't use this automated deployment method and will need to use the MSI method instead.

### Deploy client software using an MSI installer

As I mentioned, if you have machines on which you can't use the domain installer, or if you already have a software distribution system in place, you should consider using the MSI client installer included with the Trend Micro Antispyware software.

To use the MSI file, you need to provide it with some parameters that allow the installed client to communicate with your server. On my XPP1 machine, I used the MSI installer with the following switches, most of which are pretty self-explanatory:

```
msiexec /i tmasclnt.msi ALLUSERS=1 RebootYesNo=No /Lve
tmasclnt.log /qn SERVERIP=192.168.160.128
```

- The /qn switch indicates that the installation should proceed quietly, with no notice to the user.
- The /Lve switch is always followed by the name of the file to which an installation log should be written.
- SERVERIP is fairly self-explanatory, but is critical.

The default MSI-based installation installs the software in "socket mode," which is one of three possible modes in which you can run the software. You can also run in "domain mode," which uses administrative shares to communicate with the server. Or, you can opt to use a polling method in which the client occasionally polls the server for updates. I won't be going over these last two options here.

By omitting this switch (called CMDMODE), I implicitly choose CMDMODE=1, which is the default—socket mode. Socket mode requires that ports 54447, 54448, and 54449 be accessible.

Also note that, if you use the MSI method to install the client, you need to manually allocate a license to the client machines, or else it will stay in a "scan-only" mode until you do so. I'll go over this step in the next section.

### Viewing client status

From here, your use of Trend Micro Antispyware is beyond the installation basics. During your use of the product, you will have machines that are exposed to spyware and are cleaned with the software. You can see exactly what is happening by using the same console you used to install the software and create policies.

For example, right after I installed the client into W2K3-STD, seven potentially problematic items were cleaned from the machine. In this case, they were all cookies.

If you used the MSI method to install the client, you also need to allocate a license for the client, or it will only be able to scan, and not take corrective action. Address this problem by clicking the License button at the bottom of the window.

## Trending away from spyware

Trend Micro has a good product on their hands with this, version 3.0 of their Antispyware product. It's pretty easy to use, powerful, and from the centralized management console you can perform most functions, as long as your machines are part of a domain. With the ability to support multiple policies, you can handle differing workloads and requirements across your enterprise. ❖

# Uncover spyware on your systems with Spy Sweeper

*By Bill Detwiler, MCP*

Spy Sweeper from Webroot Software (**http://www.webroot.com/wb/products/spysweeper/index.php**) is one of many spyware-removal utilities on the market, and, according to Webroot, it offers you a "sophisticated database of spyware definitions, the power to disable spyware, and the knowledge you need to analyze your risks." Does it live up to these claims? Can it convince me to switch from my longtime spyware-removal favorite Ad-aware from Lavasoft (**http://www.lavasoft.de/software/adaware/**)? As an IT support pro, should I recommend this product to my users instead of Ad-aware 6 Personal? Let's find out.

## Acquiring and installing Spy Sweeper

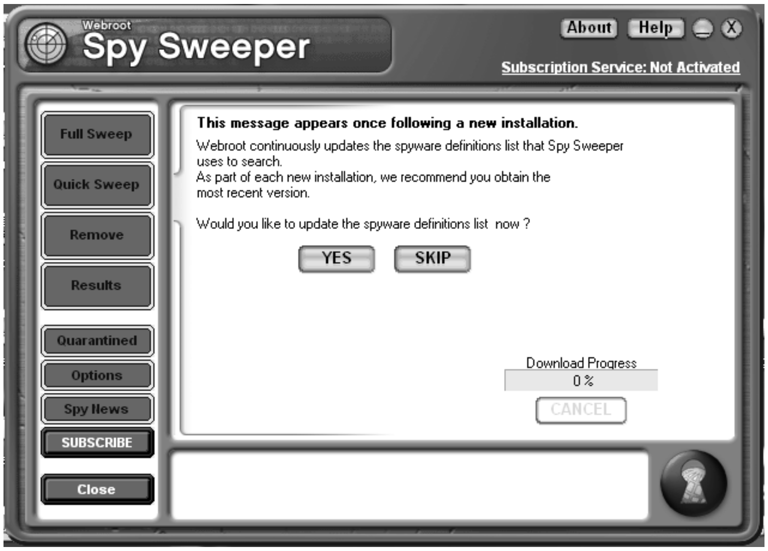
Spy Sweeper will run on Windows 98, NT4, Me, 2000, and XP. It requires a 150-MHz processor or better, 15 MB of free hard drive space, at least 32 MB of RAM, and a CD-ROM drive if you want to install it using a CD. It was easy to get my hands on a trial copy of Spy Sweeper by downloading the 1.33 MB installation file from Webroot's downloads page (**http://www.webroot.com/wb/downloads/index.php**). Although the downloads page said the installation file was 2.2 MB, the file I retrieved was only 1.33 MB. I'm not sure why there was a difference, but the file I downloaded installed properly so I assumed the information on the Web site hadn't been updated.

This brought me to my next question: How long can I use my trial copy of Spy Sweeper? Webroot's download page simply stated that I could use my fully functional trial software for a "limited time." It never specified whether this meant 30 days (as is typical of many trial software periods) or 30 years. I even read through the Spy Sweeper License agreement and was unable to come up with an answer. That left me with only one option: Call Webroot for more information.

I spoke with a very helpful and pleasant individual in Webroot's sales department who told me that the trial version of Spy Sweeper would work indefinitely, but that neither the spyware definitions nor the program itself could be updated. To update the software, I'd need to purchase a subscription: $29.95 for one year and $39.95 for two years. With that question answered, I was ready to install the software.

Installing Spy Sweeper was quick and easy. I double-clicked the installation file and proceeded through the installation wizard. As with most installation wizards, this one asked me to choose a path for the installation, to accept the EULA, to choose a location for the program shortcut, and to answer a few other standard

**Figure A**



**This message appears once following a new installation.**

Webroot continuously updates the spyware definitions list that Spy Sweeper uses to search.
As part of each new installation, we recommend you obtain the most recent version.

Would you like to update the spyware definitions list now ?

When you run Spy Sweeper for the first time, it automatically updates your spyware definitions.

questions. Near the end of the installation process, the wizard also asked me to activate my copy of Spy Sweeper by providing my e-mail address.

I assumed that this "activation" screen was merely used to collect e-mail addresses for marketing purposes, so I decided to skip it and finish the installation. Once the installation finished, I closed the wizard and ran Spy Sweeper by clicking its icon from the Start menu. Being that this was the first time I had run Spy Sweeper, I was asked to update my spyware definitions, as shown in **Figure A**. I clicked Yes, and the updating process proceeded normally. This would be the only time I'd be able to update the spyware definitions. When I tried to do so at a later date, I was prompted to purchase a subscription, as the sales representative said I would be.

Updating the spyware definitions took only a few moments, and once that process was complete, Spy Sweeper's main screen, shown in **Figure B**, appeared.

While looking over Spy Sweeper's main screen, I quickly noticed the subscription service status indicator in the top right-hand corner, as shown in Figure B. You can see that it says Subscription Service: Not Activated. This started me thinking about that "activation" screen I had seen during the installation. I began to wonder if I should have activated the software or if activation was the same as purchasing a subscription or something different. If I activated the software but didn't purchase a subscription, could I update the spyware definitions and program? Again I turned to my Webroot sales representative. Although he said he hadn't seen this screen personally, he believed my original assumption was correct.

This activation screen was used to collect marketing data and was completely unrelated to Spy Sweeper's subscription offerings.

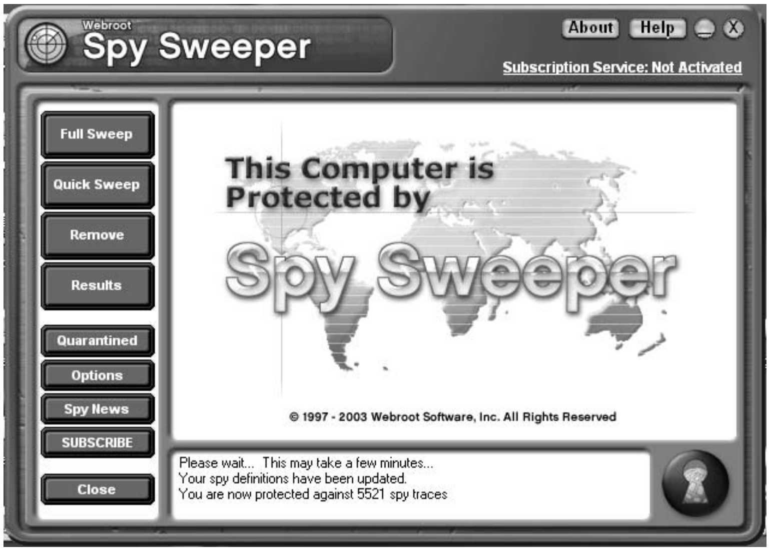
The next confusing item I noticed about Spy Sweeper was its version number. The download page said the installation file was for Spy Sweeper version 2.1, but once the installation was complete, Spy Sweeper reported being version 1.5.0 (Build 6). I was a little concerned by this discrepancy but continued with the assumption that I had the latest trial version and that the download site was simply mislabeled using the version of the latest subscription product. Later, when testing Spy Sweeper, I was informed that a new version of the software, Spy Sweeper 2.0, was available. But I was unable to update to this version because I didn't have a subscription.

## Using Spy Sweeper

With my spyware definitions updated and my questions answered, I was finally ready to begin using Spy Sweeper. Before performing my first scan, I checked out the program's Options screen, shown in **Figure C**.

For simplicity's sake, I decided to leave the default options in place and perform a Full

**Figure B**

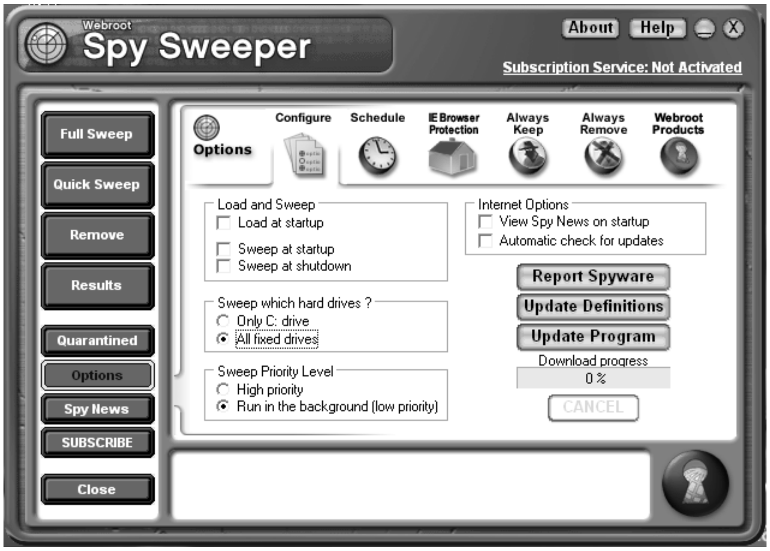


© 1997 - 2003 Webroot Software, Inc. All Rights Reserved

Please wait... This may take a few minutes...
Your spy definitions have been updated.
You are now protected against 5521 spy traces

Spy Sweeper's main screen allows you to take a variety of spyware-removal actions and easily access program options.

**Figure C**



Load and Sweep
□ Load at startup
□ Sweep at startup
□ Sweep at shutdown

Sweep which hard drives ?
○ Only C: drive
● All fixed drives

Sweep Priority Level
○ High priority
● Run in the background (low priority)

Internet Options
□ View Spy News on startup
□ Automatic check for updates

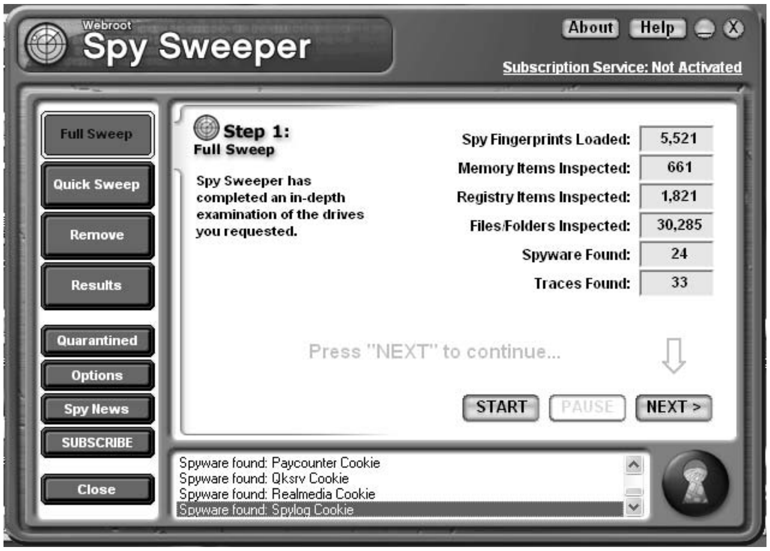
Download progress
0 %

From the Options screen, you can configure Spy Sweeper's scanning process, schedule routine scans, and set up IE protection options.

## Full Sweep vs. Quick Sweep

Spy Sweeper offers two spyware scanning options: Full Sweep and Quick Sweep. Like its name implies, a Full Sweep scans all items loaded into the computer's memory, the Windows registry, and files and folders on the machine's hard drives. During a Quick Sweep, Spy Sweeper scans the memory items and the Windows registry, but only a very limited number of files and folders on the machine's hard drives. The Quick Sweep takes around 2 1/2 minutes compared to the Full Sweep's 10 minutes or more (the file and folder scanning takes longer).

**Figure D**



**Step 1:**
**Full Sweep**

Spy Sweeper has completed an in-depth examination of the drives you requested.

Spy Fingerprints Loaded: 5,521
Memory Items Inspected: 661
Registry Items Inspected: 1,821
Files/Folders Inspected: 30,285
Spyware Found: 24
Traces Found: 33

Press "NEXT" to continue...

```
Spyware found: Paycounter Cookie
Spyware found: Qksrv Cookie
Spyware found: Realmedia Cookie
Spyware found: Spylog Cookie
```

A Full Sweep took around 10 minutes on my 1-GHz Athlon test machine running Windows XP.

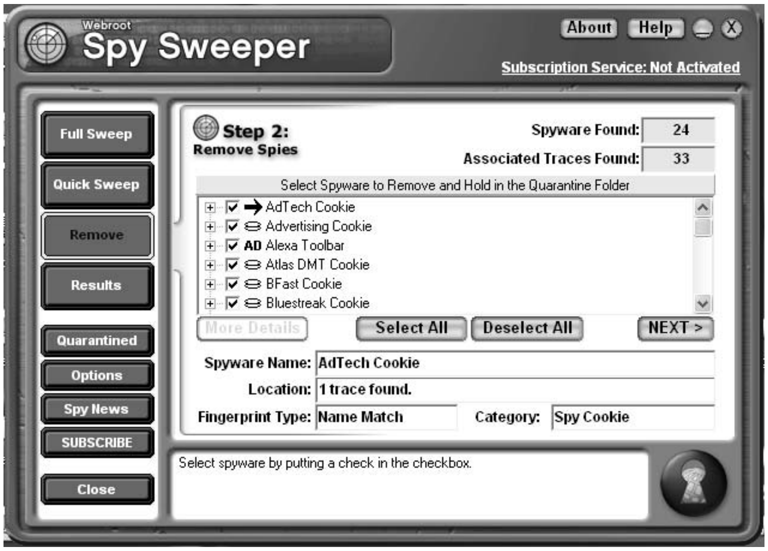
Sweep on my Windows XP, 1-GHz Athlon test machine. I clicked the Full Sweep button and then clicked Start.

When the sweep finished about 10 minutes later, Spy Sweeper reported finding 24 spyware items and 33 associated traces, as shown in **Figure D**. A single piece of spyware can manifest itself in multiple ways; the term *traces* is used to define individual instances of spyware.

I clicked Next, and Spy Sweeper displayed a list of each spyware item it found, as shown in **Figure E**.

From this screen, I was able to select which items I wanted Spy Sweeper to remove and place in the Quarantine folder. Placing items in a Quarantine folder instead of removing them instantly allows you to restore the item in case the removal causes problems. I could also get more information about each spyware

### Figure E



Spyware Found: 24

Associated Traces Found: 33

Select Spyware to Remove and Hold in the Quarantine Folder

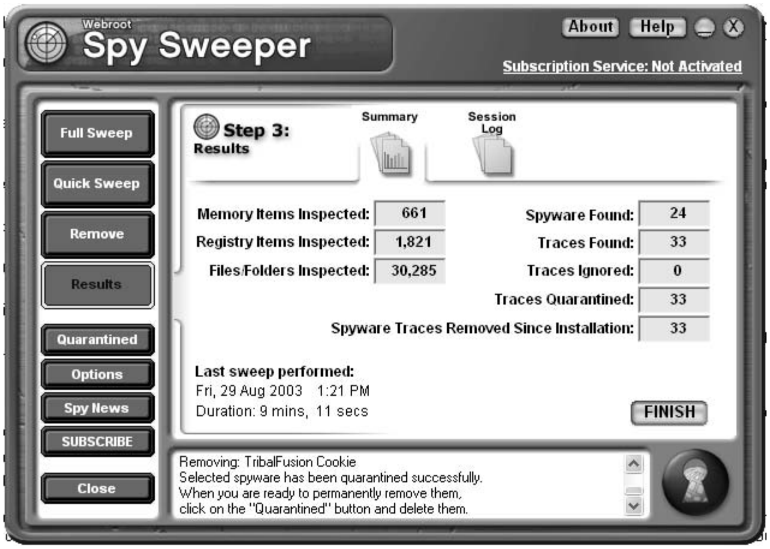
- ☑ AdTech Cookie
- ☑ Advertising Cookie
- ☑ AD Alexa Toolbar
- ☑ Atlas DMT Cookie
- ☑ BFast Cookie
- ☑ Bluestreak Cookie

|  |  |  |  |
|---|---|---|---|
| Spyware Name: | AdTech Cookie |  |  |
| Location: | 1 trace found. |  |  |
| Fingerprint Type: | Name Match | Category: | Spy Cookie |

Select spyware by putting a check in the checkbox.

Once Spy Sweeper completes a sweep, you can select which items should be removed and placed in the Quarantine folder.

### Figure F



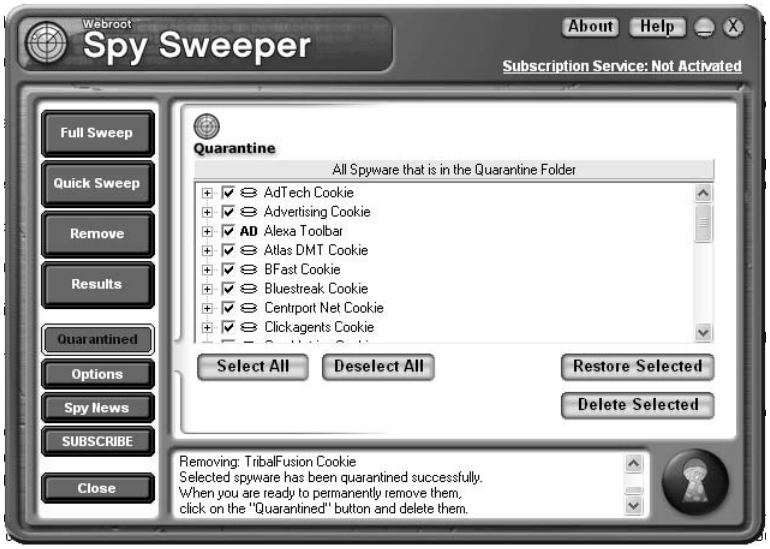
|  |  |  |  |
|---|---|---|---|
| Memory Items Inspected: | 661 | Spyware Found: | 24 |
| Registry Items Inspected: | 1,821 | Traces Found: | 33 |
| Files/Folders Inspected: | 30,285 | Traces Ignored: | 0 |
|  |  | Traces Quarantined: | 33 |
|  |  | Spyware Traces Removed Since Installation: | 33 |

Last sweep performed:
Fri, 29 Aug 2003 1:21 PM
Duration: 9 mins, 11 secs

Removing: TribalFusion Cookie
Selected spyware has been quarantined successfully.
When you are ready to permanently remove them,
click on the "Quarantined" button and delete them.

Once Spy Sweeper has removed and quarantined the spyware items it finds, you're given a summary of the process.

**Figure G**



All Spyware that is in the Quarantine Folder

- ☑ AdTech Cookie
- ☑ Advertising Cookie
- ☑ AD Alexa Toolbar
- ☑ Atlas DMT Cookie
- ☑ BFast Cookie
- ☑ Bluestreak Cookie
- ☑ Centrport Net Cookie
- ☑ Clickagents Cookie

Removing: TribalFusion Cookie
Selected spyware has been quarantined successfully.
When you are ready to permanently remove them,
click on the "Quarantined" button and delete them.

Once Spy Sweeper has placed a piece of spyware in the Quarantine folder, you can easily remove or restore it from the Quarantine screen.

item by selecting the item and clicking the More Details button. Browsing through the list, I saw nothing I wanted to keep, so I clicked Select All and then clicked Next to continue. After the spyware items were removed and placed in the Quarantine folder, Spy Sweeper displayed a summary of the scanning and removal process, as shown in **Figure F**.

With the scanning, removal, and quarantining processes complete, I decided to check out the quarantined items and remove them permanently. I clicked the Quarantined button from the left side of the Spy Sweeper screen and was presented a list of quarantined items, as shown in **Figure G**.

Normally, I would have removed all the quarantined items by clicking Select All and then Delete Selected, but I wanted to compare Spy Sweeper's scanning ability with that of Ad-aware 6 Personal, so I chose to restore the items by clicking Restore Selected.

## Spy Sweeper vs. Ad-aware 6 Personal

Now that I had performed a Full Sweep with Spy Sweeper, it was time to put Ad-aware 6 Personal to the same test. I wanted to know whether Ad-aware would find more, less, or the same number of spyware items as Spy Sweeper.

I opened Ad-aware and made sure I had the latest updates. (I really like being able to update Ad-aware without a subscription.) I then started a scan using the default settings. Ad-aware has only one type of scan, but you can customize it to be more or less thorough. Using the default settings would scan memory items, the Windows registry, and files and folders on the hard drive. This would give me a similar scan to that of Spy Sweeper's Full Sweep.

The scan took about 6 1/2 minutes to complete, less than Spy Sweeper's 10 minutes. Ad-aware had found 29 spyware instances—fewer than Spy Sweeper's 33 instances; but as I compared the lists, it appeared that Spy Sweeper counted some items twice. Both products found the same two registry entries and multiple cookies—which was the most common form of spyware found. Ad-aware did, however, flag a Windows Media Player unique ID entry in the registry as spyware. Spy Sweeper did not. Like Spy Sweeper, Ad-aware will remove and place items in a Quarantine folder until you want to delete or restore them.

## Final thoughts

Overall, Spy Sweeper did a good job of finding and removing spyware from my test PC. It installed without a flaw and ran without any problems. Spy Sweeper also offers a wide range of scanning options; plus, the staff—at least the sales rep I talked to—was polite and knowledgeable.

Despite these positives, I'm sticking with Ad-aware 6 Personal for now. Although both performed scans equally well, Ad-aware offers several benefits. First, and most important, I can update both the Ad-aware application and the definition file without spending $29.95 for a yearly subscription. Second, Ad-aware lacks the ever-present advertising that I found in Spy Sweeper's trial version. While I understand that the version I evaluated was only a trial version and that Webroot needs to sell its products, ads were a little too prevalent for my taste, and there are other free alternatives without such advertising. Third, Webroot should change the "activation" screen that asks for your e-mail address during installation to a "registration" screen. This would avoid any confusion about what this information is being used for. ❖

# Root out spyware problems network-wide with Webroot SpySweeper Enterprise 2.5

***By Scott Lowe, MSCE***

Any reasonable antispyware product has some way to centrally manage all clients—even into the tens of thousands of clients—and has a small footprint for the actual client software as well as a reasonable definition distribution system. Webroot's SpySweeper Enterprise 2.5 has all of these features and more. In this article, I will show you how to get this product up and running and managing clients in your organization.

## System requirements

Even supporting tens of thousands of clients, you don't need a very hefty server to run SpySweeper Enterprise. Overall, the system requirements are quite modest, and Trend Micro even provides a database product for smaller shops so you can avoid SQL Server licensing costs. Details are outlined below.

### Workstation

SpySweeper Enterprise supports quite a few operating systems, including some older software no longer supported by its competitors. Spy Sweeper 4.5 supports all workstation versions of Windows back to Windows 98 SE. Webroot requires that you have a minimum of a 300MHz processor, 128MB of RAM and 30MB of available disk space to handle the client. 256MB of RAM is preferred, though.

### Server

Webroot's SpySweeper Enterprise 2.5 does not require a massive server to do its job. In fact, Webroot's minimum requirements call for only a 200MHz server with 512MB of RAM, although Webroot does indicate that 200MHz is the minimum and recommends a machine that runs at least 350MHz. These days, that's one of the machines you took off a user's desktop and used as a doorstop.

If you plan to support more than a few users, I would highly recommend that you invest in a reasonable machine of at least 1GHz. Further, Webroot recommends that you have at least 60MB to 140MB of free disk space for the initial installation, with a gig or two available for growth. In the scalability section below, I've listed more exact server requirements for those of you who may have more than 500 clients.

Webroot's server also requires a database component in order to work its magic. While you can use an existing Microsoft SQL Server 2000 installation, you can also use the DBISAM database that is included with SpySweeper Enterprise 2.5. If you use the included software, you don't need to worry about any licensing issues related to the database. That's all taken care of when you buy SpySweeper Enterprise.

## Scalability

While SpySweeper Enterprise is capable of handling large numbers of clients from a single server, Webroot has taken the issue of scalability seriously in their product. For example, suppose that you need to support tens of thousands of desktops strewn about dozens of locations. Using what Webroot calls "Distribution Servers," which you can place in each location, you can more easily and affordably support just about as many clients as you can throw at the product.

A distribution server is a single server in any location that receives its updates from the central enterprise server. Clients are then updated from the distribution server rather than having to connect back to the central server. This type of scenario helps you better manage inter-site bandwidth and support larger numbers of clients.

During the server installation, you will be asked to select which database you want to use to store information for your SpySweeper Enterprise service—DBISAM or SQL Server 2000. Webroot recommends that you only use SQL Server 2000 if you have more than 10,000 clients running from your SpySweeper server and that, of course, you actually own SQL Server 2000. Otherwise, they recommend that you use the DBISAM option. If you select the SQL Server 2000 option, you will need to manually create a database for SpySweeper to use.

Webroot provides recommendations for how much horsepower your server should have and how many distribution servers you should plan based on how many clients you intend to support. **Table A** outlines these recommendations. Bear in mind that these are the minimum specifications.

## Installation

The SpySweeper Enterprise 2.5 installation process follows a fairly typical client/server installation scenario. Your first task is to get the server deployed. In

**Table A**

| # clients | RAM | Processor | Database | Distributors |
|---|---|---|---|---|
| < 500 | 512MB | 1 x 350MHz | DBISAM | None needed |
| Up to 10,000 | 512MB | 1 x 1 GHz | DBISAM | Up to 2 |
| Up to 40,000 | 1 GB | 1 x 1 GHz | SQL 2000 | 2 or 3 |
| Up to 75,000 | 2 GB | 2 x 1.1GHz | SQL 2000 | 3 to 6 |

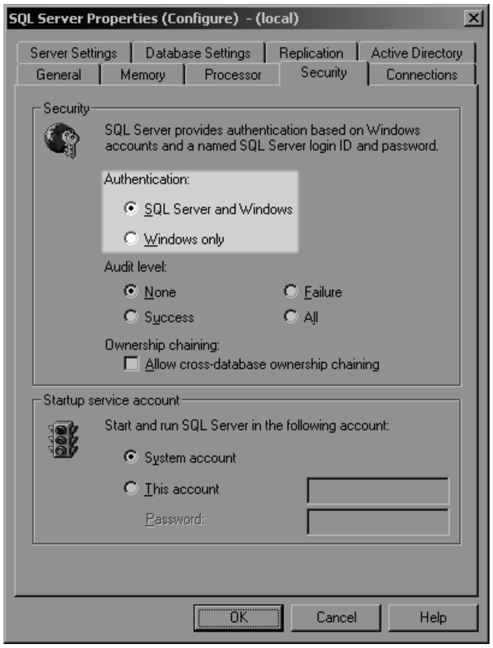
Minimum specifications based on number of clients in your environment this case, the server holds the SpySweeper management console, from where you can centrally manage your antispyware rollout. In my opinion, installing any enterprise management software without some kind of centralization is asking for a support nightmare.

Once the server component is in place, SpySweeper provides you with a number of options for deploying the client to your workstations. All of the methods use a standard MSI installation file. You can push the client installation from the management console, install from a login script or via an Active Directory group policy, or deploy from a software distribution system, such as SMS or ZenWorks. Or, you can just walk around with a CD and install the client manually. If you have thousands of desktops, I don't recommend this method, unless you want to get out and about in userland for weeks at a time.

### Before you begin the antispyware software installation

If you intend to use SQL Server 2000 as your database, you need to manually create a database for SpySweeper as well as a related database user. For this purpose, Webroot recommends that you use SQL authentication for the user you create rather than relying solely on Windows authentication to the database. Further, SpySweeper requires that you use case-insensitive collation on your SQL Server 2000 system.

**Figure A**



Security

SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password.

Authentication:

● SQL Server and Windows

○ Windows only

Audit level:

● None ○ Failure

○ Success ○ All

Ownership chaining:

□ Allow cross-database ownership chaining

Startup service account

Start and run SQL Server in the following account:

● System account

○ This account

Password:

The highlighted area needs to be examined.

To create this database, from whatever server on which you have SQL Server installed, start SQL Server Enterprise Manager by going to Start | All Programs | Microsoft SQL Server | Enterprise Manager. Once you are in Enterprise Manager, make sure that your SQL Server supports both Windows authentication and SQL Server logins. Go to Tools | SQL Server Configuration Properties and select the Security tab to check this setting, as seen in **Figure A**.

If you are currently set for Windows-only authentication, change this option and click OK. When you do so, you will be told that SQL Server must be stopped and started, but this happens automatically.

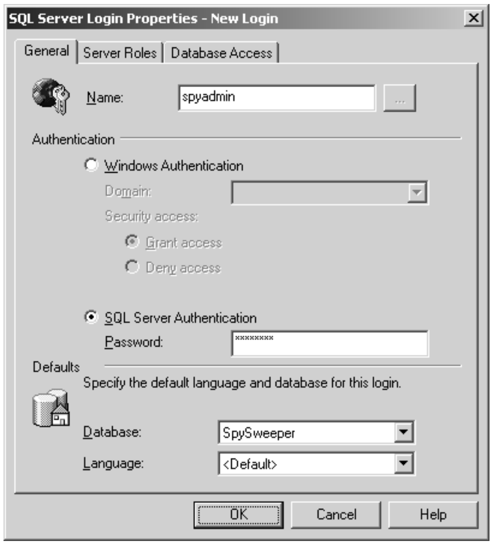
Now, expand the tree until you see the Databases option under your server. Right-click the Databases option and choose New Database from the shortcut menu.

On the resulting Database Properties window, in the Name field, enter the name of the database you want to create to use for SpySweeper. In this example, I've given it the name 'SpySweeper.' I know… not very original. Once you enter a name, click OK.

At this point, your new database is created, but you need to create a SQL user so SpySweeper can access the database. Right-click your newly created database and choose New | Database User from the shortcut menu. On the resulting Database User Properties window, click the drop-down button next to the Login name field and choose the New option from the menu.

The resulting SQL Server Login Properties window has a bunch of option to which you need to pay attention, as you can see in **Figure B**. First, give your user a name. In this example, I've used the ever original name 'spyadmin.' Choose the SQL Server Authentication option, and provide a password for this user. Finally, one thing I like to do with SQL database users, when possible, is assign them a default database. Click OK when you're done. You will be asked to confirm the password you've assign to this new user. If you did grant the user the default database of SpySweeper, you may receive an error message indicating that the user does not have access yet. Click Yes to continue past and ignore this message for now. We'll fix that next.

**Figure B**



SQL Server Login Properties - New Login

Name: spyadmin

Authentication

○ Windows Authentication

Domain:

Security access:

● Grant access

○ Deny access

● SQL Server Authentication

Password: ********

Defaults

Specify the default language and database for this login.

Database: SpySweeper

Language: <Default>

Make sure you select the right properties to make your SpySweeper installation go more smoothly.

Now, on the Database User Properties window click the down arrow next to Login name and choose the database administrative user that you just created, and make sure to assign this user the db_owner role so that the user can make any modifications that it needs to make to the SpySweeper database. Click OK when you're done.

You can close SQL Server Enterprise Manager now. I will use this database during the installation of the SpySweeper product.

## Server

For this article, I'm going to stick with a single centralized server and will not be installing any distribution servers. To start the installation, run the file WebrootEnterpriseServerSetup.exe from your distribution media or download.

As usual, the first couple of screens give you a quick overview of the software, followed by the ever-present software licensing agreements. Read each one, and click the Next button to continue.

Next, provide an installation path for SpySweeper Enterprise. The default location is C:\Program Files\Webroot\Enterprise\Server, which I have used for this example. If your chosen directory doesn't exist, the installation asks you if you really want to create a new folder.

Now, in a not-so-important step, choose the Start Menu group into which you want SpySweeper's launch icons to be installed.

On the next screen, you start doing something that gets you somewhere. First, the installer asks you for the name of your company. Second, you're asked to enter your keycode that uniquely identifies what your installation is to do. Your keycode is sent to you enclosed in { curly braces }. Make sure that, when you enter your keycode, you include these curly braces. Click Next.

After your installation, the SpySweeper server needs to occasionally poll Webroot central command in order to obtain updates, including software updates and information regarding new spyware. Webroot recommends that you don't set this to be less than twelve hours, which is the installer's default period.

The reason: Webroot releases updates only on Tuesdays and Thursdays, so polling their servers more often is generally a fruitless endeavor. On this screen of the installer tell SpySweeper how often you'd like it to poll for updates. Even though Webroot does not provide constant updates, SpySweeper gives you a choice in the range from hourly to weekly. With your polling period defined, also tell SpySweeper into which directory updates should be stored. The default is C:\Program Files\Webroot\Enterprise\Server\Updates. Click Next.

The next screen asks you to enter information regarding your proxy server, if you have one. I don't have a proxy server in my lab, so I've left this screen blank. Click the Next button to continue.

Like your server does with Webroot, each client needs to periodically chat with your SpySweeper Enterprise Server to look for new definitions and to see if you've made any configuration changes that may need to be applied. In this polling scenario, the client, by default, polls the server every hour. You can change this interval to be as short at 10 minutes or as long as a day. Also, provide the static IP address and IP port on which clients can communicate with this server. If you're using a software firewall on the server, make sure to allow communication on this port. By default, SpySweeper uses port 50,000 for this conversation.

The SpySweeper server needs an SMTP server through which it can send notification messages. Specifically, you need to provide the name of an SMTP server, as well as a real e-mail account, which SpySweeper will use as the From address. For this example, I've created an e-mail account specifically for SpySweeper. If your mail server requires that you authenticate in order to send mail through, provide your credentials on the next screen. In my lab, I've allowed relay from my SpySweeper server (and only from this server) to my SMTP server instead.

When you deploy the client, do you want the user to see the process? If not, you can run the client installer either minimized or even invisibly. These choices, plus the option of popping up a window, are presented to you on the next screen of the installer. For this example, I've opted for the Stay Minimized option.

The next screen asks you to choose which database—DBISAM or SQL Server 2000—you want to use for your installation. Webroot recommends that you use SQL Server 2000 only if you have more than 10,000 clients running from your SpySweeper server and that, of course, you actually own SQL Server 2000. Otherwise, they recommend that you use the DBISAM option. For this article, I will be using the SQL Server 2000 database option. Of course, if you have only a few (or a few thousand—up to 10,000, actually) clients, you can use the included DBISAM database instead.

The next screen asks you to verify your entries. Once you do so, the installation begins. At the end of the installation, you are told that you have a number of options for client deployment, including an automatic deployment from SpySweeper's console. Of course, you can also deploy the client via group policy, Active Directory, SMS, or whatever method you would normally use. The client installer (MSI) files are located at C:\Program Files\Webroot\Enterprise\Server\Client.

Do note that the server installation installs only the SpySweeper Enterprise console, and does not install a client. For this example, I will install the client to the server using an MSI file and will push deploy a client to a workstation using the management console.

## Server MSI client installation

To install the client on your server, browse to the MSI client installer location and double-click the file SpySweeperSetup.exe. That's *all* you have to do. The installation is completely automatic beyond that. When you're done, the SpySweeper icon will appear in your system tray.

## Centralized client deployment

Before you can deploy clients using SpySweeper's push feature, you need to configure the SpySweeper Admin Console service with the credentials of a domain administrator. To do this, go to Start | Administrative Tools | Services (Windows 2000—Start | Control Panel | Administrative Tools | Services). Locate the service named Webroot Admin Console and right-click it, choosing Properties from the resulting shortcut menu.

From the Properties page, select the Log On tab. On this tab, choose the This Account option and provide the credentials for an account that has domain administrator privileges. Note that Windows will add the Log On As A Service right to this account when you do this. Using Active Directory Users and Computers, I've created an account named SpyAdmin and added it to the Domain Administrators group. You need to stop and restart the service once you make this change.

Now, go to Start | All Programs | Webroot (Enterprise) | Admin Console. The default username is admin, as is the default password for the console.

In the Admin Console, choose the Client Deployment option. Select the domain or workgroup that contains the system onto which you want to deploy the client, and then look for the client in the right-hand window. It may take a little time for this window to fully populate. Select your target system and click the Deploy Client button located at the bottom of the window.

Wait between 30 seconds and a minute and click the refresh button. When you do so, you should have a green indicator with a check mark next to your client and, if you look at one of your client machines, you will see the SpySweeper icon sitting in the system tray. Even better, with the exception of the icon appearing, the entire process is transparent to the user.

## Managing clients

At this point, you have the management console installed and working, and you've successfully deployed a client. Like any good enterprise antispyware product, SpySweeper provides you with the capability to define policies for different groups of computers. For example, you might want computer A to do a full scan between 5 and 6 in the morning while computer B should perform a scan sometime in the evening.

### Adding groups

To add a new group into which you can place workstations, go to Admin Tasks | Client Management and click the Add Group button. A box appears asking you for the name of the new group. I've created the group named 'TR sample.' The group named 'EXAMPLE' was already there, and the name was derived from the name of my domain (example.com).

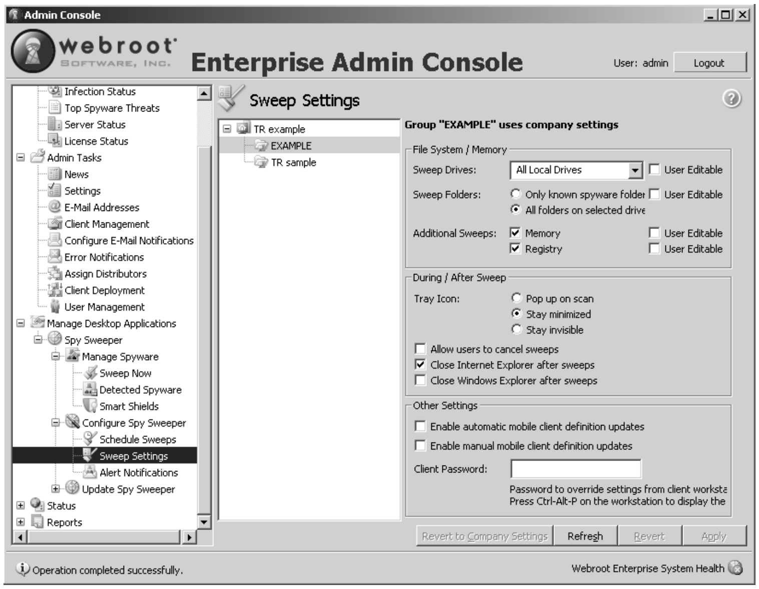
To add a workstation to a group, drag and drop it from the right-hand section of the screen into the group in which you want the client to reside.

### Managing group settings

Each group can have its own policies, including scheduling scans and determining what a client should do once spyware is found. To manage group settings, in the admin console, go to Manage Desktop Applications | Spy Sweeper | Configure Spy Sweeper | Schedule Sweeps.

Notice that there are two groups here that match what we looked at before. However, there is also a top-level group here named 'TR example.' By default, this top-level group holds a global policy that can be overridden by lower-level groups. In fact, the group TR sample uses its own settings. You can tell by looking at the bold text that reads "Group 'TR sample' uses group settings." If I had not made any changes to TR sample's settings, that text would have instead read "Group 'TR

## Figure C



Sweep Settings

Group "EXAMPLE" uses company settings

File System / Memory

Sweep Drives: All Local Drives ☐ User Editable

Sweep Folders: ○ Only known spyware folder ☐ User Editable
● All folders on selected drive

Additional Sweeps: ☑ Memory ☐ User Editable
☑ Registry ☐ User Editable

During / After Sweep

Tray Icon: ○ Pop up on scan
● Stay minimized
○ Stay invisible

☐ Allow users to cancel sweeps
☑ Close Internet Explorer after sweeps
☐ Close Windows Explorer after sweeps

Other Settings

☐ Enable automatic mobile client definition updates
☐ Enable manual mobile client definition updates

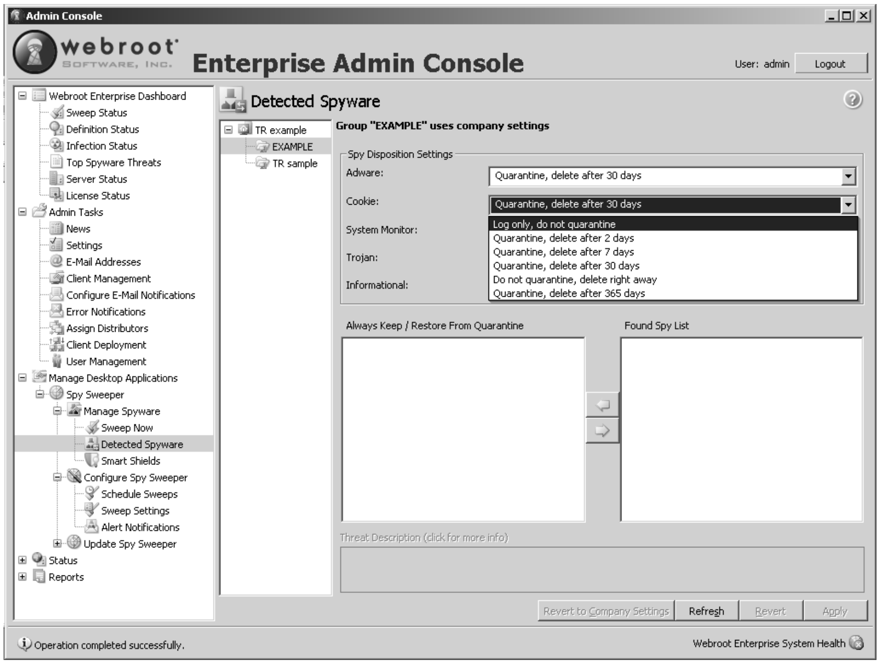
Client Password:

Password to override settings from client workst
Press Ctrl-Alt-P on the workstation to display the

Operation completed successfully.

This is the Sweep Settings screen on which you can dictate which drives the SpySweeper client will scan as well as other parameters, including whether or not SpySweeper will scan memory and the registry and much more.

## Figure D



Detected Spyware

Group "EXAMPLE" uses company settings

Spy Disposition Settings

Adware: Quarantine, delete after 30 days

Cookie: Quarantine, delete after 30 days

- Log only, do not quarantine
- Quarantine, delete after 2 days
- Quarantine, delete after 7 days
- Quarantine, delete after 30 days
- Do not quarantine, delete right away
- Quarantine, delete after 365 days

System Monitor:

Trojan:

Informational:

Always Keep / Restore From Quarantine

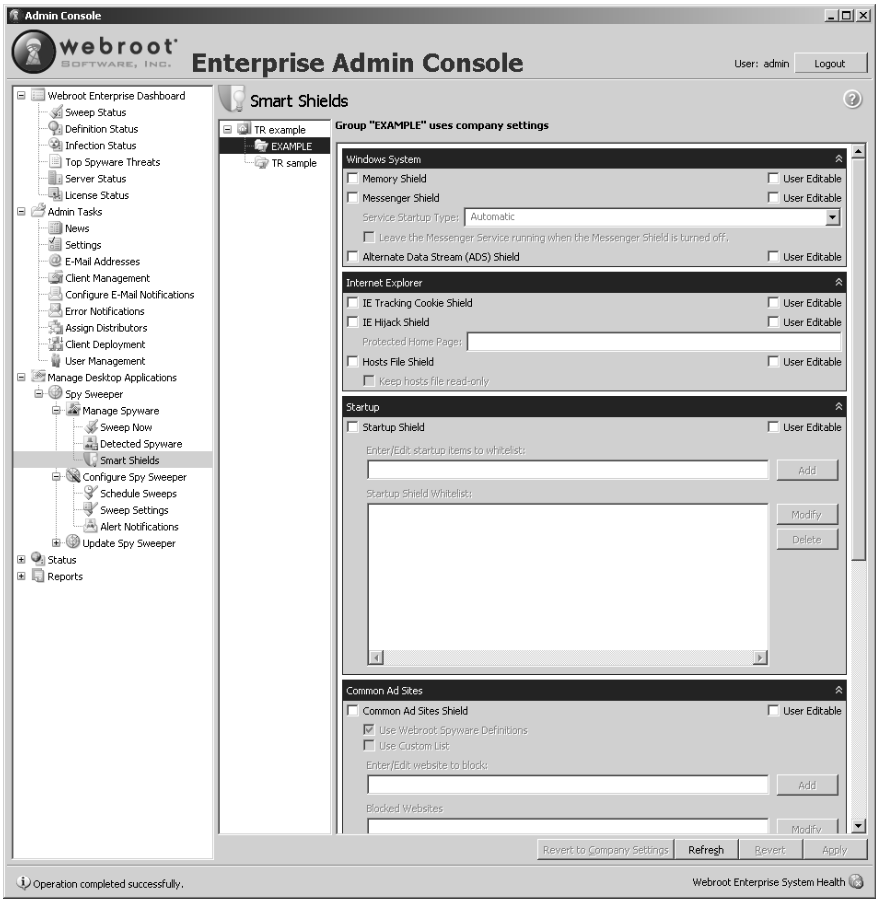
Found Spy List

Threat Description (click for more info)

Operation completed successfully.

What would you like the SpySweeper client to do with the various kinds of detected spyware?

**Figure E**



Group "EXAMPLE" uses company settings

Windows System

- □ Memory Shield □ User Editable
- □ Messenger Shield □ User Editable
- Service Startup Type: Automatic
- □ Leave the Messenger Service running when the Messenger Shield is turned off.
- □ Alternate Data Stream (ADS) Shield □ User Editable

Internet Explorer

- □ IE Tracking Cookie Shield □ User Editable
- □ IE Hijack Shield □ User Editable
- Protected Home Page:
- □ Hosts File Shield □ User Editable
- □ Keep hosts file read-only

Startup

- □ Startup Shield □ User Editable
- Enter/Edit startup items to whitelist:
- Startup Shield Whitelist:

Common Ad Sites

- □ Common Ad Sites Shield □ User Editable
- ☑ Use Webroot Spyware Definitions
- □ Use Custom List
- Enter/Edit website to block:
- Blocked Websites

Operation completed successfully.

Which Smart Shields would you like to enable? Webroot uses the term “Smart Shield” to refer to a continuous, active monitoring activity.

sample’ uses company settings,” which are the default settings that you establish for the top-level group.

**Figures C**, **D**, and **E** show you the other primary configuration screens for centrally configuring the client side of SpySweeper. I won’t go over every option in this article, but will show you the screens so you get a feel for what SpySweeper can do.

## Getting to the root of spyware

SpySweeper is a feature-packed product with just about all of the components that make for a viable enterprise-grade antispyware service, including central administration, an active scanning feature, and more. ❖

# Protect your workstations from spyware with Symantec's Client Security

*By Scott Lowe, MSCE*

There are two ways to handle antispyware clients. Provide an antispyware client on its own that either includes its own central management system or that integrates into an existing management console. Or, make the antispyware component an integral part of an antivirus solution. Both have pros and cons. In the bundled scenario, it's possible that you have selected an antivirus vendor that does not provide antispyware, or, for some reason, you don't want to use that vendor's antispyware offering. On the plus side, it's a whole lot easier to manage a single desktop-protection infrastructure!

Symantec, through their Symantec Client Security offering, has taken the bundled approach. I will go over much of Symantec Client Security in this article and show you how to get this product up and running in a centrally managed way and to protect your desktops from spyware infestations.

## System requirements

SCS, like all software, requires certain minimum system requirements in order to function as you expect. As your client base grows, you may need more horsepower, but this section goes over the minimum specifications suggested by Symantec.

### Workstation

As is typical with most antispyware clients, Symantec Client Security does not impose overwhelming system requirements. In fact, a system running at a speed of greater than 150MHz with 128MB or RAM and 115MB of available disk space is the minimum configuration recommended by Symantec. On the operating system side, you're somewhat limited, but if you're running a newer operating system, you're in good shape since SCS supports Windows 2000 Pro and both Windows XP Home and Pro. Regardless of your operating system, you do need to be running Internet Explorer 5.5 SP2 or greater.

### Server

On the server side, Symantec's requirements vary depending on which components you want to install, but are also fairly minimal for lower-end applications. Obviously, as you scale up client support, you should also expect to scale up your server specifications. Symantec supports both Windows and NetWare servers for the server side.

On the Windows side, Symantec's Security Management Server requires Windows 2000 (any edition), Windows XP Pro, or any edition of Windows Server 2003, with at least 64MB of RAM and 111 MB of disk space installed in a machine with a 150MHz or faster processor.

For NetWare users, you minimally need NetWare 5.x SP8, NetWare 6 SP5, or NetWare 6.5 SP2 with 15MB of available RAM for Symantec's antivirus NLMs. You also need a 150MHz or faster computer with 116MB of available hard drive space.

### Management workstation

Like many of today's desktop management applications, Symantec's client tools can be installed on any number of workstations, which is particularly useful for your IT staff. I generally recommend installing management tools on your Symantec servers, too. In this case, the requirements for the management tools are ridiculously low. For the management tools to operate, any version of Windows 2000 or better will work as long as you have 36MB of disk space and 32MB of available RAM. You also need the Microsoft Management Console since Symantec's management application uses it.

### Network security considerations

In any client/server type installation, the network plays the integral role of providing a communications channel. As such, you need to make sure that any security policies you have in place are modified to support the needs of Symantec Client Security. Specifically, Symantec wants ports 1,024 to 5,000 open at both the client and the server. Of course, you don't need to provide carte blanche access. To keep a lid on things, just open up these ports between specific machines or networks. Further, in order to provide for remote installation, you need to have TCP port 139 open in the same fashion. Finally, at the server side of the equation, open UDP ports 38,293 and 1,024 to 5,000 to allow discovery to take place.

Additionally, the firewalls included with Windows XP and Windows Server 2003 can interfere with SCS's ability to do its job. For example, when these operating system-provided firewalls are enabled, you may have problems installing or deploying the Symantec software.

## Installation options

You have a number of installation options to consider when you decide to deploy Symantec Client Security. For example, you can opt to install the Symantec System Center, which installs the following, by default:

- **Symantec AntiVirus snap-in:** Manages Symantec's antivirus client, which includes antispyware scanning capabilities.

- **Symantec Client Firewall Administrator:** Manages Symantec's client-based firewall.
- **AV Server Rollout tool:** Allows you to push the antivirus server install to other servers in your organization.
- **Client Remote Install tool:** Provides you with the capability to remotely install the SCS client on Windows computers in your organization.

For this article, I will be performing a default installation of Symantec Client Security on a Windows Server 2003 system.

## Installation—Symantec Client Security

To get started, double-click the setup.exe file from your distribution media. Choose the option Install Symantec Client Security.

From the next menu, choose the Install Symantec Client Security option to get started with the main product installation.

First, you need to accept the license agreement and click Next. On the next screen, you have your first decision to make: is this going to be a client installation or a server installation? If you really wanted to, you could just walk from workstation to workstation and perform a client install. I wouldn't recommend it, though. It's a whole lot easier to manage all of your clients from a single location. As such, choose Server Install and click Next.

Now, you can opt for a complete installation, or pick and choose what you want. I've opted to perform a complete installation, which installs the product to C:\Program Files\Symantec Client Security and installs Antivirus User interface and help as well as the Quarantine Client.

Next, you need to either create a new Server Group—a group of protected servers—or join an existing server group. Since this is a new installation of Symantec Client Security, I don't have an existing server group. I've accepted the default name of "Symantec AntiVirus 1" for this group.

Also on this screen, you need to provide the administrative username and password for this group. The default username is "admin," and I provided the password. Click Next when you're ready.

If you create a new group, the installer asks you to verify the password you entered on the previous screen. During the installation, you can opt in to a couple of options, both described here:

- **Auto-Protect:** This is a process that stays running all the time, watching your computer to look for nefarious activity. I highly recommend you run Auto-Protect wherever possible.
- **LiveUpdate:** LiveUpdate is Symantec's automatic product and definition update service.

Take both of these. You'll be glad you did!

Now, the installer has enough information to move forward. The next screen just asks you to click the button marked Install to finish the process. When the installation is finished, click the Finish button.

If you opted to do a LiveUpdate after the installation completed, you will perform this operation now. Click Next to continue through the process.

All you've done at this point is install the actual scanning tools and limited management software. In the next section, I'll go over the installation of the Symantec System Center, a centralized management console.

## Installation—management component

You do need to install the management software to your Symantec servers and to the workstations of the IT folks that will manage the service. For this article, I'm installing the management component just to the Symantec server itself. Symantec's documentation indicates that the management component should be installed first, but I've never had any trouble installing it after other services.

To get started, double-click setup.exe file from the distribution media. From the main menu, click Install Administrator Tools.

From the resulting menu, select Install Symantec System Center.

On the next screen, accept the license agreement and click Next.

Component selection in the management console is fairly straightforward. By default, everything except the Alert Management System Console is selected, and this default selection is what I am covering in this article. The Alert Management System Console (AMS) is Symantec's centralized alerting system. Click Next to continue.

**Note:** If you decide to use AMS, be sure to carefully read the documentation that comes with Symantec Client Security. If you don't follow the recommendations from Symantec, you could run into problems as you promote and demote primary and secondary servers.

By default, the management console is installed to C:\Program Files\Symantec\Symantec System Client. You can change this by clicking the Change button and choosing a new folder. Click Next when you're done.

After you've made all of your selections, click the Install button to make the installer work its magic.

When the installer has completed its task, click the Finish button. You will need to restart the system to finish the installation, though.

### First-time administrative requirement

Before you can do a whole lot, you need to identify which Symantec server will lead the group you created during the installation. Even if you have only a single Symantec server you need to explicitly identify it as a primary server. To do this, start the Symantec System Center console from Start | All Programs | Symantec System Center Console | Symantec System Center Console. Provide the username and password you designated during the installation.

Before you can manage a server group, you need to unlock it. Under Symantec System Center | System Hierarchy, right-click your server group and, from the shortcut menu, choose Unlock Server Group. In the resulting authentication window, provide the username and password you created during the product installation.

Browse to your server. In this example, my Symantec server lives under Symantec System Center | System Hierarchy | Symantec AntiVirus 1.

Right-click your server and choose Make Server a Primary Server from the shortcut menu. A message will appear warning you that, if you already have a primary server, all primary server operations will be transferred to this server, and secondary servers will be updated accordingly, and the event collection could be interrupted while this transition is under way.

## Centralized client deployment preparation

Before you get started with client deployment, you should determine how clients will receive their definition updates. Symantec recommends that you use what they called VDTM—Virus Definition Transport Method—for definition updates. Under VDTM, the primary server in a group is configured to retrieve updates from Symantec or from another internal LiveUpdate server.

By default, when you create a new server group, the primary server is configured to propagate definitions to clients every week between Thursday and Friday and within 480 minutes of 8:00 PM. The nice part about VDTM is that it conserves bandwidth to the Internet. Only the primary server in a group may need to contact Symantec. All other traffic can stay internal.

If you want to change your group's VDTM settings, right-click your server, and choose All Tasks | Symantec AntiVirus | Virus Definition Manager.

Now, before you start to deploy clients, you should also configure scan schedule and Auto-Protect settings.

We'll start with scan schedules. Configure a scan schedule by right-clicking your server *group* and selecting All Tasks | Symantec AntiVirus | Server Scheduled Scans from the resulting shortcut menus. This opens the *server group name* Schedule Scans window. In this window, click the New button to create a new schedule.

From this new scan window, you can choose the frequency and time of day to run a scan. If you choose to do a weekly scan, a day picker shows up. You can also choose the type of scan: Quick, Full, or Custom. A full scan scans everything, including the boot sector, executables in RAM, and all files and folders. A quick scan, on the other hand, looks at RAM and only common infection locations.

## Deploying clients

Now, with the brunt of the basic configuration out of the way, let's deploy a client. Symantec provides you with a tool called ClientRemote Install for this purpose. In order to use this tool, you need to have domain administrative rights with the currently logged in user account. Refer to the Symantec documentation for information on what to do if you need to deploy the client to workgroup machines that are not part of a domain.

To use it, from the management console, go to Tools | ClientRemote Install. This starts a wizard that helps you deploy the client to one or more computers in your organization.

Your first task is to tell ClientRemote Install where your client installation files are stored. If you selected the default location for the client security program, choose Default Location here. Otherwise, select the blank box's radio button and provide the location of the files. Click Next when you're ready.

On the next screen, you can associate a workstation with a Symantec server. If you have multiple Symantec servers, you'll need to decide with which one you want to associate a client. To associate a client with an antivirus server, in the Available Computers windows, browse for the desired client and click it. Next, browse for the Symantec server with which this client will work and click the Add button.

After a few seconds (or more, depending on your network and speed of your clients and such), your client selection will appear under the Symantec server in the right-hand column. Note that this does not install the Symantec client on the machine. It just creates a logical connection between a client and server. You can make as many associations as you like in this step. Click Finish.

After you make all of your associations and click Finish, an installation status window pops up. Since the previous step only made client/server associations, this step is responsible for actually installing the client on the systems you specified. Click Done when the installation is complete.

When you go back to the management console and click on a Symantec server, you'll see the client as one of its management entities.

From here, you can update your definitions to bring your software and definitions current. You can also enable continuous updates, from the management console, by changing your virus definition manager settings. ❖

# Controlling spyware with McAfee Antispyware

***By Scott Lowe, MSCE***

Spyware has become as big, if not a bigger problem for IT professionals than viruses. One of the big players in the antivirus space, McAfee also has an enterprise-level solution for battling spyware. McAfee's antispyware offering is similar to Symantec's in that it rides on top of their existing antivirus software. Unlike Symantec's solution, however, McAfee's is still somewhat separate. Unlike Symantec, which has combined virus and spyware scanning into a single client, McAfee's antispyware client is separate and plugs in to the enterprise antivirus client. In order to use McAfee's antispyware software, you need either version 7.1 or 8.0i of McAfee's enterprise-edition antivirus software installed, with version 8.0i being preferred.

In order to centrally manage this combined client, you also need McAfee's management platform, called ePolicy Orchestrator. For this article, I will be installing ePolicy Orchestrator 3.6 as well as version 8.0i of both the antivirus client and the antispyware plug in.

I'm going to go over basic information regarding the antivirus capabilities of the McAfee offering, but will go over handling the antispyware solution more in depth.

## System requirements

The thing that requires the most in terms of software requirements is McAfee's ePolicy Orchestrator (ePolicy Orchestrator) software. As such, the system requirements listed below for the server and database server are actually reflective of the requirements for ePolicy Orchestrator. I'm installing everything, including the database, on a single server.

While McAfee supports non-Windows machines for client installations, I will be focusing on the Windows environment in this article. You can also install the ePolicy Orchestrator agent and various clients on NetWare (4.11 – 6.0). Keep in mind that ePolicy Orchestrator is the management solution that covers *all* of McAfee's products. The ePolicy Orchestrator installation guide includes a complete product support, compatibility, and feature matrix.

### Workstation

In order to install the client software, a workstation must meet a few minimal requirements. First, non-NT-based versions of Windows are not supported. This means that, if you're still running Windows 95, 98, or ME, you're out of luck. Windows NT, 2000, XP, and 2003 are all supported, as long as you have a reasonably recent service pack.

Beyond this, the antispyware offering has the same system requirements as the antivirus product:

- At least a 166 MHz processor
- At least 32 MB of RAM
- At least 38 MB of free disk space
- Internet Explorer 6.0 or later
- A trust relationship with the domain's primary domain controller

As you can see, the client software doesn't exactly require a powerhouse of a machine!

### Server (including ePolicy Orchestrator)

On the server side, you're more limited in your operating system selection, but only slightly. McAfee supports every server version of Windows back to Windows 2000 SP3, but does not support Windows XP, which makes sense since XP is not a server operating system. While McAfee does provides wide support for all versions of Windows server, you do need a reasonably current service pack installed.

Beyond this, the antispyware offering has the following requirements, based on the antivirus software core of the product and the ePolicy Orchestrator system requirements:

- At least a 450 MHz processor
- At least 512 MB of RAM, with 1 GB recommended
- At least 500 MB of free disk space, with at least 2 GB recommended
- Internet Explorer 5.0 or later
- A static IP address for the server (highly recommended)

### Remote management station (ePolicy Orchestrator)

If you install a remote management station (for example, on an IT staffer's machine), the machine needs to meet the following minimum requirements:

- At least a Pentium II processor
- At least 128 MB of RAM
- At least 250 MB of free disk space
- Internet Explorer 6.0 or later
- Any version of Windows back to Windows 2000 SP3, including Windows XP Professional (with SP1 or better)

### Database

McAfee's solution runs using MSDE or Microsoft SQL Server 2000 SP3+ database software. You also need MDAC 3.8 for use with ePolicy Orchestrator. If you're managing more than 5,000 clients, McAfee recommends that you use a dedicated SQL Server rather than running ePolicy Orchestrator and SQL on the same hardware.

## Installation procedure

McAfee's solution is significantly more distributed and scalable than some other solutions on the market. As such, care needs to be taken during deployment to make sure that you have no problems. For this article, I will be installing all of the necessary components

- SQL Server 2005 (In my lab, SQL Server 2005 is installed on its own server separate from the McAfee server.)
- McAfee ePolicy Orchestrator—McAfee's central management console that manages all of their products.
- AntiVirus Enterprise 8.0i
- AntiSpyware Enterprise 8.0i (the plug-in that works with the antivirus software)

## AntiVirus Enterprise 8.0i

In this section, I'll be installing McAfee's antivirus client on the target ePolicy Orchestrator server. This client installation is handled the same way that you would a manual client installation on a workstation. Later in the article, I will go over an automated deployment method for your clients as well.

**Note**: If you're wondering what the letter 'i' means at the end of McAfee's newer products, it denotes the newish intrusion prevention system (IPS) capabilities in the product.

To get started with the AntiVirus client installation, double-click the setup.exe file from your AntiVirus 8.0i distribution media.

Look at, read, and accept the software license agreement that is shown on the first screen of the installer. Click the OK button to continue with the installation.

Your next major decision is to decide between a typical or a custom installation. A typical install installs everything, including various email scanners. If you want to limit what gets installed, choose the Custom option. I've selected the Typical option for the example. If you need to change the installation directory, you need to choose the Custom installation method.

That's all you need to do to install the virus scanning software. On the summary screen, click the Install button to proceed with the installation based on your selections.

After all of the files are copied and the installation completed, you'll get a status window that also allows you to update your software with the most recent patches and to run an on-demand scan of your system.

### Add spyware scanning to AntiVirus Enterprise 8.0i

I mentioned before that McAfee's antispyware scanning capability is actually an add-on to the virus scanning product. As such, you need to make sure you have successfully installed the antivirus product before you embark on your antispyware quest. McAfee has announced a stand-alone version of their spyware scanner that will not require AntiVirus Enterprise 8.0i. This will give you the option to use virus and spyware utilities from different companies, if you want. This stand-alone edition was just announced and was not available at this writing.

The AntiSpyware module is installed by executing the VSE80MAS.exe file from your McAfee AntiSpyware distribution media. The opening screen clearly states that this version enhances the capabilities of your antivirus product and installs as a module. There is no license screen in the product since it uses the antivirus product license. Click Next to continue with the installation.

That's all there is to it. The software installs and you are presented with a status screen. Click Finish on this screen.

You should run a full scan of your ePolicy Orchestrator system before continuing. You don't need to manually install these clients across the board. You can deploy using ePolicy Orchestrator later on.

## ePolicy Orchestrator

McAfee's ePolicy Orchestrator is a centralized management console that works in conjunction with all of McAfee's enterprise products. It is not bundled with the antivirus and antispyware software, though, and is a separate installation.

To get started installing ePolicy Orchestrator, run the setup.exe program from your ePolicy Orchestrator distribution media. The first screen, as usual, includes McAfee's product license agreement. Read it if you like, choose the Accept option, and click OK to continue.

You have two primary installation options with ePolicy Orchestrator. You can install both the ePolicy Orchestrator server and the management console, or you can install just the console. On the server side, you do need both components, but if you're just installing the management tools on an administrative workstation, choose the Install Console Only option. I'll be installing both components.

You also need to specify the folder into which you want to install ePolicy Orchestrator. The default location is C:\Program Files\McAfee. Click the Next button to continue.

ePolicy Orchestrator uses its own built-in administrative account and password for the initial log in to the ePolicy Orchestrator server. As such, in order to provide the maximum security, the installer asks that you provide this initial password. This is definitely preferable to every ePolicy Orchestrator installation being shipped with the same default password! On this screen of the installation, provide and confirm the password you want to use for this purpose. Click Next when you're done.

I mentioned earlier that ePolicy Orchestrator needs a database in order to work. ePolicy Orchestrator is bundled with Microsoft's MSDE product, which you can opt to install in this step by choosing the Install A Database Server On This

Computer And Use It option. Or, as I have done for this article, you can point ePolicy Orchestrator at an existing SQL Server (SQL Server 2000 SP3 or higher) installation. I've installed SQL Server 2005 on a server named W2K3-STD. To use this option, select Use An Existing Database Server On The Network and, with the drop-down arrow, choose the name of your network's SQL server. If you have installed SQL Server on the ePolicy Orchestrator computer, use the Use The Existing Database Server On This Computer option instead. Click Next when you're ready.

SQL Server works with either domain logins or logins created in SQL Server. For the installation, ePolicy Orchestrator needs an account that provides the rights necessary to create its database in SQL Server and to make updates to this database as part of the routine. I've opted to provide ePolicy Orchestrator with the SQL Server 'sa' account. When you're done, click Next.

ePolicy Orchestrator relies on the ubiquitous HTTP protocol for communication between consoles and agents. As such, you need to make sure that communication on specific ports is enabled. McAfee allows you to completely customize which ports you want to use. The only value I've changed for this example is the Agent-To-Server Communication Port. The default is 80, but I've changed this to 82 on the recommendation of the ePolicy Orchestrator installation guide. Click Next to continue.

If you want to be notified about specific events in ePolicy Orchestrator, you must provide an e-mail address to which notifications can be sent. The default is administrator@example.com. I happen to use the example.com domain in my lab as well, so I accepted this default. Click Next when you're done.

That's all the questions you need to answer. The final screen you see before the installation commences outlines the steps that the ePolicy Orchestrator installer will take to complete your product's installation. Note that there is a reboot step, so be prepared! If you're installing ePolicy Orchestrator on a production server, do it during a maintenance window. Click the Install button to begin the installation.

After the installation completes, you're presented with a summary window that provides you with options to start the management console and to create a desktop shortcut. Click Finish.

## ePolicy Orchestrator post-installation tasks

Once ePolicy Orchestrator is installed, you need to take care of some critical tasks that make the product actually work and that protect your organization's systems:

- Create the ePolicy Orchestrator directory.
- Install ePolicy Orchestrator agents on systems you wish to be managed by ePolicy Orchestrator.
- Tell ePolicy Orchestrator which products you want to manage via ePolicy Orchestrator.

### Create the ePolicy Orchestrator directory

I'm not going to go into great detail regarding the ePolicy Orchestrator directory, but will provide you with enough information to get started. Like Active Directory, the ePolicy Orchestrator directory is used to group objects in some logical way. By creating groups of computers, for example, you can apply different management policies to different systems in your organization. For example, for the Marketing group, you might want to scan their systems early in the morning during their regular team meeting while, for Engineering, you might want to scan their systems late at night.

ePolicy Orchestrator uses two different kinds of organizational units:

- **Sites:** A site is a top-level major group that can contain both computers as well as other sub-level groups (described next). Every site contains a group called "Lost&Found," which contains managed systems that ePolicy Orchestrator was unable to assign to a sub-level group (i.e. you installed the ePolicy Orchestrator agent to a system, but deleted that system from the directory without removing the agent).
- **Groups:** Like Sites, groups can contain nested groups, but every top-level *Group* belongs to a Site. Groups do not contain Lost&Found objects.

The ePolicy Orchestrator directory also uses the concept of inheritance to handle policy and rights propagation. Inheritance is enabled by default in ePolicy Orchestrator, but can be disabled.

I will be using two methods to populate and maintain my ePolicy Orchestrator directory for this article. First, I will use ePolicy Orchestrator's Active Directory Import Wizard to initially synchronize ePolicy Orchestrator with my existing Windows domain. As a part of the importation process, I will enable a task that routinely synchronizes ePolicy Orchestrator with my Active Directory domain.

I particularly like the synchronization features provided by ePolicy Orchestrator. One great thing about an enterprise directory is its inherent ability to be centrally managed. ePolicy Orchestrator/VirusScan/AntiSpyware, while they do add some maintenance burden to your IT staff, at least the IT staff does not need to manually maintain multiple directories!

Before you can synchronize anything, you need to log in to ePolicy Orchestrator. Do so by going to Start | All Programs | McAfee | ePolicy Orchestrator 3.6.0 Console. Once you're at the main ePolicy Orchestrator screen choose the Log On To Server option.

In the Log On To Server box, provide the password you specified during the installation of ePolicy Orchestrator. The default administrative user name is admin.

The initial synchronization is accomplished by right-clicking the Directory option under the name of your ePolicy Orchestrator server and selecting All Tasks | Import Active Directory Computers.

In short, you need to specify the following items when it comes to the importation and synchronization of Active Directory computers:

- To which ePolicy Orchestrator site do you want to import your AD information? You can only import to a site you create or to the Root site. For this example, I have not created any sites and will import my Active Directory computers to ePolicy Orchestrator's root.
- From which AD server would you like to pull computer information? You also need to provide the credentials for a user with rights to extract information from AD.
- From which AD *container* would you like to pull computer information? A default AD infrastructure uses the Computers container and many people created groups nested within this top-level container. I am using the Computers container for this example. Note that ePolicy Orchestrator will search through subgroups if you have created them in Computers. If you want to exclude a particular subgroup, click the Add button and browse for it.
- During what timeframe would you like the synchronization to take place? I've used the default, which specifies that synchronization will take place every night at midnight.

The final screen summarizes what ePolicy Orchestrator accomplished. Note that the two systems found—XPP1 and W2K-BASE—were placed into the Lost&Found group.

### Deploy ePolicy Orchestrator agents to manage systems

There are a ton of ways you can get an ePolicy Orchestrator agent on your desktops. You can use your normal enterprise software distribution method, for example, or you can use ePolicy Orchestrator itself.

To deploy an agent from within ePolicy Orchestrator, in the Directory find the target system (often found in Lost&Found). Right-click the system and select Send Agent Install from the shortcut menu. You can also deploy to an entire group by choosing Send Agent Install from the group's shortcut menu instead.

On the resulting screen—the Install Agent screen—choose the appropriate options and click OK. You do need to provide credentials for a user account with rights to install software on the target machine.

Note that the default settings deploy the client at midnight. I overrode this setting for this example by selecting the machine in the directory and choosing the Tasks tab in the right-hand pane. I opened the Deploy task and unchecked the Inherit option and enabled the task. Next, from the tasks Schedule tab, I changed the deployment to run immediately.

### Allow ePolicy Orchestrator to manage the VirusScan product and AntiSpyware module

ePolicy Orchestrator handles all updating and replication of software for your entire organization. Before this can happen, you need to tell ePolicy Orchestrator which software packages it should manage for your clients.

Click the Repository option in ePolicy Orchestrator. This opens a flowchart like screen that shows you how ePolicy Orchestrator propagates updates.

To add the VirusScan Enterprise 8.0i and AntiSpyware module packages, do the following. For each of the two products, you need to both add the package to the master software repository and add the package to the ePolicy Orchestrator server.

Click the Check In Package option. This starts a wizard. Browse to the location of the product's PkgCatalog.z file, usually located in the directory to which you extracted the contents of the product (i.e. AntiVirus Enterprise 8.0i). There is a separate package file for both the virus and spyware scanning products, which means that you need to go through this process twice—once for each product.

Likewise, you need to check in a .NAP (Network Associates Package) file to locate your ePolicy Orchestrator server. From the main Repository screen, choose Check In NAP. You will be presented with two options: Add New Software, or Add New Reports. I will add new software only. Locate the .NAP file for each product (again, perform this process once for each product) and follow the instructions. The software is then available for use.

Now, to see what your clients are using, from the Directory, select a client, or select a group (including the whole directory itself or a site). Notice that there are options available to configure policies for both antivirus and antispyware features.

### Modify policies

To change a policy, choose the Policy Catalog option from ePolicy Orchestrator and select the policy you'd like to modify. I'm not going to get very deep into this as ePolicy Orchestrator policies could be an entire series of articles all by itself.

However, suppose you wanted to modify the way that the end user sees the AntiVirus client. Perhaps you don't want them to even be able to see the McAfee icon in the system tray, for example. To change this policy, expand the VirusScan Enterprise 8.0.0 group and choose User Interface Policies and then click the policy name McAfee Default.

## Stopping spyware the McAffee way

When it comes to complexity, McAfee's antispyware solution takes the cake in that it's the most difficult to get up and running. However, with that difficulty comes extreme flexibility and scalability. I haven't touched one-tenth of the capabilities of ePolicy Orchestrator coupled with AntiVirus and AntiSpyware, but with these steps, you should be able to get your McAfee products going in a minimal way. ❖

# Category Report: Anti-Spyware

# 4

# Fast Facts: Anti-spyware report

*By Steven Pittsley, CNE*

Spyware. The term has been used to describe everything from tiny espionage cameras to miniature electronic tracking devices. Then techies adopted it as their own in 1999. Since then the term's been used to describe sinister software that infests computers and records user information. Virtually anyone who's used a computer in the last several years understands that spyware programs, like viruses, are a plague that impacts almost everyone connecting to the Internet.

Regardless of how well you police network nodes for the nefarious and obnoxious programs, spyware installations still find their way into organizations. Users are often the culprit, as they unwittingly download and install self-described helpful programs and toolbars.  In addition, new variations of spyware are often found lurking in shadows, at least until antispyware companies recognize the new form and create an equivalent inoculation.

As spyware and adware programs have matured, they have become increasingly difficult to remove. These applications no longer simply generate pop-up advertisements. Now, spyware programs track user surfing habits, slow system performance, compromise security, introduce Trojan horse worms, install keystroke loggers, hijack Internet browsers, and collect personal information (including credit card numbers, usernames, and passwords). The complexity and prevalence of spyware can potentially do more damage to the user and the user's computer than the majority of computer viruses.

Unlike computer viruses, spyware is a profitable business. Webroot Software Inc.'s Q1 2005 State of Spyware Report stated adware creates $2.4 billion in annual revenue. Companies, such as Claria (formerly Gator), have profited by creating and distributing adware applications. Claria, one of the largest adware firms, generated $35.6 million in profit on revenues of approximately $90.5 million in 2003 and even filed preliminary IPO documentation with the Securities and Exchange Commission.

With so much at stake for adware firms, it should come as no surprise vast numbers of vendors have joined the fight. Software manufacturers are introducing antispyware applications at a dizzying pace. Early pioneers in the emerging field, such as Lavasoft and Safer Networking, have been joined by the big guns at Computer Associates, McAfee, Symantec, and Microsoft, among others.

The market is there. According to a recent Forrester Research survey of 185 North American companies, 69 percent of large enterprises surveyed claimed plans to deploy antispyware applications in 2005.

As more companies join the fray, organizations and consumers are faced with a constantly increasing array of antispyware products and features. No single antispyware program removes all spyware variations. It is common to clean a system with one application, immediately run a spyware scan using a second antispyware program, and discover a multitude of additional infestations.

As you will see in the accompanying antispyware product comparison tables, each application possesses strengths and weaknesses. Typically, organizations leverage two or more products to protect against the wide variety of spyware programs active in the wild.

With such a bewildering array of products and features, determining which antispyware product to deploy enterprisewide, or for one-time use to eradicate a particular strain of spyware, proves challenging. Features and toolsets are becoming increasingly complex.

Eventually the market will consolidate. Acquisitions and mergers will likely help shape the landscape, too. Until then, organizations, information technology professionals, and consumers must all place their bets as to which products offer the best spyware defenses for their specific needs.

The accompanying comparison tables serve to simplify selection. These tables compare twelve leading antispyware products; these tables do not aim to rank or judge these products. Instead, the tables were built to objectively list manufacturer information, product attributes, and feature sets.

## Anti-spyware applications

The Anti-spyware Applications table (**Table A**) provides top line information about the twelve antispyware products included in this report. Most of the products are designed for corporate use, with the exceptions of Internet Cleanup, Spybot Search & Destroy, Spyware Doctor, and Spyware Eliminator.

Trend Micro's corporate product is Trend Micro Anti-Spyware For Small and Medium Businesses. However, the company claims the Trend Micro Anti-Spyware version "has shipped on more new PCs from major computer manufacturers than any other anti-spyware product," so that's the version covered by this report.

Many of these applications are intended for use on a single computer. Nevertheless, many are deployed on individual computers within corporate environments, which is why they are included in this comparison.

Note that listed prices are for corporate editions, when applicable. Thus, programs that might be free for individual, noncorporate users must be purchased if used on a corporate workstation. As with many corporate applications, the price for several antispyware packages is reduced as the volume of seats increases. Always be sure to review your antispyware program's license terms before deploying the software to ensure your organization's use is consistent with the software's licensing terms.

**Table A: Anti-spyware applications**

| Application | Company | Version | Price |
|---|---|---|---|
| Ad-Aware SE Plus | Lavasoft | 1.06 | $31.95 - $21.95 per seat |
| Anti-Spyware Enterprise | McAfee | 2.0 | $25.00 - $6.60 per seat |
| Anti-Spyware | Trend Micro | 3.0 | $29.95 |
| Antivirus Corporate Edition | Symantec | 10.0 | $44.95 - $17.95 per seat |
| Counterspy Enterprise | Sunbelt Software | 1.5.265 | $24.00 - $10.00 per seat |
| eTrust PestPatrol 2005 | Computer Associates | 5.0 | $39.95 |
| Internet Cleanup | Allume | 4.0 | $29.99 |
| Spy Sweeper Enterprise | Webroot | 4.0 | $29.95 |
| Spybot Search & Destroy | Safer Networking | 1.4 | Free / Donation Supported |
| Spyware Doctor | PC Tools | 3.2 | $29.95 |
| Spyware Elimator | Aluria Software | 4.0 | $29.99 |
| Windows Antispyware | Microsoft | 1.0 (Beta) | Not available; beta product |

## Spyware scanning

Anti-spyware packages should, at a minimum, scan the computer's memory, the system registry, and all attached drives. All packages in this comparison offer these features. In addition, all packages covered here permit users to create customized scans, which allow users to scan specific portions of drives. These four features (memory, registry, attached drives, and customized scans) have become de facto standards for all anti-spyware applications.

The final three columns in **Table B** indicate additional functions most anti-spyware applications provide. Configuring prescheduled scans for specific drives is a helpful feature that enables users to regularly scan systems during low usage periods. This feature is extremely important in corporate environments where downtime must be minimized. The ability to schedule scans for system starts is important, as many stubborn spyware applications cannot be removed while running. Many require rebooting to ensure complete removal.

## Spyware prevention

Most modern antispyware programs contain a resident component that actively prevents spyware applications from being installed on active systems. This is particularly important, as it is more difficult to remove an existing infestation than automatically prevent a new infection.

**Table B: Spyware scanning**

| Application | Memory | Registry | Drive | Custom | Scheduled | System Start | Remove on Reboot |
|---|---|---|---|---|---|---|---|
| Ad-Aware SE Plus | X | X | X | X | X | X | X |
| Anti-Spyware Enterprise | X | X | X | X | X |  | X |
| Anti-Spyware | X | X | X | X |  | X | X |
| Antivirus Corporate Edition | X | X | X | X | X | X | X |
| Counterspy Enterprise | X | X | X | X | X | X | X |
| eTrust PestPatrol 2005 | X | X | X | X | X |  | X |
| Internet Cleanup | X | X | X | X | X | X | X |
| Spy Sweeper Enterprise | X | X | X | X | X | X | X |
| Spybot Search & Destroy | X | X | X | X |  | X | X |
| Spyware Doctor | X | X | X | X | X | X | X |
| Spyware Elimator | X | X | X | X | X | X |  |
| Windows Antispyware | X | X | X | X | X |  | X |

**Table C: Spyware prevention**

| Application | Memory Processes | Browser Hijack | Startup Settings | HOSTS File | ActiveX | Restricted Sites |
|---|---|---|---|---|---|---|
| Ad-Aware SE Plus | X | X | X | | | |
| Anti-Spyware Enterprise | X | X | X | X | | |
| Anti-Spyware | X | X | | | | |
| Antivirus Corporate Edition | X | X | X | | | |
| Counterspy Enterprise | X | X | X | X | X | |
| eTrust PestPatrol 2005 | X | | | | | |
| Internet Cleanup | X | | X | | X | X |
| Spy Sweeper Enterprise | X | X | X | X | | |
| Spybot Search & Destroy | X | X | X | X | X | X |
| Spyware Doctor | X | X | X | X | X | X |
| Spyware Elimator | X | X | X | | X | |
| Windows Antispyware | X | X | X | X | X | |

All of the programs in this comparison scan system memory for spyware modules. As you can see in **Table C**, this is another de facto standard that is a requisite component of any solid antispyware initiative.

Browser hijacking programs perform a number of irritating functions, including changing the browser's home page and rerouting popular search engine sites to different locations that help power adware networks. Browser hijacking programs are becoming much more prevalent, and preventing them should be considered a priority when choosing an antispyware application.

Many spyware applications modify the system's startup settings to ensure the spyware application is automatically launched when the system starts. Preventing changes to the startup settings is another important feature to seek when selecting an antispyware application.

The Windows Hosts file maps IP addresses to host names. This file is loaded into memory when Windows starts, and it is checked before querying DNS servers when resolving Internet addresses. Preventing changes to this file is a helpful feature that can guard against one form of DNS poisoning.

Spyware frequently installs through an ActiveX plug-in when the browser opens. Several programs in this comparison prevent these plug-ins from executing by preemptively blocking specific ActiveX controls using kill bits for known spyware applications.

Restricting sites, or blocking installations from a black list of sites, is a unique feature employed by a few of the products in this comparison. This is a popular feature of Spybot Search & Destroy, and it is one reason for this program's popularity (it's price—donations requested—being another).

## Centralized administration

For network administrators, a centralized administration console makes managing an antispyware application much more efficient by easing deployment, configuration, and management tasks. This is especially true in large or geographically diverse organizations, where individual management of each workstation isn't practical or cost efficient.

While remote control software offers some degree of additional management functionality, it only provides for individual workstation management from other locations, such as a centralized administrative office. In larger organizations, having to manually configure each workstation, even remotely, proves impractical. Centralized administration tools, shown in **Table D**, allow for large scale deployment, updates, and configuration of antispyware applications on computers connected to the enterprise network.

Remote deployment allows administrators to install an antispyware application on a client computer without physically visiting the workstation. Such a tool is

**Table D: Centralized administration**

| Application | Remote Deployment | Program Updates | Definition Updates | Monitor Log Files | Remote Scanning | Remote Scheduling |
|---|---|---|---|---|---|---|
| Ad-Aware SE Plus |  | X | X | X | X | X |
| Anti-Spyware Enterprise | X | X | X | X |  |  |
| Anti-Spyware |  |  |  |  |  |  |
| Antivirus Corporate Edition | X | X | X | X | X | X |
| Counterspy Enterprise | X | X | X | X | X | X |
| eTrust PestPatrol 2005 | X | X | X | X | X | X |
| Internet Cleanup |  |  |  |  |  |  |
| Spy Sweeper Enterprise |  | X | X |  | X | X |
| Spybot Search & Destroy |  |  |  |  |  |  |
| Spyware Doctor |  |  |  |  |  |  |
| Spyware Elimator |  |  |  |  |  |  |
| Windows Antispyware |  |  |  |  |  |  |

invaluable in geographically diverse organizations, especially when deploying the software to a number of computers simultaneously.

The ability to push antispyware program updates to client computers makes short work of this task when new application versions are released, which is often. Once again, such a tool is invaluable in geographically diverse organizations, especially when managing a large number of computers in numerous locations.

Antispyware applications are only as good as their last update, of course. If the spyware definition files are not kept current, the program will be unable to remove or defend against the latest variety of spyware. Centralized administration tools allow administrators to push these updates to all of the systems on the network simultaneously. In large organizations, such a tool is virtually a requirement.

The ability to generate and monitor log files from a centralized management console allows network administrators to determine which computers on the network have experienced spyware-related problems, as well as the nature of those problems. Not only does such functionality help pinpoint problem machines, it can also help reveal which users are particularly susceptible to infestation and who might benefit from a lunch-and-learn-style training session or refresher prevention course.

Remote scanning and remote scheduling tools allow network administrators to initiate and schedule scans using the centralized administration console. Such functionality is, again, advantageous when these tasks must be performed on multiple systems.

## Diagnostic tools

The diagnostic tools compared in **Table E** allow for the searching and removal of the problems described in Table C, such as might be required on unprotected systems or systems with outdated antispyware signatures, that have accessed the Internet.

Diagnostic tools work by allowing you to examine specific system aspects for signs of spyware infestation. When signature matches are found, the antispyware application can take the appropriate steps to remove the infestation. Feature distribution among leading antispyware programs varies, as illustrated in this table, but certainly the more of these tools you have at your disposal the better.

Two of the more important tools included in many antispyware applications are the ability to examine browser settings and system startup locations. These two areas tend to be the most troublesome spyware playgrounds.

One feature exclusive to this table is the ability to repair the Winsock Layered Service Provider (LSP) interface. This feature can be extremely helpful if the Winsock LSP chain is damaged by a spyware application. When this occurs, the Winsock LSP chain is broken and the user will prove unable to access the Internet until the error is corrected.

**Table E: Diagnostic tools**

| Application | BHOs | ActiveX Conrols | Browser Settings | Startup Locations | HOSTS File | Winsock LSPs |
|---|---|---|---|---|---|---|
| Ad-Aware SE Plus | | | X | | | X |
| Anti-Spyware Enterprise | | | X | X | | |
| Anti-Spyware | | | | | | |
| Antivirus Corporate Edition | | | | | | |
| Counterspy Enterprise | X | X | X | X | X | X |
| eTrust PestPatrol 2005 | | | | | | |
| Internet Cleanup | | X | | X | | |
| Spy Sweeper Enterprise | | | X | X | X | |
| Spybot Search & Destroy | X | X | X | X | X | X |
| Spyware Doctor | X | | | | | |
| Spyware Elimator | X | X | X | X | | |
| Windows Antispyware | X | X | X | X | X | X |

**Table F: Updates**

| Application | Manual | Scheduled | Program Start |
|---|---|---|---|
| Ad-Aware SE Plus | X | | X |
| Anti-Spyware Enterprise | X | | X |
| Anti-Spyware | X | | X |
| Antivirus Corporate Edition | X | | X |
| Counterspy Enterprise | X | X | X |
| eTrust PestPatrol 2005 | X | | X |
| Internet Cleanup | X | | X |
| Spy Sweeper Enterprise | X | X | X |
| Spybot Search & Destroy | X | | X |
| Spyware Doctor | X | X | X |
| Spyware Elimator | X | X | X |
| Windows Antispyware | X | X | X |

## Updates

Antispyware applications, like antivirus programs, are only as good as their latest update. If spyware definition files are not kept current, the program will be unable to remove or defend against the latest variety of spyware infestations.

All programs listed in **Table F** provide support for configuring regular updates. These programs also provide an option to search for updates whenever the program starts. In most cases, any updates that are found require manual installation.

Some programs provide support for scheduling updates, enabling automatic location and installation of update files.

## Supported operating systems

Lastly, all of the antispyware programs featured in this comparison are fully compatible with Windows XP and Windows 2000. As illustrated in **Table G**, many antispyware programs do not support legacy operating systems, such as Windows NT, Windows ME, Windows 98, and Windows 95. If these legacy systems are still used within your organization, be sure to consider a platform that will protect those nodes, as well. ❖

**Table G: Supported operating systems**

| Application | Windows XP | Windows 2000 | Windows NT | Windows ME | Windows 98 | Windows 95 |
|---|---|---|---|---|---|---|
| Ad-Aware SE Plus | X | X | X | X | X |  |
| Anti-Spyware Enterprise | X | X | X |  |  |  |
| Anti-Spyware | X | X |  | X | X |  |
| Antivirus Corporate Edition | X | X |  |  |  |  |
| Counterspy Enterprise | X | X |  | X | X |  |
| eTrust PestPatrol 2005 | X | X | X | X | X |  |
| Internet Cleanup | X | X |  | X | X |  |
| Spy Sweeper Enterprise | X | X |  |  |  |  |
| Spybot Search & Destroy | X | X | X | X | X | X |
| Spyware Doctor | X | X |  | X | X | X |
| Spyware Elimator | X | X | X | X | X |  |
| Windows Antispyware | X | X |  |  |  |  |

## Notes:

# 5 Phishing and Pharming

# 10 things you should do to a new PC before surfing the Web

*By Mark Kaelin*

It is only natural that when you get a brand-new PC, especially one with broadband capabilities built in, you want to connect to the Internet and see it in action. For many, the browser and the World Wide Web are the "killer-apps" of the modern PC—the Internet is what you have a PC for, everything else is just extra fluff.

However, connecting to the Internet with a new unprotected and unpatched PC is practically inviting the nefarious and malicious to infect your PC. According to research published by Sophos in July 2005 (**http://www.sophos.com/pressoffice/pressrel/uk/midyearroundup2005.html**), there is about a 50 percent chance that an unpatched PC will be infected with malicious software within 12 minutes of connecting to the Internet. Once infected, it is almost impossible to get a PC clean again without completely re-installing the operating system. (We are restricting this conversation to Windows PCs for the moment.)

To prevent the frustration that comes with re-installing Windows, you should take the necessary steps to update, configure, and patch your new PC. Keep in mind that no matter how new your PC is, it will most likely need patching and it will definitely need to be properly configured. Here are 10 basic things you should do before attaching the Internet to a new PC.

## 1. Make a starter CD-ROM

Before you disconnect your old computer, take a few minutes to burn a starter CD-ROM that contains the latest version of your favorite anti-virus software. I prefer to keep this simple and inexpensive by using AVG from Grisoft, but if you like Norton or McAfee those will work just as well.

To save time later, you should put other security applications on this disk like Spybot Search & Destroy, AdAware, etc. It would also be a good idea to include any updated drivers you might need—drivers for your video card for example. Just like Windows, your video card drivers are likely to be a little old also. You should also put drivers on this disk for peripherals that you will be connecting to your new PC, like cameras, scanners, printers, and game interface devices. Having all of these device drivers residing on a single CD-ROM means you will not have to go to the Internet to retrieve them as you set up your new PC.

## 2. Remove the promotional apps

After going through the initial setup process where Windows identifies devices you may be asked to register and/or activate your copy of the Windows operating system—hold off on that for now, you can always do that later. The first thing to do is to clean up the mess that shipped in your PC. You should remove all of the promotional and trial software that you do not intend to use from your new PC. This is usually the first thing I do, because invariably one of those apps will ask if I want to activate it or register it—a process that usually involves accessing the Internet. (Some times they don't ask—they just assume I want them on my pristine PC.) At this point you should have no connection to the Internet at all, wireless or not.

The applications to be deleted are usually ISP's advertisements like AOL and Earthlink, an antivirus app from a competitor of your current application (something you should already have ready on your CD-ROM), trial versions of Money or Quickbooks, etc. If you are not going to use these, go to the Add/Remove Programs applet in the Control Panel and remove them completely.

## 3. Install antivirus software

Install the antivirus software that you burned onto a CD-ROM in step 1. The assumption is that any PC purchased after this document is published will have Windows XP SP2 installed, but if SP2 is not installed, you could have that update ready on your disk too. In fact, if you know how, you could have some of the more important Windows patches and updates on your disk also. This would be a good time to install anti-spyware software too.

## 4. Turn on a software firewall

Windows XP SP2 comes with a modest but still useful software firewall. Before you start surfing the Internet you should turn it on—or you can install an alternative third-party software firewall like Zone Alarm. Any alternative firewalls should have been included on the startup CD-ROM you made in Step 1.

## 5. Install printers and other peripherals

Before you connect to the Internet it is a good idea to install your other peripherals to your new PC. Performing this step means that when you do connect to the Windows update page, it will see your devices and make suggestions for new Microsoft-tested (WHQL) drivers if they are available.

## 6. Establish a password for the administrator account

One of the most glaring security vulnerabilities in any new Windows-based PC is that it ships with a wide open administrator access to the root directory. You never want anyone but you to have unfettered access to the admin settings on your PC. And while a password could easily be bypassed by a skilled cracker, it will deter the less determined intruder.

## 7. Create a new user account with password

This is almost as equally important as password protecting your administrator account. For general day-to-day activities, you do not want to be using your admin account. Instead, you should be using a user account that is also password protected (a password that is different than the one you are using for the admin account, please). This adds another layer of protection for your new PC because a user account does not have the same all-access permissions as an admin account. In some cases, malicious software will be thwarted by this level of permissions restriction alone.

## 8. Turn off unnecessary Windows services

Microsoft has been doing a better job of this with the release of SP2, but there are still numerous unnecessary Windows services and processes running by default on most PCs. If you'd like to see how many there are just perform the three finger salute (CTRL-ALT-Delete), click Task Manager and then select the Processes tab. All of those applications, services, processes, etc. are operating in the background on your PC. The problem is that many can actually open access to your PC to the outside world without your knowledge or active consent. That access is usually justified for what the process is supposed to be doing, it is just that many times your PC doesn't need that process at all—Web servers, network messengers, debuggers—are all processes you probably don't need on your personal PC. (Check out this TechRepublic download **http://techrepublic.com.com/5138-10877-5747817. html** for an in-depth examination of these services and for some suggestions for which can be deactivated.)

## 9. Establish a system restore point

Now that you have performed the first eight steps you should take a moment to establish a system restore point. To manually create a Restore Point, you launch the System Restore utility by clicking Start | All Programs | Accessories | System Tools | System Restore and then follow the steps in the wizard. This step will establish a fall-back point if something happens to go haywire later.

## 10. Install and configure a router

This last step may seem like an unnecessary added expense to some, but in this age of viruses, worms, and other nasty Internet infections, a router standing between you and the outside world coming at you at broadband speeds offers another significant layer of protection. Connecting a PC directly to the Internet means that PC gets its own IP address, which means it can be seen by every sleazebag with malicious intent. By adding a router to your broadband setup, the router gets the visible IP address and gives your new PC an internal address. In addition, routers have hardware firewalls and other features that help block the bad guys before they get to your new PC.

This is especially helpful because the first thing you should do when you do actually connect to the Internet is head directly for Windows Update. This is the most important tip in this guide—the only place you should be heading on the Web when you first connect your PC to the Internet is the Windows Update page. You will not have time to check movie times or football scores. The 12-minute countdown to possible infection starts as soon as you connect. ❖

# 12 steps to avoid phishing scams

*By Steven Warren, MCSE, MCDBA*

Some computer users (and even some IT professionals) have been confused about the defition of a "phishing" attack. What exactly is a phishing attack? A phishing attack is when you receive an official-looking e-mail from an online banking or financial institution—it could even be eBay or PayPal, or any other service that deals with money. The e-mail states that you should click a link and confirm your login and password to this particular institution (or enter your account number or credit card number).

As soon as you click on the link, you are sent to a Web page that looks remarkably similar to the company's real Web site, but it's not the company's real Web site. What is happening is that you are sent to a fake page that is controlled by the criminal who is behind the phishing scheme. As soon as you type your login\password or account information or credit card number, the thieves or hackers capture the information and then commit identity theft by using your credit card or stealing money from your account. Below are 12 steps that users can take to keep from being victimized by phishing scams. And after that are some examples of phishing scams.

1. **Keep antivirus up to date**—One of the most important things you can do to avoid phishing attacks is to keep your antivirus software up-to-date because most antivirus vendors have signatures that protect against some common technology exploits. This can prevent things such as a Trojan disguising your Web address bar or mimicking an https secure link. If your antivirus software is not up-to-date, you are usually more susceptible to attacks that can hijack your Web browser and put you at risk for phishing attacks.
2. **Do not click on hyperlinks in e-mails**—It is never a good idea to click on any hyperlink in an e-mail, especially from unknown sources. You never know where the link is going to really take you or whether it will trigger malicious code. Some hyperlinks can take you to a fake HTML page that may try to scam you into typing sensitive information. If you really want to check out the link, manually retype it into a Web browser.
3. **Take advantage of anti-spam software**—Anti-spam software can help keep phishing attacks at a minimum. A lot of attacks come in the form of spam. By using anti-spam software such a Qurb, you can reduce many types of phishing attacks because the messages will never end up in the mailboxes of end users.
4. **Verify https (SSL)**—Whenever you are passing sensitive information such as credit cards or bank information, make sure the address bar shows "https://" rather than just "http://" and that you have a secure lock icon at the bottom right-hand corner of your Web browser. You can also double-click the lock to

guarantee the third-party SSL certificate that provides the https service. Many types of attacks are not encrypted but mimic an encrypted page. Always look to make sure the Web page is truly encrypted.

5. **Use anti-spyware software**—Keep spyware down to a minimum by installing an active spyware solution such as Microsoft Antispyware and also scanning with a passive solution such as Spybot. If for some reason your browser is hijacked, anti-spyware software can often detect the problem and provide a fix.
6. **Get educated**—Educate yourself on how to prevent these types of attacks. A little research on the Internet may save you a great deal of pain if you are ever the victim of identity theft. You can report any suspicious activity to the FTC (in the U.S.). If you get spam that is phishing for information, forward it to spam@uce.gov. You can also file a phishing complaint at www.ftc.gov. Another great resource is the FTC's identity theft page to learn how to minimize your risk of damage from ID theft. Visit the FTC's spam page to learn other ways to avoid e-mail scams and deal with deceptive spam (**http://www.ftc.gov/spam**).
7. **Use the Microsoft Baseline Security Analyzer (MBSA)**—You can use the MBSA to make sure you have all of your patches up to date. You can download this free tool from Microsoft's Web site (**http://www.microsoft.com/technet/security/tools/mbsahome.mspx**). By keeping your computer patched, you will protect your systems against known exploits in Internet Explorer and Outlook (and Outlook Express) that can be used in phishing attacks.
8. **Firewall**—Use a desktop (software) and network (hardware) firewall. On the desktop, you can use a software firewall such as Zone Alarm or use Microsoft's built-in software firewall in Windows XP. The incorporation of a firewall can also prevent malicious code from entering your computer and hijacking your browser.
9. **Use back-up system images**—Keep a back-up copy or image of all systems in case of foul play. You can then revert back to a pure system state if you suspect that a phishing attack, spyware, or malware has compromised the system. Tools such as Symantec Ghost and Acronis True Image are perfect for this.
10. **Don't enter sensitive or financial information into pop-up windows**—A common phishing technique is to launch a bogus pop-up window when someone clicks on a link in a phishing e-mail message. This window may even be positioned directly over a window you trust. Even if the pop-up window looks official or claims to be secure, you should avoid entering sensitive information because there is no way to check the security certificate. Close the pop-up windows by clicking on the X in the top-right corner. Clicking cancel may send you to another link or download malicious code.

11. **Secure the hosts file**—A hacker can compromise the hosts file on desktop system and send a user to a fraudulent site. Configuring the host file to read-only may alleviate the problem, but complete protection will depend on having a good desktop firewall such as Zone Alarm that protects against tampering by outside attackers and keeps browsing safe.
12. **Protect against DNS pharming attacks**—This is a new type of phishing attack that doesn't spam you with e-mails but poisons your local DNS server to redirect your Web requests to a different Web site that looks similar to a company Web site (e.g. eBay or PayPal). For example, the user types in eBay's Web address but the poisoned DNS server redirects the user to a fraudulent site. This is what I consider new age phishing. This needs to be handled by an administrator who can use modern security techniques to lock down the company's DNS servers.

## What does a phishing e-mail scam look like?

As the technologies get better and better, the people behind the phishing scams also become more devious. They now use pop-up windows, official logos, and mock-secure connections copied from actual Web sites.

The link in a phishing scam e-mail I recevied recently, purportedly goes to eBay, but actually goes somewhere else. When I mouse over it, I can see that this text is actually masking a link to another site (66.246.90.60). Also, note that the original link text does not have an "https://" secure address, but if a link like this read "https://" you might think it was safe while it could actually be masking a fake, non-secure URL.

## What does a hijacked browser scam look like?

When your browser is hijacked in a phishing attack, the real address bar is suppressed and is spoofed using Javascript and frames.

When the user enters a URL into the address bar, the frame retains control and the hacker can gain information from you. A simple pop-up blocker will keep this attack from working or from closing the current session of your browser. ❖

# Take steps to prevent phishing attacks by using best practices when selecting URLs

*By John McCormick*

Phishing attacks are on the rise, but do your organization's URL naming practices help protect customers or help the attackers?

## Details

March has been an incredibly slow month, and I'm not complaining. It's wonderful to have a rest from installing emergency patches and fighting increasingly more virulent malware.

But of course, this unexpected lull gives me the chance to think about some important topics that I usually don't have the time for, such as proactive steps I can take to strengthen my organization's security.

Several recent high-profile security breaches have caused enough of a stir that many companies are reevaluating their potential liability and their security best practices. If your company isn't already discussing this, there's no better time than the present.

The big news focuses on ChoicePoint, a company that most people had never heard of until recently. The company wound up answering some rather tough questions at a congressional hearing (**http://techrepublic.com.com/2100-10595_11-5621496.html**). However, while the 145,000 stolen records have been a high-profile story, it hasn't been the only one. Other major problems include:

- Hackers may have gained access to 59,000 personal records of staff, students, and even potential students that were on a supposedly secure server at Cal State Chico.
- LexisNexis lost control of 32,000 personal records.
- The Discount Shoe Warehouse (DSW) announced that hackers had compromised credit card records for 103 of its 175 stores.
- Someone accessed a University of California San Diego (UCSD) computer system that held data on nearly 400,000 people.
- Someone accessed 178,000 personal records on San Diego State University computers, leading to a number of identity theft cases.

Everyone knows that phishing attacks are on the rise, but virtually all the advice for combating attacks has been on the user side of the equation. Examples include warning users not to click links in e-mails and telling them to make sure a site's URL as listed in the browser is legitimate.

But what about the Web site owner's responsibility in all of this? Some sites prominently post an easy way for customers to notify the business of phishing attempts, but is that sufficient? Do certain poor practices actually contribute to phishing attacks either by making a site easier to fake or by making the URL so confusing that even regular visitors can't tell whether a Web site is legitimate?

Many companies use different top-level domain (TLD) names to simplify the development and maintenance of Web sites, but they often do this without giving much thought to how it affects customers. So what difference does it make if a URL is long and complex or uses some internal company shorthand to make things simpler for the Webmaster? In fact, it can make a big difference. Let's look at an example.

Let's say the XYZZ Company uses www.xyzzcompany.com as its main Web site, but it uses www.xyzzcompany-purchase.com or www.secure-xyzzcompany.com as the address of its online store.

While this may seem simple enough, consider what happens to customers when they surf the site and the URL keeps changing, in what probably seems to be a random fashion. If this is the case, how can you expect customers to differentiate between a phishing site and a legitimate one by the URL?

Let's look at some best practices for naming URLs. To begin with, always keep your TLD the same if at all possible. In other words, make it easy for visitors to determine whether they're at a legitimate site by always showing the same beginning text in the URL. So, for our example company, a better choice for the online store's URL would be www.xyzzcompany.com/secure or www.xyzzcompany.com/purchase.

A white paper from NGS Software Ltd. offers the following advice for companies with an international presence (**http://www.ngssoftware.com/papers/NISR-BestPracticesInHostURLNaming.pdf**). Let's say our company also has a branch in the United Kingdom or maybe conducts a lot of business there. It seemingly makes sense to buy www.xyzzcompany.co.uk, if only to keep some competitor or prankster from grabbing it. However, using one foreign-based URL could help convince visitors to accept a fake URL, such as www.xyzzcompany.co.au.

To prevent this occurrence, the company could buy every possible URL, which may or may not be feasible. Or, it could use automatic redirection so visitors entering www.xyzzcompany.co.uk would access the site either from the main site (www.xyzzcompany.com) or from www.xyzzcompany.com/UK.

In addition to making it easier for visitors to determine the site's legitimacy, you can also take other steps to help harden your site. For example, we've all visited sites that generate long, complex URLs as you navigate your way through a session.

Many of these include some session-specific data in the URL where anyone can see it—and learn something about how your site security works. Organize your Web site to make the displayed address as short as possible, containing as little information as possible that could aid hackers.

## Final word

This applies to all businesses that have any sort of secure information on their Web site or require visitors to use passwords (or even cookies) to access various features. Of course, it applies a hundred times over to any company that has an online store or that provides confidential information to visitors.

If there is any possibility someone might want to try some phishing among your customers or even staff, then your organization must make it easier for visitors to know they've reached a legitimate site. ❖

# Why phishing isn't just a crime against individual users

*By John McCormick*

## The "governator" goes phishing

While phishing (**http://techrepublic.com.com/5138-1009-5731546.html**) may appear to be a threat that primarily affects individual users, it also poses a major problem for businesses, both directly and indirectly. The goal of most phishing attacks is to obtain personal information from an individual.

However, some scams are beginning to target business credit information—companies are often a better target because they have more money. Businesses are accustomed to paying an invoice when they get it without doing much research. In fact, this is an old scam: Just mail out a bunch of invoices using a professional-sounding name, and many companies will just send a check. This means that even seemingly harmless information about billing cycles and sample invoices can pose a threat.

As phishing increases, consumers are becoming more leery about giving out personal information online, which negatively affects confidence in online buying—just as companies are turning to the Internet for an increasingly significant proportion of their sales. This change in attitude is having a measurable impact. According to Forrester Research, 600,000 online banking users in the United Kingdom have turned their backs on online banking due to the phishing threat (**http://www.vnunet.com/computing/news/2142004/users-desert-online-banks**).

And according to BBC, 90 percent of American PC users have changed their online habits due to a fear of spyware (**http://news.bbc.co.uk/1/hi/technology/4659145.stm**). This includes changing browsers, dropping file-sharing software, and even avoiding some Web sites.

Given that number, how can this fail to affect online sales? Any way you look at it, this can't be good news for companies.

In an effort to fight back, California recently became the first state to actually make phishing a crime that you can sue over. On Sept. 30, 2005, Governor Arnold Schwarzenegger signed the nation's first anti-phishing bill (**http://www.informationweek.com/story/showArticle.jhtml?articleID=171202672**). As hard as it may be to believe, until the new law went into effect, there was little or nothing you could do about phishing—even if you caught someone red-handed trying to steal your personal information.

The California Anti-Phishing Act of 2005 finally made it a civil offense to take any action to induce people to disclose personal data by falsely representing themselves as doing so for a business. The law included fines of $2,500 for each violation, and it lets victims sue for actual damage or $500,000 per violation, whichever is greater.

But the new California law is too narrow in its definition of phishing, and it doesn't apply to malware-based phishing. In addition, it poses little if any concern for any attacker not based in the state. However, it may trigger action in other states as have other pioneering California privacy laws.

U.S. Senator Patrick Leahy introduced a similar bill to Congress in February 2005 (**http://leahy.senate.gov/press/200503/030105.html**), but the proposal has received little attention. Leahy's proposed bill would make it a federal crime even to create a fake business site that spoofs a legitimate business or to attempt to obtain personal information via e-mail. The bill provides specific protection for parody sites and includes other First Amendment protection.

And while the number of new security vulnerabilities and serious virus threats has remained very low recently, two-thirds of companies have suffered "significant" financial costs associated with IT failures in the last year, according to Silicon.com. One-third suffered damage due to direct phishing and hacking attacks (**http://software.silicon.com/security/0,39024655,39153094,00.htm**).

## Microsoft gets serious about security

For the past few years, the Redmond giant has been concentrating on plugging security holes in its products. However, industry insiders have been waiting for the company to enter the lucrative security field ever since Microsoft began acquiring security companies. Last week, Microsoft announced plans to release its business-oriented Client Protection software, which will put it into direct competition with Symantec and other security specialists.

While few details are available, we do know that it will integrate with Active Directory. Client Protection is the business equivalent of Windows OneCare, Microsoft's subscription-based end-user repair software. The new Client Protection software will ship in 2006, and testing will begin later this year. You can also look for the full working version of Windows OneCare to arrive next year, and it's currently in limited beta release.

Even if it isn't perfect, security software provided by Microsoft should help slow the spread of some viruses. That's because far more PCs will likely have the protection implemented than the excellent third-party antivirus tools already available today.

## Recent threats

- A Wi-Fi vulnerability has surfaced in fully patched Windows XP Service Pack 2 systems (**http://www.soonerorlater.hu/index.khtml?article_id=62**). The hole in the Wireless Zero Configuration service is a local threat that can allow a user to gain higher privileges.
- A highly critical vulnerability has emerged in Kaspersky Anti-Virus programs (**http://techrepublic.com.com/2100-1009_11-5887857.html**). See the Secunia report for more details (**http://secunia.com/advisories/17024/**).
- Red Hat has announced updates for Thunderbird (Enterprise Linux AS4, ES4, and WS4) that fix remote spoofing and other vulnerabilities (**http://secunia.com/advisories/16175/**).

## Final word

Reports about people changing their surfing habits should concern any business that's selling online. Phishing and spyware don't just affect unsophisticated individuals—they also have a financial impact on those who want to do business with them. ❖

# ‘Puddle phishing’ comes to small banks and local credit unions

*By Mark Vernon*

Many large banks are all too familiar with the problem of phishing: customers receive an e-mail, as if from the bank, asking for logons and passwords and other personal information. The financial services sector typically accounts for four out of every five phishing attacks. But no matter how many times banks tell customers to take no notice of e-mails purporting to come from the bank, the scam continues to fool the unwary.

Phishing scams are increasingly being directed at smaller, more targeted firms, including local banks and credit unions. Websense, a provider of employee Internet management solutions, has coined the term *puddle phishing* to describe this latest security development. The company warns that the customers of small financial institutions are being targeted.

Websense monitors 50 million URLs per day, searching for Web sites infected with malicious code, such as spyware and phishing dummies. Earlier this year, it reported that more than 13,000 infected sites were discovered in the first quarter of 2005 alone. They have seen a growing number of small credit unions falling foul of this latest development: more than 30 since the beginning of the year. Dan Hubbard, senior director of security and technology research at Websense, reports that one of the community banks recently under attack operates only 11 branches. Researchers also noted that a credit union that serves employees and staff of the White House was also hit with a phishing scam.

## Customers and users still need education about e-mail scams

The concern is that puddle phishing, presumably, works. When a bank has millions of customers, it only takes a fraction of one percent to oblige for the fraud to succeed (according to Websense, around four percent of polled individuals have fallen for a phish at least once, and clicked a link to a fraudulent Web site while at work). If phishing is working when customers are numbered only in the thousands, then it suggests that widespread efforts and news stories that might educate customers as to the dangers of such online risks are not getting through (**http://techrepublic.com.com/2100-1009_11-5807779.html**).

“The fact that we are seeing more and more of the smaller financial outlets being targeted by phishing attacks may indicate that this is a highly profitable scam,” continues Hubbard.

On the other hand, it could be that the customers of larger banks are now wising up to the fake e-mails, whereas those of smaller banks are not—perhaps thinking that the smaller institutions are more likely to use e-mail as a personal means of communication. Hubbard thinks this is unlikely, though, since according to another recent study, two-thirds of bank employees polled said that they had never even heard of phishing.

Puddle phishing represents a potentially serious problem for smaller banks to combat. The difficulty is that it is more or less impossible for banks to stop spam being sent out as if from a valid e-mail. And it is often easier to imitate the Web sites of smaller institutions.

Websense says that although the specific size of the financial institution being targeted is a new phenomenon, the phishing method used by the attackers has not changed. Typically, the e-mail is still delivered as if it were from a legitimate financial institution and contains a message that threaten users' accounts being deactivated, blocked, or restricted in some way if they do not update their personal account information.

End users are instructed to visit a Web site where they are prompted to enter confidential information such as ATM pins, credit card numbers, Social Security numbers, or e-mail addresses. "The attack style and dynamics are very similar on many of these recent puddle phishing attempts, which may mean that there is some tool sharing or a small amount of attackers behind this recent wave," Hubbard explains.

One of the only ways banks can help prevent phishing exploits is to continue to educate customers about the threat. For example, the American Bankers Association provides a series of brochures describing different scams and identity theft methods (**http://www.bankstuffers.com/sec2.html**) that can be stuffed inside statements or displayed at the banking locations. The Web site also provides a list of other anti-phishing resources to help banks combat e-mail scams (**http://www.aba.com/About+ABA/phishing.htm#Resources**). ❖

# DNS servers—an Internet Achilles' heel

*By Joris Evers, CNET News*

In a scan of 2.5 million so-called Domain Name System machines, which act as the White Pages of the Internet, security researcher Dan Kaminsky found that about 230,000 are potentially vulnerable to a threat known as DNS cache poisoning.

"That is almost 10 percent of the scanned DNS servers," Kaminsky said in a presentation last week at the Black Hat security event in Las Vegas. "If you are not auditing your DNS servers, please start," he said.

The motivation for a potential attack is money, according to the SANS Internet Storm Center, which tracks network threats. Attackers typically get paid for each spyware or adware program they manage to get installed on a person's PC.

Information lifted from victims, such as social security numbers and credit card data, can also be sold. Additionally, malicious software could be installed on a PC to hijack it and use it to relay spam.

The DNS servers in question are run by companies and Internet service providers to translate text-based Internet addresses into numeric IP addresses. The cache on each machine is used as a local store of data for Web addresses.

In a DNS cache poisoning attack, miscreants replace the numeric addresses of popular Web sites stored on the machine with the addresses of malicious sites. The scheme redirects people to the bogus sites, where they may be asked for sensitive information or have harmful software installed on their PC. The technique can also be used to redirect e-mail, experts said.

As each DNS server can be in use by thousands of different computers looking up Internet addresses, the problem could affect millions of Web users, exposing them to a higher risk of phishing attack, identity theft, and other cyberthreats.

The poisoned caches act like "forged street signs that you put up to get people to go in the wrong direction," said DNS inventor Paul Mockapetris, chairman and chief scientist at secure DNS provider Nominum. "There have been other vulnerabilities (in DNS) over the years, but this is the one that is out there now and one for which there is no fix. You should upgrade."

There are about 9 million DNS servers on the Internet, Kaminsky said. Using a high-bandwidth connection provided by Prolexic Technologies, he examined 2.5 million. Of those, 230,000 were identified as potentially vulnerable, 60,000 are very likely to be open to this specific type of attack, and 13,000 have a cache that can definitely be poisoned.

The vulnerable servers run the popular Berkeley Internet Name Domain software in an insecure way and should be upgraded, Kaminsky said. The systems run

### How does DNS get poisoned?

There are a few steps to go through before a DNS server starts redirecting Web surfers to bogus sites.

Most people's PCs access a DNS server at an Internet service provider or within a company to map text-based Internet addresses to actual IP addresses. One DNS server can be used by thousands of Internet users.

For performance reasons, DNS servers cache the returned data, so that it takes less time to respond to the next request. When a DNS cache is poisoned, it affects all future lookups of the affected domain, for everyone who uses that particular DNS server.

To poison a DNS server:

- First, the target machine has to be tricked into querying a malicious DNS server set up by the attacker. This can be done, for example, by sending an e-mail message to a nonexistent user at the target ISP. Another way is to send an e-mail with an externally hosted image to an actual user.
- The target DNS server will then query the attacker's DNS server. In the DNS reply, the scammer includes extra data that will poison the victim's DNS cache. The extra information can be a malicious URL or even an entire domain space, such as .com.
- If the target DNS server is not configured properly, it will accept the new numerical IP listing and delete the proper entry.
- Once this has occurred, any queries sent to the DNS server for the affected URLs will be redirected to the replacement IP addresses set by the attacker. If a domain space is poisoned, all queries ending in that domain will be redirected.

Source: SANS Internet Storm Center, CNET News.com

BIND 4 or BIND 8 and are configured to use forwarders for DNS requests—something the distributor of the software specifically warns against.

BIND is distributed free by the Internet Software Consortium. In an alert on its Web site, the ISC says that there "is a current, wide-scale...DNS cache corruption attack." All name servers used as forwarders should be upgraded to BIND 9, the group said.

DNS cache poisoning is not new. In March, the attack method was used to redirect people who wanted to visit popular Web sites such as CNN.com and MSN.com to malicious sites that installed spyware, according to SANS.

"If my ISP was running BIND 8 in a forwarder configuration, I would claim that they were not protecting me the way they should be," Mockapetris said. "Running that configuration would be Internet malpractice."

## The new threat—pharming

Kaminsky scanned the DNS servers in mid-July and has not yet identified which particular organizations have the potentially vulnerable DNS installations. However, he plans to start sending e-mails to the administrators of those systems, he said in an interview.

"I have a couple hundred thousand e-mails to send," he said. "This is the not-fun part of security. But we can't limit ourselves to the fun stuff. We have to protect our infrastructure."

The use of DNS cache poisoning to steal personal information from people by sending them to spoofed sites is a relatively new threat. Some security companies have called this technique pharming.

Poisoning DNS cache isn't hard, said Petur Petursson, CEO of Icelandic DNS consultancy and software company Men & Mice. "It is very well doable, and it has been done recently," he said.

Awareness around DNS issues in general has grown in the past couple of years, Petursson said. Four years ago, Microsoft suffered a large Web site outage as a result of poor DNS configuration. The incident cast a spotlight on the Domain Name System as a potential problem.

"It is surprising that you still find tens of thousands or hundreds of thousands vulnerable servers out there," Petursson said.

Kaminsky's research should be a wake-up call for anyone managing a DNS server, particularly broadband Internet providers, Mockapetris said. Kaminsky said he doesn't intend to use his research to target vulnerable organizations. However, other, less well-intentioned people could run scans of their own and find attack targets, he cautioned.

"This technology is known to a certain set of the hacker community, and I suspect that knowledge will only get more widespread," Mockapetris said. ❖

# Why you should disable DNS caching on workstations

*By Jonathan Yarden*

Earlier this year, news broke that the amount of phishing e-mails, which sport ostensibly legitimate offers through which attackers attempt to glean personal and financial information, has slowed in the first two months of this year. But don't start celebrating yet: Attackers are simply getting smarter, not slower. In fact, they're honing their skills and turning to more sophisticated ploys.

Would-be attackers are now setting their sights on the domain name system (DNS), an integral part of the Internet, in hopes of making it more difficult to determine authenticity. Referred to as "pharming" or "DNS poisoning," this practice involves redirecting users to malicious Web sites that look perfectly legitimate, where attackers attempt to either steal personal information or install spyware.

It should come as no surprise that the people behind these scams are targeting primarily Windows-based systems—and exploiting a known DNS cache bug found in several Symantec firewall products (**http://techrepublic.com.com/2100-10595_11-5604555.html**). However, this is not a new Internet security issue. In fact, the popular UNIX BIND nameserver software identified and addressed the current Windows DNS security problems, especially the issue of cache poisoning, years ago.

The details of who and what malware are responsible for this are currently under investigation, but organizations can't afford to wait for authorities to resolve this issue. While companies are more than likely unable to prevent attempted attacks, they can take steps to mitigate risks.

Of course, a company's first step should always be user education. Make your users aware of these threats and attackers' various methods, and teach them to closely examine any e-mails and Web sites before trusting them with personal information.

DNS is critical to the functioning of the Internet, and it's probably as critical a process as the routing of IP packets on the Internet itself. Without a properly functioning DNS, any number of problems can occur, many of which mimic network-level problems.

In fact, even simple DNS problems, either locally or on the Internet, can cripple the ability to communicate over the Internet. This is why I stress that companies should regard DNS services and servers as network-level services, in the same category as routers and switches rather than e-mail or Web servers.

At its basis, DNS is the service that translates hostnames to IP addresses and resolves IP addresses to hostnames. Root DNS servers—probably the busiest servers on the Internet—do nothing more than provide pointers to authoritative nameservers (called "NS records") for a particular domain. An NS record contains the hostnames for authoritative nameservers for a particular domain, and it also provides the IP address of these servers.

DNS servers typically cache previously obtained information for future use to minimize the number of queries to other DNS servers, including NS queries to root DNS servers. Because DNS is all about minimizing the number of external lookups for domain information, caching this information whenever possible is vital.

But DNS servers aren't the only machines with this ability. Microsoft and many other software companies—even those that provide Internet security products—have made the mistake of including the ability to cache DNS information on workstations. For example, Microsoft Windows includes a DNS Cache service.

However, I strongly believe that only DNS servers should cache DNS information. In fact, I recommend that organizations disable the DNS cache service, which Microsoft has enabled by default.

Client workstations that use DNS should never cache DNS information locally. Once the workstation has stored DNS data locally, any process with the ability to access or change that information can trivially redirect services that depend on DNS to other hostnames.

DNS cache poisoning is yet another concern for systems using Microsoft DNS. Working at the DNS server level, cache poisoning involves changing the IP address of authoritative DNS servers so subsequent DNS lookups for hostnames come from someplace other then a legitimate one. DNS poisoning can affect entire networks that rely on Microsoft DNS services on a variety of Microsoft Windows versions, with the exception of Windows Server 2003.

I also recommend that companies have a minimum of two authoritative DNS servers and keep them on two separate physical and logical networks. This helps prevent a single point of failure with DNS because incorrect or nonfunctional DNS is a recipe for disaster.

And under no circumstances should workstations be using any manner of DNS caching services. DNS caching is for DNS servers; these servers should focus solely on this task. Companies must take steps to secure the DNS servers and distribute them on separate networks to prevent would-be attackers from hijacking or poisoning them with incorrect information.

I'm disappointed in Microsoft and Symantec: Shame on them for not learning from history that DNS is a service that should place security first. ❖

# 6 User Education

# Helping users combat spyware

*By Steven Pittsley, CNE*

You've done it all. The servers are patched with the latest code, the workstations are protected with the top-of-the-line spyware detection software, and you've configured the firewall to block all unnecessary outbound ports. You sit back, take a breath, and congratulate everyone on a job well done.

But while you're enjoying the moment, a new employee in another part of the building is installing WeatherBug so she can get the daily forecast before driving home. By the time your party's over, she'll have convinced two of her coworkers to install the application as well. Your safe and secure network was just breached at the weakest point: the user.

In this article, we'll discuss steps you can take to enlist your users' help in fighting the spyware battle. We've also included a spyware prevention checklist, which you can use as a quick reference for anti-spyware best practices.

## Raising user awareness

One of the key components of an anti-spyware initiative is educating users. Start with the basics, such as what constitutes spyware and what risks it poses. Once you've introduced the fundamentals, you can teach users how to spot spyware and what they can do to keep it off their machines. Depending on the size of your organization, these lessons can be taught in formal classes or in one-on-one sessions, where technicians visit users. Topics you'll want covered include:

- **Recognizing installed spyware.** Users need to be aware of spyware symptoms. Most spyware is easily detected because it generates advertising pop-up windows, but users should also look for sluggish system performance, new home pages in their Internet browser, Internet pages that are rerouted to other Web sites, and the sudden appearance of new toolbars.
- **Downloading and installing cautiously.** When users are presented with a pop-up window that asks them to click OK to install a "helpful" application, instruct them to either click the X in the upper-right corner of the window or press [Alt][F4] to close the window. They should never click OK or I Agree to close a pop-up window.
- **Carefully reading the EULA.** If users elect to install a software program, they should take a few minutes to read the end-user license agreement (EULA) and all installation options to ensure that there aren't any additional applications hidden within the installation package. Even a trustworthy program like the Google toolbar has benign spyware options offered as part of the installation routine.

Be prepared to encounter users who believe that spyware applications are helpful. For example, at first glance, WeatherBug may appear quite handy. However, it also installs the My Search toolbar and generates pop-up advertising windows. So, in addition to removing the spyware, you must convince users that these programs can potentially lead to other problems.

## Tightening browser security

Internet Explorer 6 offers several security settings designed to keep spyware at bay. These features attempt to strike a balance that allows users to browse the Web while still protecting their computers from harmful software.

To access the IE security settings, click Tools | Options. The security settings are located on the Security and Privacy tabs. **Figure A** shows the four security zones where all Web sites are gathered:

- **The Internet Zone** contains all Web sites that are not placed in the other three zones.
- **The Local Intranet Zone** contains Web sites on your company's intranet.
- **The Trusted Sites Zone** contains all sites that you believe to be trustworthy and that you want your users to be able to view.
- **The Restricted Sites Zone** contains all the sites you don't want anyone who uses the computer to view.

By adding sites to the Restricted Sites Zone, you can prevent users from viewing sites you deem dangerous. For example, you might want to consider blocking the download site for WeatherBug to keep users from downloading and installing the program.

To add sites to the Restricted Sites Zone, click the Sites button. When the Restricted Sites dialog box appears (**Figure B**), enter the address of the site you want to restrict and click Add. The site will be added to the Restricted Sites list.

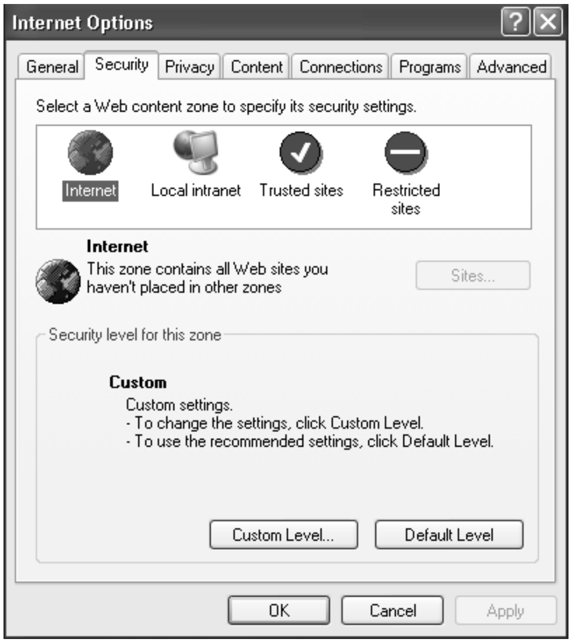
You can also customize the security settings for a particular zone. Click the Custom Level button to open the dialog box shown in **Figure C**. Here, you can change the security level or modify the default settings.

The Privacy tab, shown in **Figure D**, allows you to modify the security level for the Internet Zone. To adjust the level, simply move the slider to the desired setting. The Privacy tab also lets you modify the settings for the Microsoft Pop-up Blocker program, which we'll look at next.

## Installing pop-up blocker software

Pop-up blocker software won't prevent spyware from being installed on a computer, but it will at least keep pop-up advertisements from displaying. These programs use a database of known pop-up sites to prevent them from opening. When a Web site in the database attempts to display, the pop-up blocker closes the new window.

**Figure A**



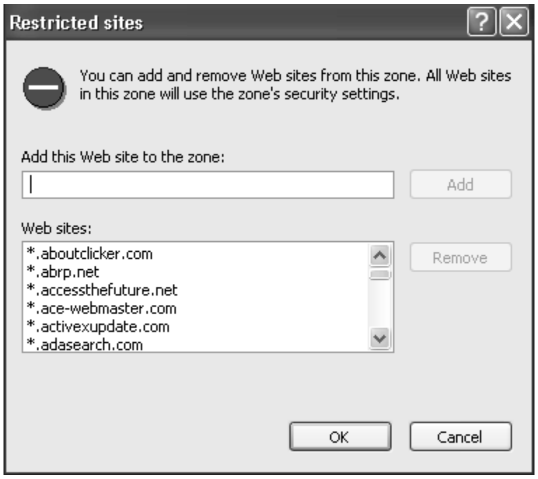
Select a Web content zone to specify its security settings.

**Internet**
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

**Custom**
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

**Figure B**

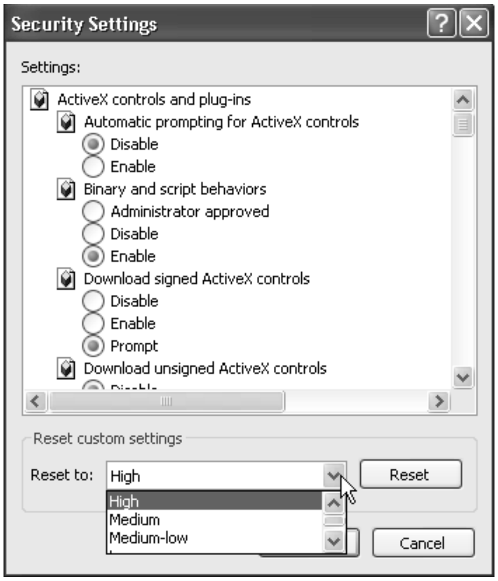


You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.

Add this Web site to the zone:

Web sites:
*.aboutclicker.com
*.abrp.net
*.accessthefuture.net
*.ace-webmaster.com
*.activexupdate.com
*.adasearch.com

**Figure C**

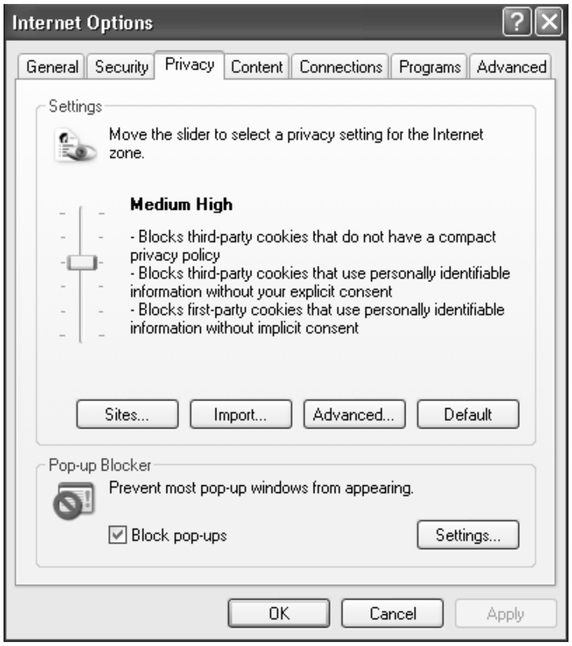


Settings:
- ActiveX controls and plug-ins
  - Automatic prompting for ActiveX controls
    - ● Disable
    - ○ Enable
  - Binary and script behaviors
    - ○ Administrator approved
    - ○ Disable
    - ● Enable
  - Download signed ActiveX controls
    - ○ Disable
    - ○ Enable
    - ● Prompt
  - Download unsigned ActiveX controls

Reset custom settings

Reset to: High
High
Medium
Medium-low

**Figure D**



Settings

Move the slider to select a privacy setting for the Internet zone.

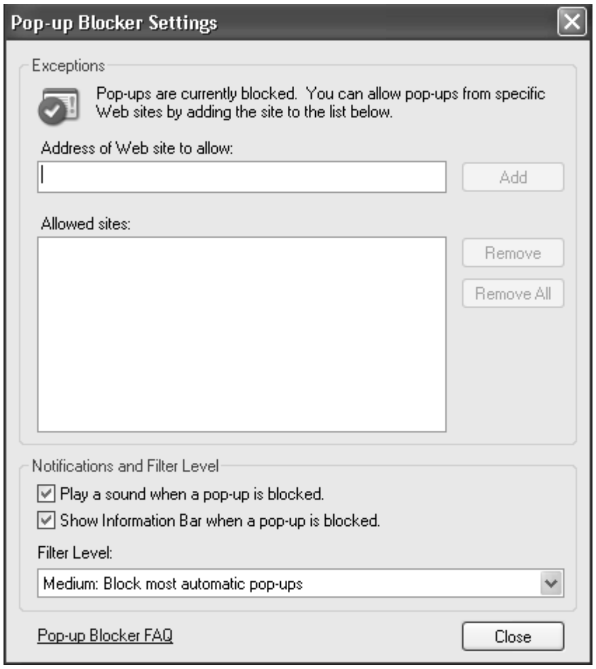
**Medium High**
- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your explicit consent
- Blocks first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

☑ Block pop-ups

**Figure E**



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow:

Allowed sites:

Notifications and Filter Level

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

Pop-up site databases are populated in two ways. Some pop-up blockers require users to specify every Web site they want blocked, usually by selecting from a list of open windows. There are a couple of problems with this approach. First, it's a time-consuming method of populating the database. Second, the pop-up window must be opened at least once before it is blocked. This type of program works well, but users quickly tire of adding Web sites to the database.

Other pop-up blockers use a pop-up window definition file, which is a better alternative. The definition files are constantly updated, providing a current list of pop-up sites. These programs are easier to use and only require users to update the definition file, not actually build their own. The IE Pop-up Blocker that's installed with WinXP SP2 is an example of this type of software.

To view Pop-up Blocker settings, open Internet Explorer and click Tools | Pop-up Blocker | Pop-up Blocker Settings. **Figure E** shows the options that are available.

First, you can add Web site addresses to the Allowed Sites list. These sites override the definition file and allow you to view pop-up windows from certain Web sites that might otherwise be blocked. You can also select the type of notification you receive when a pop-up is blocked and set the Filter Level. In general, the Medium setting does a good job of blocking most pop-ups from adware companies. If you want to block all pop-ups, select the High setting. The Low setting blocks all pop-ups except those from secure sites listed in the definition file.

## Using anti-spyware tools

Spyware detection software scans a computer's hard drive for known spyware. Teaching your users how to use these applications allows them to remove spyware at the first sign. You should also instruct your users to run the spyware detection software at least once a week, even if they don't notice any signs of spyware. Regularly running the detection program can prevent problems before they surface.

**Table A: Spyware prevention checklist**

- ❑ Educate users about the dangers of downloading and installing software that has not been approved for the corporate network.
- ❑ Explain the importance of reading the end-user license agreement (EULA) when installing software.
- ❑ Install anti-spyware software, such as Lavasoft's Ad-Aware, on all computers in the corporate environment.
- ❑ Teach users how to recognize and remove spyware using anti-spyware software programs.
- ❑ Inform users of new spyware programs that appear in the corporate environment. This can prevent them from downloading and installing something that a coworker or friend shows them.
- ❑ Configure browser security settings to reduce the amount of spyware that can be downloaded.
- ❑ Install pop-up blocker software or use the Internet Explorer Pop-up Blocker addition.
- ❑ Configure firewalls to block all outbound traffic on unused ports to prevent spyware from covertly sending information through them.
- ❑ Use group policies to prevent software installation on corporate workstations.
- ❑ Reduce the amount of Web surfing allowed on corporate computers.

These measures will greatly reduce the amount of spyware that gets installed on a computer. Of course, they won't eliminate the threat entirely, but they'll give you a healthy head start on keeping spyware under control.

## Wrap-up

In today's world, spyware is a constant threat. However, computer users can help combat spyware by understanding the risks, downloading cautiously, carefully reading EULAs for every piece of software they install, and regularly using spyware detection software. The checklist in **Table A** covers the basic steps you and your users can take to stay on top of the spyware situation. ❖

# Knowledge is power against new social engineering schemes

*By Brien M. Posey, MCSE*

In the past, social engineering schemes traditionally involved a hacker posing as someone from the support department and either trying to assist the user with a problem or getting the user to help run a test. But hackers like to break with tradition, and current social engineering methods are all about defying expectations.

To help you understand the new face of social engineering, here are some of the new ways that hackers are manipulating social engineering to get what they want—access to your data. By reading through these new social engineering schemes, you can better educate yourself and your staff about the techniques being used, which in turn will help everyone in your company avoid falling prey to these security breaches.

### SOCIAL ENGINEERING

*Social engineering* refers to an act in which a hacker tricks a user into disclosing a password or other sensitive information, rather than relying purely on traditional hacking techniques.

## Relationship social engineering

I had the chance to watch firsthand a social engineering stunt using common conversation to obtain password information. This particular job wasn't an illegal hack, but rather a situation in which a client paid a security company, Relevant Technologies, to see if its employees would fall victim to a social engineering scheme. The company felt it better to identify security holes under controlled conditions than to be exploited by someone who really did have malicious intentions. Unfortunately, the social engineering scheme went off without a hitch, and the company's owner realized that he needed to place a greater emphasis on employee training.

For this particular scheme, a woman was hired by the security company to call sales representatives at the client's company and pretend to be interested in buying its product. Part of the conversation went something like this:

Social engineer: "My kids will love this product. I have a two-year-old named Fred and an eight-year-old named Beth. Do you have any kids?"

User: "Yes, I have a four-year-old son named Shawn."

This is seemingly innocent chitchat, but in organizations that don't enforce a strict password policy, employees often use their kids' names as passwords. In this particular case, the employee had one son named Shawn, which was the employee's password. Of course, that was a lucky guess, but the security company's social engineer was able to worm other personal information out of the employee as well.

For this particular test, the woman never asked for a password—or anything else related to the computer system. What she did do was build a relationship with the victim. Even if nothing on the password list had matched, she had developed enough trust that, on a future call, she may have been able to get more damaging information out of him.

## Password conundrum

People have more passwords to remember than they used to. As a result, it's common for people to use the same password for access to multiple locations, including using the same password for system access at work and at home.

In some cases, hacker groups set up Web sites advertising a bogus sweepstakes. They then require anyone registering for the sweepstakes to supply a username and password for future access to the site. Soon a database of thousands of usernames and passwords is compiled. A "robot" then systematically attempts to log on to many popular Web sites using the supplied usernames and passwords. The hacker group can then use details from these sites to gain more information. For example, if a hacker is able to get into a person's Hotmail account, he or she might be able to figure out where the person works and then be able to try to break in to that company's computers using the person's logon name and password.

## New twist to an old scheme

I'm starting to see more subtle uses of social engineering that rely on traditional hacking techniques and the popularity of the Web. In a recent case, a bank fell victim to one such social engineering scheme. The hacker registered an Internet domain name that was very similar to the bank's domain name. Next, the hacker created an official-looking form and telephoned bank employees to tell them there was going to be a change to their benefits package and that they needed to go to this particular Web site and fill out the new benefits form. The hacker then told them that the Web site required authentication and to simply enter their normal logon name and password.

Of course, the Web site was not actually performing authentication. Instead, the supposed authentication mechanism was nothing more than a Web form that collected usernames and passwords and entered them into a database. All the hacker then had to do was examine the database's contents to retrieve usernames, passwords, and other personal information.

## Windows XP remote assistance scheme

Yet another new social engineering stunt involves exploiting Windows XP's remote assistance. It involves someone claiming to be from the IT department asking an employee if he or she can connect to the computer via remote assistance to load a security patch. After the connection is made, a spyware module is loaded onto the machine. The spyware module then collects username and password information and e-mails them to the hacker. The beauty of this technique is that the hacker never has to ask for a password. Instead, the user actually lets the hacker work on his or her machine by remote control. Since the user never actually sees the hacker's face, the hacker's identity is protected, especially if specific path routing is used.

### PATH ROUTING TECHNIQUE

*Specific path routing* is a technique by which a hacker can direct the path of a TCP/IP connection from the hacker to a victim. This technique is often used to obscure the hacker's true IP address or geographic location.

## Chat trick

Social engineering exploits that have traditionally been conducted by phone are now starting to show up in instant messaging and in IRC-based chats. According to Internet security Web site CERT (**http://www.cert.org/incident_notes/IN-2002-03.html**), this exploit commonly involves tricking the user into downloading either a spyware module or a module that can be used by the hacker in a distributed denial of service attack.

One particular message that's sometimes used to trick people into downloading these malicious programs is, "You are infected with a virus that lets hackers get into your machine and read your files, etc. I suggest downloading [*malicious filename*] and cleaning your machine. Otherwise, you will be banned from the IRC network."

To prevent situations like this, I recommend installing ViRobot from Hauri onto everyone's machines (**http://www.hauriusa.net/products.htm**). If ViRobot is running, users can rest assured that they don't have a virus. Also, ViRobot is designed to spot various hacker tools that could have been installed through this or similar exploits.

## What you can do

Many companies are becoming aware of the risks of new social engineering techniques and have begun to develop policies designed to combat social engineering schemes. One of the most widely publicized examples of such a policy is the way

AOL tells its customers that no customer support representative will ever ask them for their password.

Unfortunately, there are countless other social engineering techniques available to the hacker. The only real defense against them is to use strong passwords and to educate your users about the different types of schemes, warning them especially about the hidden dangers of innocent conversation. ❖

# Change your company's culture to combat social engineering attacks

*By Jason Hiner, MCSE, CCNA*

A consultant was hired by a business executive to test the security of the executive's enterprise. The consultant was not hired to try to hack through the firewall or bypass the intrusion detection system. He was hired to see how easy it would be for a motivated intruder to gain physical access to the company's mission-critical systems.

So the consultant created a fake company ID badge for himself. He even simulated a magnetic swiping strip on the back of the ID by using a piece of electrical tape. He used this fake ID to get into the company's main building, then made his way up to the data center where he began swiping his fake ID badge through the scanner. After several failed attempts, a friendly employee walked up and said, "Sometimes, that thing doesn't work." The friendly fellow proceeded to swipe his own badge, letting the consultant into the data center.

At that point, the consultant walked to the center of the room, raised his arms, and said, "Okay everyone, I'm conducting a surprise security audit. I need everyone to leave the room immediately." Although there were a few surprised faces, all the employees in the data center filed out.

The consultant pulled out his cell phone, called the executive who hired him, and said, "Guess where I am?"

## Why people are the weakest link

Gartner analyst Rich Mogull used this example to show how motivated attackers can have much more success by manipulating people rather than trying to hack through various levels of sophisticated security technologies. Mogull addressed this subject in detail in his presentation, "Human Security Issues: Managing People and Defending Against Social Engineering," on May 15 at the Gartner Information Security (InfoSec) conference in Chicago.

Mogull explained that people are, by nature, unpredictable and susceptible to persuasion and manipulation. Attackers that utilize social engineering techniques take advantage of what Mogull calls "primal motivators" such as fear, greed, and sexuality to manipulate employees into releasing information (usually unwittingly) or providing access to information systems.

"Social engineering is the single greatest threat to enterprise security," Mogull said, adding that many of the most damaging security breaches are due to social engineering and not electronic hacking.

He also described social engineering as "the most difficult [security] issue to manage" and said that most IT departments do a poor job of combating the threat.

## Understanding social engineering attacks

Social engineering is essentially a way to bypass technology-based security mechanisms by manipulating people. Mogull said social engineering attacks typically originate from one of three zones:

- Internal
- Trusted
- External

Internal threats come from employees who manipulate other employees to gather sensitive information and access to IT systems. These offenders can include disgruntled employees, temporary employees, employees with criminal tendencies, and ancillary workers such as housekeeping and maintenance staff. Enterprises grant a certain amount of trust to all of these individuals, which can make it easier for them to execute attacks.

Trusted threats come from other individuals who are formally associated with your organization on a regular basis but are not on your payroll. These can include contractors and consultants, as well as partner organizations. Often, these individuals have a very high level of trust, and thus have access to sensitive data and systems. Yet such potential risks are rarely incorporated into security plans.

External threats come from people who are not associated with your organization. This category can include recreational hackers, competitors wanting to uncover confidential information, or criminals wanting to steal something. These people have no established trust with your organization, so they look to create short-term trust by using various social engineering techniques.

Some examples of these techniques are:

- Playing the role of an authority, such as an IT administrator.
- Playing the role of an end user.
- Playing the role of someone from a partner organization.
- Playing the role of a telecom technician or another individual who would have physical access to the company's data systems.
- Tricking an employee into planting malicious software on internal systems.
- Stealing the identity of someone with inside access to IT systems.

Individuals who use social engineering techniques usually follow a common pattern of activity that Mogull calls the Social Engineering Attack Cycle.

In the first phase, information gathering, an attacker uses various techniques to track down detailed information that can be used to gain the trust of an individual connected to the targeted organization. The attacker will then use this information to develop a relationship with the individual in phase 2 of the attack cycle. This can take one phone call or it can happen over a period of weeks or even months.

After the relationship is established, the attacker will exploit the relationship (phase 3) to get the target to reveal information or perform an action that would not otherwise take place. Phase 3 either accomplishes the attacker's objective or opens the door to achieving the final objective in phase 4.

## Guarding against social engineering

As you've probably already figured out, social engineering attacks are elusive and underhanded. However, they are not impossible to combat. "This is a business process issue," Mogull emphasized. As such, organizations need to implement processes that undermine the effects of social engineering and, beyond that, establish a culture of security and accountability within the company.

One way you can test the current security culture of your organization is to do a simple self-quiz. Think about how the employees in your organization would react if an unfamiliar person who looked out of place sat down in a cubicle and started working on a computer. Now, ask yourself three questions:

- Would one of your employees become suspicious about this event?
- Would any employee choose to report it?
- Would any employee know how to report it and who to report it to?

If you don't feel confident that your employees would be able to intervene in this potential security breach, you need to take several concrete actions to improve your organization's security culture.

Assuming you already have a well-conceived security policy in place, the first and most important action is to educate users about your company's security policy, or at least the parts of it that potentially affect them. You should also raise employee awareness of the threat of social engineering.

Many organizations will also need to improve the physical security of their facilities. Mogull made some other recommendations for preventing social engineering attacks, including:

- Do background checks when hiring employees.
- Screen temporary and ancillary workers.
- Set up a clear reporting process for security problems.
- Open the lines of communication between physical security and the IT department.
- Monitor employee behavior patterns for abnormal activities and access violations.
- Lock out terminated employees immediately.

- Create a positive work environment, which will cut down on disgruntled employees.
- Publish a formal written company policy stating that the IT department will never ask for a user's password.
- Require ID badges for employees and mandate that an employee with a badge accompany visitors.

## Be on the lookout

Social engineering attacks are elusive and can have very damaging consequences for an organization, but you can take a number of steps to mitigate such attacks. By increasing your users' awareness of social engineering techniques and setting up commonsense business processes, you can change the culture of your organization to guard against these attacks. ❖

# Notes: