



828 West Taft Avenue  
Orange, CA 92865  
714-282-6111  
714-282-6117 Fax  
www.8e6.com

## 8e6 3000 | Enterprise Filter



# Neutralizing the Spyware Threat

By The Forsite Group

### Introduction

*Spyware is an executable program with a single objective: to secretly monitor a computer and surreptitiously report information on activity to anyone willing to pay for it.*

Add spyware to the list of urgent security concerns. With resources already stretched thin in fighting viruses, stopping spam, and complying with data-protection requirements laid out in federal regulations like Health Insurance Portability and Accountability Act (HIPAA), companies now also have to defend against a threat that strikes silently and does much of its damage before it's even detected.

Spyware is an executable program with a single objective: to secretly monitor a computer and surreptitiously report information on activity to anyone willing to pay for it. While it can serve a legitimate purpose for companies legally tracking user behavior, it's also an ideal tool for corrupting or stealing the sensitive business data residing on corporate PCs and systems. What's more, spyware can seriously degrade performance, reduce employee productivity, and impose extensive administrative expense. And spyware is virtually everywhere: Industry experts estimate that 90 percent of all employee computers harbor at least 30 spyware programs apiece. Whether it implants itself upon a visit to an unauthorized Web site or arrives as part of a worm's payload, spyware immediately sets out to perform its surreptitious functions.

Stopping unauthorized programs at their source and staying abreast of potential infections are critical in keeping spyware from doing harm. 8e6 Technologies helps on both fronts. Its R3000 Enterprise Filter network appliance is a flexible, highly scalable approach to identifying known spyware sites and blocking installation of suspicious programs. Thanks to 8e6's continuously updated library of spyware sites, it can be dynamically configured to recognize the latest threats. Simple setup allows rapid rollout as part of a comprehensive spyware defense, while an open-source OS rounds out the R3000 feature set. Additionally, 8e6's Enterprise Reporter appliance helps in developing the detailed reports on user activity that can aid in detecting spyware's presence. Together, 8e6's products can be deployed as an integral part of a company's overall approach to defending against spyware.

## The Spyware Dossier

*It's a relatively simple and inexpensive technology that when used by legitimate companies to legally track customer behavior, generates considerable revenue. The trouble is that those same attributes appeal to criminal entities looking to profit from its use in stealing corporate data.*

Spyware is not a new technology, and not all of it is malicious. On one end of the spectrum are programs that come bundled as part of a legitimate software package and that customers consent to run when they sign an end-user license agreement (EULA). Further, some of it is actually intended to help users: Software that tracks online activity, for example, is necessary in implementing the personalization features that so many users want.

On the other end of the spectrum is spyware that's clearly malicious. There is no other way to characterize programs that snoop files and systems for sensitive data. Some track keystrokes, so that credit card and other personal information can be stolen. Others can reconfigure browsers, install additional spyware, and even activate Webcams. Spyware is also living up to its name as a real-world espionage tool: North Korea has been identified as one of the nations using it to gather data on potential adversaries, sometimes even selling that information to international criminals who use it to launch distributed DoS attacks.

But it's the gray area in the middle that's causing problems for both the industry and the government in devising a comprehensive approach for dealing with spyware. At what point does surreptitious monitoring turn into breach of privacy? There's no disagreement over the threat posed by viruses, but opinion isn't nearly as united on spyware (some, for example, consider cookies an insidious form of spyware, while others say they meet none of the criteria). The U.S. Congress has introduced bills like the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) and Internet Spyware Prevention Act (ISPA), but they've had little effect simply because of the disagreement over what constitutes a malicious program.

In other words, spyware is here to stay: It's a relatively simple and inexpensive technology that when used by legitimate companies to legally track customer behavior, generates considerable revenue. The trouble is that those same attributes appeal to criminal entities looking to profit from its use in stealing corporate data. And they're the ones that companies have to be most concerned about.

## Covert Operations

With spyware a permanent part of the landscape, it's incumbent on companies to learn how it operates, how to recognize it, and how to minimize the damage.

Spyware can reside as a persistent file on a hard drive or present itself as a hostile ActiveX control or java applet. It can install itself on user machines in a variety of ways. As noted, it's often part of a legitimate software installation. In such cases the EULA contains information about the presence of spyware code; signing off on the agreement means consenting to spyware—even if the only mention of it is buried in the fine print (as it often is).

*If companies or users aren't specifically looking for spyware, the signs of possible infection can be so innocuous that they're ignored.*

Spyware can also implant itself in a PC from the Web sites a user visits. Sometimes a key stroke or mouse click in a deceptive pop-up window is needed to start the download, but the most insidious programs simply land on the PC via a "drive-by" installation: Just opening the page can be enough to become infected. Not surprisingly, this is how much of the most harmful spyware is delivered. Equally unsurprising is that it can be traced to sites typically not authorized for employee use—like pornographic or gambling sites—or to sites with disguised links.

Spam and worms might also harbor spyware. Programs that arrive in this manner are almost always of the malicious strain, often hiding code that tracks key strokes or that turns the PC into a zombie for use in a DoS attack.

Regardless of how it arrives, spyware begins to do its work immediately, reporting back to its source on user behavior, site visits, and other activity. Even as corporate secrets or other confidential data is leaving the premises via this back-door channel, users might not know that their PC harbors code—or is the conduit to the outside world.

If companies or users aren't specifically looking for spyware, the signs of possible infection can be so innocuous that they're ignored. Whether it's a whirring disk drive, a slowly responding application, or just general sluggishness, the symptoms can go unnoticed or be just as easily blamed on a balky server or congested link. Pop-ups that elude pop-up blocking software or spontaneous home-page resets are more obvious signs of spyware's presence, but even these often go overlooked.

As if the security concerns weren't serious enough, spyware also takes its toll in employee productivity and administrative resources. Endlessly spawning pop-up windows interfere with work and eat up valuable time. Trouble tickets filed for unexplained performance slowdowns swamp IT departments. The communication overhead generated by some malicious code contributes to network congestion, slowing down the entire enterprise. Given the overall impact of spyware on the business, companies have no choice but to mount a comprehensive anti-spyware campaign.

## Cloak, Dagger, and Education

Right now, there is no single solution for fighting spyware. The most effective defense is a combination of user education and technology.

On the educational front, companies should begin by creating and disseminating a clear policy for employees on how to avoid spyware. It should make clear the hazards of visiting unauthorized sites, and of downloading free or unlicensed software—including file-sharing programs, which can often harbor malicious code. The policy should warn against unauthorized installation of pop-up blockers or anti-spyware applications, since these can just as easily function as delivery systems for even more spyware. And it should instruct users on what not to do when visiting suspect sites—such as clicking "agree," "OK," or any other command that may appear in a window (they should instead hit the red "X" in the corner of the window rather than risk consenting

*Right now, there is no single solution for fighting spyware. The most effective defense is a combination of user education and technology.*

hit the red “X” in the corner of the window rather than risk consenting unknowingly to a spyware download).

It’s also important to inform employees of the damage that can be done when they or their family members use the company laptop at home, where they might have access to sites they can’t visit from the workplace. IT departments have become familiar with the spyware-laden laptop brought in for servicing after Mom, Dad, and the kids have used it all weekend for Web surfing.

Of course, companies need to complement the educational outreach with technology. There are three key components in the tech approach: prevention, entrapment, and disinfection.

Prevention, of course, calls for stopping spyware from getting into systems in the first place. And companies shouldn’t rely solely on firewalls and anti-virus software. After all, spyware often arrives via legitimate means and can thus pass through firewalls undetected, and it doesn’t exhibit the classic “viral” behavior that anti-virus applications search for. Instead, businesses should evaluate the software programs now widely available that can be installed on gateways and other network appliances to stop spyware at the network perimeter.

Other types of anti-spyware applications work by detecting known spyware programs and locking them down inside the network. They then block the intrusive code from establishing a link back to its source, thus keeping it from doing its damage.

But the nature of spyware makes infection inevitable, and in these cases the only choice is to address infection after the fact. Companies have no shortage of products to choose from when it comes to wiping spyware from infected systems—some of which have become very well known. Still, they should take special care in evaluating the growing number of products on the market: Some are nothing more than spyware themselves, masquerading as solutions.

Maybe the most important thing to keep in mind is that no one approach is sufficient in combating spyware. The best strategy: Be smart in educating employees, and choose technology that can be readily deployed as an integral part of the anti-spyware fight.

## The 8e6 Solution

That’s where the R3000 from 8e6 comes in. It’s a flexible, highly scalable network appliance that sits at the gateway or aggregation point of the network, and features a range of Web filtering capabilities that give companies a valuable edge in the fight against spyware.

How? By stopping spyware that has entered the network from phoning home to its source. Without that vital connection, spyware can’t send any information back outside the corporate network—rendering it impotent.

*The key is in identifying spyware URLs. 8e6 does this by gathering suspect links in a “flytrap” system in its own lab...*

The key is in identifying spyware URLs. 8e6 does this by gathering suspect links in a “flytrap” system in its own lab; essentially, it’s an unprotected network that acts as a magnet for rogue programs, which are then isolated and examined. If they’re determined to be spyware, 8e6 adds the source URL to its extensive library of violating URLs—links that the R3000 can be configured to recognize and block via dynamic updates.

Here’s how that works in a production network. The R3000 uses deep packet inspection to scan all internal traffic heading out to the Web. When it spots a violating packet—that is, one headed back to a known spyware source—it sends a block page to the PC that generated the request, typically within 2 to 4 ms. Then it sends a TCP reset to the site to cancel the session. By sealing off access to spyware sites so quickly, the R3000 prevents confidential information from leaving the premises—while simultaneously securing the network from unauthorized intrusion and more malicious code.

The same process can help keep spyware from entering the enterprise in the first place. 8e6 boasts a database library supporting 80 categories (from “alcohol” and “games” to “pornography” and “weapons”), so that companies can exert as much control as they want over the types of sites their employees are allowed to visit. Further, enhanced keyword filtering means the R3000 can block file download by type or extension—helping companies build a wall against executable programs. By blocking access to suspicious links and preventing unauthorized downloads, companies lower the risk of spyware infection.

8e6 also addresses the spyware vulnerabilities inherent in IM and P2P communications. Its Intelligent Footprint Technology (IFT) identifies IM packets sent to unknown servers, private servers, or proxy servers, thus increasing detection rate and decreasing the ability to bypass blocking. IFT monitors AOL Instant Messenger, MSN, and Yahoo—and is one of only a few solutions to monitor ICQ. IFT also identifies P2P packets to block log-in or file transfer; among the applications it monitors are KaZaA, WinMx, eDonkey, eMule, and Gnutella.

Of course, fighting a stealthy enemy requires corresponding speed and agility: The last thing companies need in the battle against spyware is technology that’s inflexible, that doesn’t scale, or that takes a bite out of productivity and performance. The R3000 offers peace of mind in all of these areas.

First, it’s based on Red Hat Linux. That makes for a stable and resource-efficient platform, while helping companies leverage open-source advantages like improved global support and interoperability with a wide range of devices.

Second, it can grow along with the business. The R3000 scales to 20,000 users or more per appliance; with authentication enabled, it can support up to 30,000 user connections at a 30-connection-per-second build rate.

Third, the R3000 is easy to set up and run. It comes with software pre-installed, so it can be put to work right out of the box. A Java-based GUI

furnishes intuitive navigation, aiding administrators as they define parameters and user groups. And an online help feature keeps customers close to the information they need to optimize operation. Fourth, the R3000 runs in “invisible mode.” It’s not proxy-based but sits on the network, where it inspects packets without stopping them to do so. In other words, the R3000 adds zero latency—thoroughly assessing Web-bound traffic without incurring a penalty in performance.

Reporting functions are also critical in getting a handle on the scope of spyware infection, and 8e6 delivers them with its Enterprise Reporter appliance. Companies can use it to compile detailed records based on a variety of parameters, such as user name or IP block, and capture the full URL of every site visited. If a PC is trying to connect back to a spyware source, it will show up in the report—giving companies the evidence of infection so they can take quick corrective measures.

## Conclusion

*Mounting an effective defense against spyware means developing and disseminating a clear acceptable use policy for employees, and backing it up with a mix of technology focusing on prevention, entrapment, and disinfection.*

Spyware has joined viruses and spam atop the list of critical security concerns for businesses. It can easily and surreptitiously implant itself on user PCs—whether as part of a legitimate software download, a “drive-by” download from a suspicious Web site, a pop-up window, or even as part of “anti-spyware” freeware masquerading as a solution. Once it infects a system, it can report back to its source on user activity, opening a back-door channel through which valuable corporate and personal data can be lost. It also reduces employee productivity and wastes administrative resources—issues that go directly to a business’s bottom line.

Spyware also is likely here to stay. Disagreement over how to define it has hindered both industry and legislative efforts to combat it, while giving encouragement to its creators and others who profit from it—whether they’re legitimate companies or criminal enterprises.

Mounting an effective defense against spyware means developing and disseminating a clear acceptable use policy for employees, and backing it up with a mix of technology focusing on prevention, entrapment, and disinfection.

The R3000 Enterprise Filter and Enterprise Reporter from 8e6 Technologies can play a critical role in a company’s anti-spyware strategy. The R3000 features filter parameters and blocking technologies that stop spyware from phoning home to its source, so that sensitive information never leaves the network. An extensive and regularly updated library of known spyware URLs keep companies ahead of the latest threats, while Intelligent Footprint Technology reduces the risks posed by IM and P2P connections. Scalability, simple setup, and an open-source operating system all help to ease administration and configuration, while performance is never an issue. Meanwhile, the Enterprise Reporter helps companies track user activity to detect the presence of spyware programs.

Stealth makes spyware inherently difficult to defend against. But when deployed as part of a comprehensive anti-spyware strategy, solutions from 8e6 can help companies neutralize the threat.



For more information on 8e6 Technologies and 8e6 appliance-based solutions for Internet Filtering, Web-use Reporting, and Spam Control, visit [www.8e6.com](http://www.8e6.com).