

Industry Standards and Other Next Steps to Securing Networks in a Spyware World

By **Tori Case** and **Sioux Fleming**

SPYWARE represents an astonishing security risk and is getting worse every day. It represents a multi-million dollar black market¹ that is threatening the very nature and usefulness of the Internet as a vehicle for information exchange and e-commerce. Revenue figures taken from public filings by adware companies show that for one company alone, Avenue Media, 2 million PCs running its software brought in \$7m of revenue per year.² Further, deceptive and often clearly illegal software download practices are a regular part of the business of many American companies operating in online commerce. These practices are funded and given incentives through poorly policed download commission programs, programs that, in turn, are funded by large, mainstream advertisers.³

The threat to companies of all sizes is increasing rapidly as spyware, adware, and other non-viral malicious programs continue to proliferate and become more complex. Spyware does more than just steal information about your employees' computing habits, or worse still, confidential employee or customer data. It also robs your system of speed and efficient Internet access.

Controlling spyware in a business-computing environment can be a difficult task. Unlike viruses, which all seek to cause harm, spyware seeks to profit off the continued operation of a computer. It is not always evident and can range from simple adware to sophisticated, backdoor hacker tools. Spyware and adware also present serious threats to internal productivity⁴.

PCs affected by these programs may slow to a crawl, impacting all business operations. Frustrated users flood your help desk with calls, and manual identification and removal of unwanted applications can reduce the amount of time that IT staff can dedicate to strategic business projects.

According to recent data from Osterman Research, thirty-four percent of companies are having significant problems with spyware⁵. And yet, a majority of corporations remain complacent and in many instances are not paying attention to, nor responding to changing security threats. By some estimates as few as 20 percent of enterprises are

actively responding to the spyware threat either by assessing their security risk or implementing anti-spyware solutions.

A belief by some that antivirus makers will solve the problem for them if they just wait, and lack of budget to invest in an anti-spyware solution are major reasons for the lack of action. So too is the fact that spyware is not always perceived as a security issue, despite a continuing onslaught of increasingly sophisticated attacks. In June this year a "bundled" threat involving spyware began by spamming out a downloader—8 different kinds were sent out at hourly intervals. In step 2, the downloader killed the firewall and antivirus protection and also installed filters to stop the machines from running antivirus updates. In step 3 it downloaded an actual Trojan, turning the machine into a proxy.

The end goal of such an attack is to create a network of zombies; a botnet, which can then be rented out. Typically botnets have been used for spam and online extortion. Now they are more commonly used to install adware and to make money.

Despite such threats, spyware continues to be viewed by some corporations solely as a productivity problem affecting the help desk. Clearly spyware has the ability to impact both security and productivity.

Just as the threat from spyware continues to escalate and become more complex, the battle against spyware continues to increase in complexity. A number of initiatives are necessary to help combat the problem:

- ▼ *Development and agreement on an industry definition for spyware*
- ▼ *Certification of anti-spyware products using a standardized test bed*
- ▼ *Legislation and active prosecution under existing federal and state laws*
- ▼ *Education within the enterprise from the C-level down coupled with systematic auditing by businesses for risk and security preparedness*

▼ **Implementation of policies and enterprise strength product solutions to combat spyware.**

DEFINING SPYWARE

Notice, consent and control remain central to agreeing on a definition for spyware, and a new group called the Anti-Spyware Coalition run by the Center for Democracy and Technology (CDT) recently released a draft definition for public comment. Their definition characterizes malicious non-viral code as “spyware and other potentially unwanted technologies.”

Agreement on a workable definition for spyware is a necessary prerequisite for the anti-spyware industry to take the next step toward the development of products that perform according to agreed performance parameters, and are certified according to an industry standard test bed.

A common acceptance of what does and does not constitute spyware will also free anti-spyware vendors from time spent defending themselves against spyware vendor’s legal challenges, and allow them to spend time developing more robust products that will provide users with the choices and tools they need to deal with spyware.

A definition will also aid federal and state legislators as they grapple with how to legislate and prosecute bad behavior rather than the technology. The problem is one of context and the development of anti-spyware products that can give users the flexibility to decide what goes and what stays on their computer.

Clearly at this point, the burden still rests with IT to decide what is and is not spyware, and therefore what is and is not appropriate and safe on their system.

STANDARDIZATION AND CERTIFICATION NEEDED

Product reviews remain a powerful source of information, but as with much else in the world of spyware, the review process is still not standardized, and there are as many “false” reviews in the public domain (generated by spyware purveyors)⁶ as legitimate, albeit inconsistent or meaningless, reviews.

Reviews of anti-spyware by recognized technical publications such as PC Magazine or Secure Computing Magazine, are conducted according to each publication’s set of criteria. This means results often are contradictory and confusing, even to an IT audience.

IT managers need to remain aware that each vendor has a different “black list” of offending spyware applications and code. Ultimately the apparent effectiveness of any vendor’s solution depends on the test bed being used for a particular review. Testing needs to reflect real-world situations and the flexibility and customization needed in differing enterprise environments.

IT managers need to know whether the review also tested the product’s ability to remove spyware, not just identify it. Does the product allow spyware to be identified and held for a disposal decision? Can the product be customized to reduce false-positives? Does the review clearly distinguish between standalone products and true enterprise products?

Similarly, certification of anti-spyware products; recently begun by West Coast Labs through its company Checkmark, certifies products on their ability to detect spyware and to not report false-positives; as measured by Checkpoint’s spyware test suite. No mention is made of spyware removal, and yet it is the removal of spyware that is the most difficult.

Independent certification of all anti-spyware products, using an industry-agreed test-bed, is a necessity similar to the accepted practices in other like industries. The antivirus industry went through the same transition to standardized testing and certification in the early 90s. And today, virtually every antivirus product is tested by two organizations: the antivirus product developer consortium (AVPD) and the publication *Virus Bulletin* out of the UK.

LEGISLATION AND PROSECUTION

An increasingly complex web of state bills and laws are outlawing spyware and setting tighter security and disclosure standards for financial services firms and commercial data aggregators. In fact, most spyware practices are already illegal under deceptive-business laws but to date federal and state law enforcers have sued relatively few spyware purveyors.

In May 2005 the U.S. House of Representatives also passed two anti-spyware bills, which if they are in turn passed by the Senate, will establish new penalties for those who use or distribute spyware that disables users’ computers and secretly monitors their activities.⁷

The bills (The Securely Protect Yourself Against Cyber Trespass Act (SPY Act) and the I-SPY Act), while differing in their approach to the spyware problem, would impose jail sentences and multi-million dollar fines. Specifically the bills outlaw a number of practices associated with spyware such as reprogramming the start page on a user’s Web browser, logging keystrokes to capture passwords and other sensitive data, or launching pop-up ads that can’t be closed without shutting down the computer. The use of stolen data to commit other crimes such as identity theft would incur even stiffer penalties.

The development of an agreed definition for spyware, based on its ability to covertly collect and transmit user information, its ability to resist un-installation, as well as the unwitting or unknown downloading of spyware by users, will provide anti-spyware vendors with a clear aim in developing tools to block and remove these programs.

EDUCATION WITHIN THE ENTERPRISE FROM THE C-LEVEL DOWN COUPLED WITH SYSTEMATIC AUDITING FOR RISK AND SECURITY PREPAREDNESS

Awareness and commitment to containing the risk from spyware among some C-level audiences remains low. While those in the banking, financial, and health care services industries have been forced to respond to legislation such as Sarbanes-Oxley, HIPAA and in at least one state (California), security and disclosure standards in the event personally identifiable consumer data is stolen or compromised, many other industries apart from high tech and government (county, state and federal), continue to adopt a wait and see approach, or view spyware solely as a productivity concern.

The reality however, is that when pests enter a business, they have the potential to introduce significant legal liabilities (particularly in regulated industries), compromise trade secrets, and damage corporate reputations—all at a cost to the business.

Anti-spyware solutions need to be incorporated as part of a multi-layered security strategy that also encompasses regular auditing for risk and security preparedness. Anti-spyware tools that are interoperable with, and complement traditional security technologies, including antivirus, anti-spam, firewall and intrusion detection systems, serve to provide an additional level of protection.

IMPLEMENTATION OF POLICIES AND ENTERPRISE STRENGTH PRODUCT SOLUTIONS TO COMBAT SPYWARE

Ultimately, it will be the widespread and consistent use of technology that will most effectively address the spyware threat. Successful defense requires established management policies and procedures and an automated anti-spyware solution that offers flexibility, low maintenance, and centralized controls.

Policies

Developing policies that will guide installation and application of that technology is a first step. Decisions such as whom to protect first may be a financial reality, driven by budget. Is one group of employees more vulnerable because of the way they work; for example remote users operating beyond the firewall? Or is there a particular division which processes highly confidential data, and which would be more seriously affected by a spyware attack?

Scanning the network to identify what technologies and applications are being used legitimately, and what applications exist that may be opening a security hole in the network, is a further integral step in building a picture of your network that will enable IT to develop user and security guidelines.

Part of the challenge in defining spyware is that in a number of instances an application may only be categorized as spyware if the user is not aware it is present and did not invite it onto the network or their PC, or if it is being used for nefarious purposes.

RATS are often used by IT company-wide to enable help desks to solve problems. Therefore, while hacking tools and password crackers may be legitimate if installed and used by IT or engineering, they are unlikely to be legitimate if found on a PC in accounting or marketing.

Spyware also finds its way onto users' PCs and the network in much simpler and innocent ways. Part of the IT challenge, again, is identifying those practices and applications on your network environment that are providing the opportunity for spyware to invade.

What free utility or browser helper object has someone downloaded, or who in your company is using file sharing applications such as KaZaa to legitimately exchange large files that are too big to send as email attachments?

The user's objective may be pure business, but the results can pose real security and productivity costs. For example, free compression and unzipping software uses social engineering to get itself installed, and exists as the "perfect" alternative to WinZip, a popular application that requires purchase of a license to use. The free software does what it claims, it zips and unzips files, but it also tracks and records what users do on their PCs and transmits that information to an external server.

Setting policies therefore is a combination of user education regarding what can and cannot be downloaded or installed and which behaviors are risky, as well as providing people with the tools they need to do their jobs, whether that is increased network storage space, or increased licenses for legitimate applications. The IT infrastructure must support its users.

Products

The aim of any enterprise-grade anti-spyware product is to prevent unauthorized access, information theft and diminished system performance by eliminating spyware from your PCs and proactively protecting against emerging threats in a heterogeneous environment without impacting productivity, and using existing corporate resources.

To effectively manage in today's spyware environment, corporations and large-scale organizations require a single, comprehensive anti-spyware solution that enables proactive detection, removal and management. This solution must provide timely spyware updates to prevent security incidents from affecting daily business transactions, and the power and flexibility to define and quickly modify or re-define what is identified and removed as spyware, according to changing business needs and definitions.

Centralized management via a console ensures minimum resources are required for ongoing management, and affords easy installation, deployment and administration across any sized business. It should allow administrators to enforce scanning and update policies, review logs, create reports and deploy new users for streamlined security management.

End-users are effectively removed from the process, as administrators launch scans on-demand, at scheduled times or when users login to the network, and remove pests without any action by end users. A centralized enterprise product should also enable IT to push updates to each workstation, eliminating the need for the end user to download updates over the Internet, or for administrators to personally visit each PC in the enterprise.

Automatic quarantining or deleting of pests and the ability to restore pests from quarantine is also desirable, as is the ability for IT to create "safe lists" or exclusion files of authorized applications, fine-tuned by department or individual, to prevent false alarms.

An effective anti-spyware solution also should provide the ability to generate customized reports that consolidate pest detection reports into a single log for improved management and problem isolation, and to assist with risk evaluation, even for remote users.

Flexible architecture in a product should also be considered. There are a number of situations when IT will want to deploy and administer both a stand-alone, enterprise grade product and a fully networked version. There may be parts of your business that are not connected to the corporate network (individual retail outlets for example), but which require anti-spyware protection, or employees who also work on a PC from home and connect to the network. In other instances an organization may have a vested interest in maintaining the integrity of the network, and wish to install standalone anti-spyware products on "external" PCs, even though they do not control or own many of the PCs connected to their network.

CONCLUSION

There is little doubt that spyware is a growing and potentially lethal threat to the future of the Internet and to business. According to IDC, Spyware is not going away. It is not a malicious hacking challenge for programmers; rather, it is a moneymaking revenue source for legitimate corporations.

The agreement and adoption of an industry-wide definition for spyware that can also be used to formulate effective legislation is overdue. Without such a definition, the anti-spyware industry is severely hampered in its efforts to develop industry-standardized products and to stand up to legal attacks from those they have identified as purveyors of spyware. Users and IT meanwhile are faced with a constantly moving target they must attempt to protect against.

Legislation and more frequent prosecution under existing laws are needed to maintain pressure on spyware purveyors and those who are affiliated with them, knowingly or unknowingly.


Anti-spyware products need to be tested as antivirus products are today. There needs to be a designated test bed and three parts to any certification testing:

1. Clearly defined testing criteria
2. Test detections
3. Test removals

Only then can IT managers know that the products they are buying and installing will do what they claim to do.

Education within the enterprise and the development of policies to guide how employees interact with the Internet is an ongoing challenge for IT and for the anti-spyware industry. IT infrastructure and policies must support the implementation of anti-spyware technology.

Finally, consistent and widespread use of enterprise-grade anti-spyware products that provide the necessary management features must become the norm for all businesses and organizations.

Without all of the above taking place, computer users and businesses will be the ultimate losers. The anti-spyware industry and legislators will continue to be distracted by a murky definition for the problem they are attempting to combat and spyware purveyors will continue their deceptive practices, costing business millions of dollars through reduced productivity and data theft. 

NaSPA member Tori Case is Director of Security Management Products for Computer Associates International, Inc.

NaSPA member Sioux Fleming is Director of Enterprise Management Products for Computer Associates International, Inc.

¹ One recent article cites estimates between \$500 million and \$2 billion. See Joseph Menn, Big Firms' Ad Bucks Also Fund Spyware, L.A. TIMES, May 9, 2005.
² Adware-infected PCs net slimware firms \$3 a pop, by John Leyden, 2/2/2005. http://www.theregister.co.uk/2005/02/02/adware_market_estimate/
³ Ari Schwartz Senate Testimony on "Spyware" May 11, 2005—www.cdt.org/testimony/20050511schwartzspyware.pdf
⁴ Testing by CA Security Advisory Team showed that a computer compromised by as little as two adware applications could take more than 14 minutes to boot. Assuming that employees reboot their computers daily and work five days a week for 50 weeks, every employee with a compromised machine could lose nearly 60 hours a year simply waiting for his or her computer to start.
⁵ Spyware: The Problem Grows by Demir Barlas, Line56, July 26, 2005. <http://spywarewarrior.com/asw-test-guide.htm>
⁷ U.S. House Votes to Outlaw Computer Software—eWeek http://www.eweek.com/print_article2/0,2533,a=152596,00.asp
⁸ IDC Worldwide Spyware 20004-2005 Forecast and Analysis: Security and System Management Sharing Nightmare by Hwasun Lee, Christian A Christiansen and Brian E. Burke, November 2004