InfoWorld
GET TECHNOLOGY RIGHT

UPDATED

IT Strategy Guide

Spyware

INSIDE

Updated February 2006

Introduction

WHETHER YOU'RE REFERRING TO ADWARE — supposedly benign applications that users download in exchange for agreeing to see ads or provide marketing information — or the more dangerous spyware, unwanted software is running rampant in today's enterprises. More than 92 percent of IT managers polled said that some or all of their PCs were affected (or is that infected?). Although awareness of the social, technological, and security dangers of spyware is still growing, the damage is being done today — and spyware is evolving faster than countermeasures.

While vendors quibble about definitions, some of the best-known adware and spyware products are worming their way into your PCs, everywhere on your network. The CoolWebSearch utility, affiliated with more than 1,000 Web domains, exploits unpatched browser holes to install itself. When installed, it slows PCs, changes bookmarks, pops up ads, and redirects search-engine queries.

Another popular non-favorite, Claria's GAIN (Gator Advertising Information Network), overlays ads onto Web pages, tracks what sites your employees are visiting, causes crashes, and impacts PC performance.

The dangers of spyware are growing as key loggers, phishing scams, and other malicious activities begin using this newer delivery method. You can't place your trust in individual end-users' decisions to install an anti-spyware tool. Just as with other security software — firewalls, anti-virus, and anti-spam — it's time to choose a centrally managed, policy-based solution.

The challenge is that there are few enterprise-ready tools to choose from, in part because there's little agreement as to exactly what spyware is and how to combat it. A relatively new industry group, the Anti-Spyware Coalition, hopes to change that. However, such efforts have been tried before; a similar group, called the Consortium of Anti-Spyware Technology Vendors, fell apart earlier this year. For now, the spyware makers have the upper hand while the tech industry remains in disarray.

One weapon in the hands of the black hats isn't even technological. The EULA (end-user license agreement) that many users blindly accept when downloading or installing new software apparently gives malware makers licenses to spy. That's why notorious purveyors such as Claria keep claiming that because users give their consent, their software isn't actually spyware at all. But your employees can't be relied upon to study the fine print and make the right decision every time they install or upgrade software. Something has to be done. But who will do it?

The "who" might be the government. As this guide explains, Congress is considering a number of bills focused on battling spyware. Although certainly not perfect, they may be steps in the right direction, especially because some of the challenges facing anti-spyware efforts may be legal, rather than technological. But no matter how we define the challenge, the truth remains: It's our job to fight it.

For more InfoWorld articles about spy ware, visit infoworld.com/techindex/spyware.html.

— Alan Zeichick

See the full selection of *InfoWorld* "IT Strategy Guide" reports at www.infoworld.com/store.

Spyware Infiltrates the Enterprise

DESKTOPS LITTERED WITH POP-UP ADS, COMPUTERS grinding to a halt under the weight of snoopy software, private data snatched off networks and sent to a server somewhere in Siberia or San Francisco ... all these unfortunate occurrences can be attributed to spyware, a generic term for software that regularly collects demographic and usage information from a computer and transmits it to a marketing company or other interested parties without the user's explicit permission.

Spyware is far more intrusive than spam and can cause more real problems than many computer viruses. The more benign versions — sometimes called adware — confine themselves to downloading and displaying "targeted" ads and may only be resource hogs. But many spyware applications go farther. They auto-update themselves, alter system configurations, download and install additional software, and access and disclose data stored on computers they infect — or on any shared network resources that the affected computer can access.

ISP EarthLink offers subscribers a free spyware scanning service. Of the more than 2 million computers scanned between January and September of 2004, one in three harbored spyware, with an average of 28 spyware programs per infected machine. Hardware vendor Dell says 12 percent of the support requests it receives concern spyware. Dell and EarthLink believe their respective support calls and scan requests come mainly from home or small-business users. Are enterprise networks spyware-free?

According to the results of a survey conducted on behalf of enterprise security vendor Secure Computing by independent research company TheInfoPro, only 25 percent of polled enterprise IT managers thought spyware was a major problem. That was not the response Tim McGurran, president and COO of Secure Computing, was expecting.

"Frankly, we were surprised that so few enterprises appear to be worried about spyware," McGurran says. "Statistics definitely show that spyware is a serious problem in the enterprise. Equally disturbing was that the majority of the respondents also said that they have spyware policies in place in their organizations but that the policies aren't really enforced."

Secure Computing's survey didn't ask IT managers whether spyware was or had been present on their systems. A poll by Harris Survey did ask, and 92 percent of polled IT managers said their organizations had been infected with spyware — with an average of 29 percent of their corporate PCs infected.

Because both surveys were conducted according to accepted rules of research, we're left with a conundrum: IT administrators admit a large percentage of enterprise computers have been infected and yet insist spyware isn't a real problem. Enterprise security vendors themselves have only recently begun to take spyware seriously, meaning that the best software for detecting and removing spyware still originates from a handful of small, relatively obscure software vendors.

"When a company loses a significant amount of money — or is the victim of a demonstrable case of corporate espionage — and it makes a major impact in the newspaper, then corporations will take notice," says Bruce Schneier, founder and CTO of Counterpane Internet Security. "My guess is that this kind of thing is already happening and will happen with a greater frequency in the future. Criminals, from lone criminals to organized crime, have discovered spyware."

Spyware or Adware?

Businesses aren't ignoring the spyware issue, but it's not high on the agenda, says Kevin Harvey, senior technical consultant at technology consultancy Forsythe. "Part of the problem is that spyware isn't as well understood as other security risks," he says.

The confusion over what spyware is — a plague from the darkest corners of the Internet or a nice software present with a small catch from the marketing world — and the slight but legally actionable difference between it and its less malicious sibling adware make it difficult to develop solutions and strategies to deal with the problem.

Claria, which distributes the Gator software that some refer to as spyware, in 2004 filed a libel suit against an anti-spyware program vendor. The suit was settled out of court when PC Pitstop removed information critical of the company and its software from the PC Pitstop Web site. Claria insists that Gator is not spyware because the software's behavior is clearly explained in end-user licensing agreements and the people who use Gator software know they are providing their personal information in exchange for free software. Claria claims it currently "serves" more than 43 million consumers who have agreed to receive advertising.

Claria's argument was borne out during a recent security scan of an enterprise network by Blue Coat Systems, a company that manufactures proxy appliances that control how employees use the Internet. Blue Coat offers companies a free service called a Web Traffic Assessment. During an assessment, Blue Coat installs a proxy appliance onto the network without any policy controls, allowing the appliance to simply log all Web activity taking place on the network. Steve Mullaney, vice president of marketing at Blue Coat, says this has been very effective in helping some large companies identify spyware on their networks.

"Blue Coat recently ran a Web Traffic Assessment for a large Fortune 500 enterprise manufacturing company and found out that the No. 1 visited Web site in the corporation was Gator.com," Mullaney says. "Management did not know what Gator was, and when we told them it was adware/spyware, they were shocked, to say the least."

How did Gator get on those machines and drive that traffic? Because Blue Coat can pinpoint individual users, management asked some users whether they knew they had spyware/adware on their machines. Surprisingly, the users said yes, they did know. In fact, they had installed Gator and explicitly agreed to receive aggressively served ads in exchange for Gator's e-wallet application.

"After further probing by IT staff, one user says, 'Well, I wouldn't install adware on my computer at home,' " Mullaney says. "The IT staff then learned that some of the users didn't want to slow down their home PC or home Internet connection with adware. The CIO was not amused."

So Claria may be right — some users know what they're getting, and there may be some difference between adware and spyware. But does this matter to anyone but Claria and the people contacted by the company's lawyers? Some security experts say it does.

"It's necessary to understand the difference between adware and spyware when addressing how these programs are getting onto corporate networks," says Gregg Mastoras, senior security analyst at Sophos, a security application vendor. "Adware is usually deliberately installed by a user. It is a noisy application, clearly announcing its presence on a computer through advertisements. You prevent it through policies and user education."

But spyware, Mastoras says, is stealthier. "Spyware usually installs itself without permission via holes in software or doesn't come with a clear explanation of its purposes. Spyware is a subtle, under-the-radar application that wishes to remain unnoticed so that it can collect data without interference," he says.

Aggressive spyware variants pose a severe threat, particularly for companies that subsist on sensitive data. "I know of one major HMO that has a 10-person staff dedicated solely to the eradication of spyware because they feel it is such a risk to their HIPAA compliance," says John Bedrick, group product marketing manager of system security at McAfee. "We also worked with a major financial institute that was hacked. User IDs and passwords were gathered by spyware and transmitted to a third-world country, and the company's network was then hacked with remote administrative tools."

Begone, Scum

So what strategies should enterprises use to fend off spyware and adware? As with any vexing problem that has security implications, the solution derives from a combination of policy and technology.

One approach is simply to jettison Internet Explorer. The majority of adware and spyware works only on computers running Microsoft's operating system and Web browser. Some experts advise switching to the Mozilla's Firefox Web browser to cut down on "drive-by installs" — that is, spyware that installs itself without users' knowledge or explicit permission.

Security experts agree, however, that spyware is sneaking onto corporate desktops largely as a result of user behavior. "Spyware has many vectors, but the critical issue is that the door is opened by user actions. If end-users are allowed to install software and to freely browse the Web, the enterprise is exposed," says Richard Stiennon, who until recently was a lead security analyst at Gartner and is now vice president of threat research at Webroot Software, a security software vendor.

Policy enforcement should ensure that good users don't do bad things such as installing silly programs on their desktops or running file-sharing applications that typically harbor a slew of spyware. And good patch management polices should prevent sneaky programs from installing themselves on a computer without the user's knowledge via security holes in operating systems and Web browsers.

Yet as Sophos' Mastoras notes, "End-user behavior generally triumphs over protection, patching, and policies. Few organizations are able to actually enforce the policies they create."

Factor in human behavior, and conventional security technologies alone aren't up to the task. "Typical large enterprises have firewalls and anti-virus but lack protection at the application layer. More specifically, they lack HTTP protection, which most spyware uses as its primary mode of communication," Blue Coat's Mullaney says. "Firewalls have traditionally focused on ports and, to some extent, protocols but have no visibility into content. Furthermore, attempts to extend anti-virus scanning to HTTP historically have failed due to poor performance and false positives that resulted in poor Web experiences for the end-user."

Enterprise anti-virus vendors such as McAfee, Sophos, and Symantec say they are bolstering their applications' capabilities of blocking and/or removing spyware and adware. But vendors that offer targeted enterprise anti-spyware apps point out that their products provide a good complement to anti-virus applications, offering focused, comprehensive protection against a specific threat.

Unlike anti-spyware products designed for home users, enterprise editions are fully automated, sweeping the network for infestation however often IT chooses to set the program to scan (most vendors recommend a daily sweep). Spyware can be automatically removed or remotely quarantined, as an administrator chooses.

Enterprise anti-spyware applications such as Webroot Spy Sweeper Enterprise and PestPatrol Corporate also allow system administrators to fine-tune spyware protection by defining safe lists of applications that users can install or run, a feature not yet offered by anti-virus applications. Certain or all types of cookies can be permitted.

The applications can also inoculate networks, automatically blocking the installation of known spyware. Because one person's spyware is another's useful application, each company can configure auto-blocking to suit its enterprise.

"Good security requires defense in depth," Counterpane's Schneier says. "There's no 'benefits of inoculation vs. scanning' argument with spyware; a smart company does both. Security is always a trade-off, and companies always have to weigh the costs of loss vs. the costs of risk mitigation. In this case, it's a no-brainer. There are easy — and cheap — tools that drastically reduce the risk of spyware."

Counting on Countermeasures

Enterprises may find these tools preferable to draconian measures such as preventing users from installing any applications on their computers. Paul Bryan, director at Microsoft's security business unit, says that the company is addressing the core issues of deceptive software with the goal of ensuring that what's happening on an individual machine is recognized and controllable.

"Microsoft's new IE pop-up blocker is turned on by default and cuts down on a key way consumers are enticed and tricked into downloading deceptive software. And unsolicited downloads are now blocked by default," Bryan says. "We also added additional group policy controls that allow administrators to block downloads in the intranet zone."

Bryan acknowledges, however, that "XP [Service Pack 2] is not the complete solution by any means. As with most security challenges, there is no silver bullet, but it represents the kind of technology solution that we believe will help all of our customers deal with the spyware problem."

Most security experts agree that Windows XP Service Pack 2 does a good job hardening its OS against spyware that installs without explicit user permission. And just in time, too. Security experts believe that spyware is quickly getting creepier and more capable.

"We are in the very early stages of spyware," Forsythe's Harvey says. "Spyware is likely to become even more stealthy and capture more information as current code is refined. I believe we will hear many horror stories in the coming months about confidential corporate information being divulged through spyware."

— Michelle Delio

Spyware’s and Adware’s Real Effects

NEITHER USERS NOR EVEN IT ADMINS MAY FULLY grasp what impact this spyware and adware could have on individual systems — even fully patched ones.

InfoWorld decided to install some of the most popular spyware and adware programs to assess just how damaging they could be. First, I set up a fully patched Windows XP Professional SP2 client honeypot with various in-band and out-of-band monitoring tools. Next, I installed free games found on various Web sites, including zango.com and yahoogamez.com. I also installed some free p-to-p programs known for installing unwanted programs, including BearShare.

In short, I put my honeypot in harm’s way. Although Windows in its default state should prevent a lot of spyware and adware from being loaded, if the user intentionally installs untrusted executables, even the latest patches won’t help.

To be fair, almost all of the programs installed contained information stating their “behind-the-scenes” intent, but this was only apparent if you took the time to read the licensing agreement or Web site FAQ.

Rogues’ Gallery

Spyware and adware come in various forms, all of which are capable of annoying and potentially destructive feats.

Name	Marketscore	ComSpySysSvr	NTLogonCapture	CWS	Zango
Aliases	Internet Accelerator	CSS Server	none	CoolWebSearch	Zanu
Supposed use/source	Internet download accelerator	Activity monitoring (found in Trojan graphics program)	Installed secretly using IE vulnerability	Installed with spyware-scanner program	Game
Exploits software vulnerability	N	N	N	P	P
Modifies registry	Y	Y	Y	Y	Y
Modifies Internet Explorer	Y	N	N	Y	Y
Installs proxy service	Y	N	N	Y	N
Downloads more files	Y	Y	N	Y	Y
Steals passwords	P	P	Y	P	N
Records personal information	P	P	N	P	P
Captures screen	N	Y	N	N	N

NOTE: Y = Yes, directly, N = No, or not obviously, P = Possibly, because of the mechanism, but not a directly coded feature

Not surprisingly, what I found was no less disturbing. A single installed “free” program, Poker-Party, installed dozens of other programs. Many of those programs existed only to download other programs, which downloaded other programs — all from varying Web sites.

Analyzing one program, TopRebater, I found over 200 different download links. Connecting directly to those links often just downloaded a list of hundreds of other new links. Perhaps most distressing was the fact that many of these links seemed to point to compromised home-user computers.

The downloaded malware came in as executables, compiled help files, HTML applications, files disguised as graphics that were really executables, encoded Web pages, and scripts. Several of the programs attempted to exploit known vulnerabilities in Windows and Internet Explorer, and one was designed for Mozilla Firefox. Most of the vulnerabilities were patched but not all.

As expected, these programs made dozens of system modifications, including adding to the Windows Registry key, modifying files, dropping new malware executables, sending e-mail, starting hidden and encrypted IRC messaging, installing new desktop icons, and stealing personal information.

Other programs, such as NTLogonCapture and Act-

Mon, found in freeware games, also looked for password files, recorded them, and sent them to remote locations. Several of the programs installed key-logging Trojans.

IE was a heavy target. Malware modified its toolbar and search capability, installed pop-up ads, and enforced new home pages. One of the most interesting techniques modified the browser such that keywords typed into the browser or appearing on Web sites would cause a screen capture to be taken.

Lesson learned: Even your fully patched computers can be compromised if end users are allowed to install untrusted software or visit untrusted Internet locations.

— Roger A. Grimes

Time to Own the Spyware Problem

LAST YEAR, FORRESTER RESEARCH RELEASED "ANTI-Spyware Adoption in 2005," a study by analyst David Friedlander with Natalie Lambert, that included some surprising stats. What struck me most was that 39 percent of respondents, dubbed "technology decision makers," did not know the percentage of desktops infected with spyware in their organizations. Perhaps they didn't know because 56 percent were unsure of what percentage of help desk calls were related to spyware issues.

IT departments cannot hide their heads in the sand. If you ease your conscience by telling end-users to install anti-spyware software, you are only fooling yourself.

The Forrester report says that, on average, 7 percent of all help desk calls are made in response to spyware infections; Dell's own estimate is 20 percent.

As an exercise, take 7 percent of the number of support calls you received last month and multiply that by what you believe the average cost of a single call is. (Dell claims $35 per call, on average.)

I spoke with Forrester's Friedlander on this issue, and he didn't paint a happy picture. Spyware, he says, is getting more prevalent — and more malicious — on desktops.

"The big thing with spyware is it is financially motivated, which is not usually true of viruses," Friedlander says.

Although key loggers are being used to steal personal passwords and credit card numbers today, who's to say they won't be used for full-fledged corporate espionage tomorrow?

Andy Ostrom, director of marketing at InterMute, makers of SpySubstract Enterprise, also notes that browser-hijacking software is getting tougher to remove. If you don't get every last bit of code, it comes back.

Scarier still, according to Ostrom, InterMute has seen phishing attacks move from e-mail into spyware. A spyware application might pop up a dialog that warns you of a problem with your account only to redirect you to a look-alike site.

Steve Workman, director of product management at LANDesk Software, says that fobbing off the problem to the end-user is extremely shortsighted. Relying on end-users to decide what is and isn't spyware doesn't really protect the organization. And, as any IT manager knows, just having end-users install an application can turn into a disaster. Imagine 10,000 users clogging up the network by installing individual anti-spyware applications and downloading spyware definitions.

LANDesk Security Suite centralizes spyware definitions and updates in one spot. LANDesk's subscription service keeps an up-to-date content list of new spyware definitions as they become known and sends customers updates.

LANDesk, as it turns out, is mostly owned by Intel. Workman tells me his company is participating with the giant chipmaker in its Active Management Technology initiative, which will provide management capabilities at the chip level, allowing IT to manage a device before the OS loads. For example, if policy dictates that a machine needs to be at a certain patch level, Active Management will keep spyware under control even before the machine is logged on to the network.

Nevertheless, you can't let Intel or end-users fight your battles for you. It's up to IT to take charge of the spyware problem now before it morphs from an annoying end-user problem into a full-blown corporate crisis.

— Ephraim Schwartz

Internet Sieges Can Cost Businesses a Bundle

WHEN THE FIRST EXTORTION E-MAIL POPPED INTO Michael Alculumbre's inbox, he had no idea it was about to cost his business nearly $500,000.

The note arrived in early November of 2004, as Alculumbre's London-based transaction processing company, Protx was being hit by a nasty distributed denial of service (DDoS) attack. Zombie PCs from around the world were flooding Protx.com (the company's Web site) and the transaction processing server that was the commercial heart of the business.

In extortion e-mail's broken English, someone identifying himself as Tony Martino proposed a classic organized-crime protection scheme. "You should pay $10,000," Martino wrote. "When we receive money, we stop attack immediately." The e-mail even promised one year's protection from other attackers for the $10,000 fee.

"Many companies paid us, and use our protection right now," Martino said. "Think about how much money you lose, while your servers are down."

The Protx attackers had one thing right: online attacks can be expensive. A 2004 PriceWaterhouseCoopers survey of more than 1,000 businesses in the U.K. found that, on average, companies spent more than $17,000 on their worst security incident that year. For large companies, that amount was closer to $210,000, the study found. For companies of either size, most of the loss was due to the disruption in their ability to do business, with expenses for troubleshooting the incident and actual cash spent responding to it accounting for considerably less.

It's Expensive

Law enforcement authorities told Protx that it was the victim of Russian organized crime, Alculumbre says, but criminal extortion is not the only motivation for such attacks. In April 2005, Australian anti-spyware vendor PC Tools became a target of spyware companies that didn't want users interested in PC Tools' spyware-cleansing software to reach the actual PC Tools Web site.

Simon Clausen, CEO of PC Tools.Customers whose PCs had already been infected by spyware were greeted with fake pop-up windows and shopping carts when they tried to purchase the company's Spyware Doctor product, says Simon Clausen, PC Tools' CEO. Instead of buying his company's anti-spyware software, they were tricked into purchasing useless products that left their computers infected, he said.

Even links that appeared to be from legitimate Web sites like Google or Download.com were modified on fake pages displayed to users, Clausen said. "Any link that said Spyware Doctor would be redirected to the attackers' sites."

Clausen estimates that as much as 15 percent of his company's business was lost, representing hundreds of thousands of dollars in missed sales. But the real cost was in lost productivity for his software development team, which was forced to spend hundreds of hours changing PC Tools' products and Web site in an effort to stay one step ahead of the attackers, he said. "We probably had a dozen people involved pretty heavily in it for about a month or two."

By the time PC Tools developed a way of handling the attack, the company had taken major hits in employee time and in lost business opportunities because of product delays, he said.

Online Cat and Mouse

By scrambling its IT staff and prohibiting traffic from zombie servers (at one point, Protx.com simply blocked all traffic originating from the Western United States) that company managed to survive the first wave of the attack against it.

But the 13-person company's biggest cost involved preparing for the next assaults, consisting of thousands of server requests, which came in January and April of 2005.

The April attack, which lasted for more than five days, was the most severe, as Protx and the attackers engaged in a kind of online cat and mouse: Just as Alculumbre's technicians found one way to block the flood of unwanted server messages, the attackers would switch to another tack. At one point, the cybercrooks used a new exploit of Microsoft's Microsoft Internet Information Services server that caused the Protx Web site to crash whenever certain types of secure messages got through. Protx responded by installing an SSL accelerator and analyzing the messages before letting them through.

On the final day of the April assault, the attackers hit Protx with everything they had. At the peak of the assault, the company's servers were processing 800 megabits of traffic per second, the equivalent of more than 530 T1 lines firing at full capacity.

Protx's administrators spent some long, tense hours over that weekend, scrambling with technicians from the company's Internet service provider to keep the company's Web and transaction processing server online. "It's like being in a war," said Alculumbre. "My three guys were working with three other technicians in extremely tight hosting facilities, trying to put all this bloody machinery in and wire it up... it looked like Spaghetti Junction. How they ever knew what they were doing was beyond me."

Expanding Horizons

Just a few years ago, financially motivated attackers tended to focus on fringe businesses like online gaming sites. But transaction processors like Protx are now choice prey for extortionists, according to Peter Rendall, CEO of Top Layer Networks, a security vendor based in Westboro, Massachusetts. "If you bring down your payment processor, you can bring down hundreds of [online] processors," he said. "Transaction processors like Protx will do everything in their power not to be offline; therefore, they are investing heavily in security and bandwidth."

Proportionately, online security costs are greater for smaller companies than for larger ones. According to the 2005 Computer Crime and Security Survey conducted by the Computer Security Institute and the Federal Bureau of Investigation, companies with sales of less than $10 million per year spent $643 per employee on computer security each year. For the largest companies — those with more than $1 billion in annual revenue — the amount spent on security dropped to $247 per employee.

The survey found that companies in the utilities business spent the most on computer security — on average, $190 per employee per year. Next highest on the list were transportation and telecommunication companies, with average annual costs per employee of $187 and $132, respectively.

But for companies under targeted attack, the costs are decidedly higher. Protx, for example, ended up spending a whopping $38,000 per employee on security over the past year.

Protx's Alculumbre says he had thought that his company was too small to draw the attention of organized crime, but the events of the year have taught him otherwise. "It's very alarming for us that an unknown assailant can do so much to a business that I've spent so many years trying to build," he said.

Though the first days of the assaults were stressful, Alculumbre that says he's grown more accustomed to the high costs involved. "If you're going to be in business, then you have to accept that DDoS attacks are a part of this," he says.

— Robert McMillan

Industry Tries to Unite Against Spyware

A COALITION OF TECHNOLOGY COMPANIES AND public interest organizations has hit some early milestones in its effort to combat spyware. By last October, the Anti-Spyware Coalition (ASC) had already published several documents that the group hopes will take the computer security industry a step closer toward agreeing on a set of best practices for stopping this type of annoying and invasive software.

Coalition members published a definition of the term "spyware," as well as other documents including a list of spyware and potentially harmful technologies aimed at users; a glossary defining commonly used terms relating to spyware; and safety tips about how to protect against spyware.

Spyware can be defined two ways, according to the ASC. "In its narrow sense, spyware is a term for tracking software deployed without adequate notice, consent or control for the user," the organization states in its glossary. However spyware is also used as an umbrella term encompassing not only its narrow definition, but also other "potentially unwanted technologies," the ASC adds, including harmful adware, unauthorized dialers, rootkits and hacker tools.

In its antispyware safety tips document, the ASC has six major recommendations for users to defend themselves against spyware. The organization suggests that users keep the security on their computers up to date; only download programs from Web sites they trust; familiarize themselves with the fine print attached to any downloadable software; avoid being tricked into clicking dialog boxes; beware of so-called "free" programs; and use antispyware, antivirus and firewall software.

The ASC is now seeking public comment on a "risk modeling" document that goes into technical detail about just what it is that separates spyware from any other kind of software.

Public comment is now being solicited on the risk-modeling document, and public meetings have been scheduled for Washington, D.C., and Ottawa, Canada, this year to further discuss the spyware problem, McGuire said. "One of the ultimate goals of the coalition is to come up with industrywide best practices," he said.

Though it has taken only three months to hit these milestones, getting consensus in this area has not always been easy. A similar organization, called the Consortium of Anti-Spyware Technology Vendors, fell apart in February after 16 months of effort.

The Anti-Spyware Coalition's work ultimately will help software vendors build better products that defend against spyware in a more consistent fashion, said Vincent Weafer, senior director with Symantec's Security Response team. "When we all started looking at the spyware space . . . there was no common definition of what was spyware and what was adware," he said. "It should start to align how companies behave when they look at various types of adware and spyware programs."

Symantec has already begun applying the coalition's definitions to its own products, Weafer said.

The coalition's documents will also help educate users on the subject of spyware, said David McGuire, a spokesman for the Center for Democracy and Technology, another coalition member.

Other Anti-Spyware Coalition members include Microsoft, Computer Associates, McAfee, the National

Center for Victims of Crime, and the Cyber Security Industry Alliance.

The Coalition's documents can be found at www.antispywarecoalition.org/documents/index.html.

— Robert McMillan and China Marten

A Defining Moment for Spyware EULAs

AT THE HEART OF THE SPYWARE PROBLEM LIES THE question of what constitutes proper notice and consent. As we all know, spyware purveyors claim the right to do anything as long as they give "notice" of what their software actually does somewhere in a long EULA, and their victim gives "consent" by clicking OK without reading it. So it seems a little strange to me that the Anti-Spyware Coalition would ignore this issue in its initial draft of spyware definitions.

The Anti-Spyware Coalition — a rather imposing collection of software companies and public interest groups - recently released the first draft of its Spyware Definitions consensus document designed to give anti-spyware vendors standard categorizations of unwanted software. While a noble effort, I was somewhat disappointed that the document didn't at least take a stab at defining what proper notice and consent of spyware ought to be. After all, it's the lack of a consensus on that issue that has stymied legislative attempts to come up with an effective anti-spyware law, so it would seem like one of the first issues the coalition would need to deal with.

It's not that the document ignores the problem of spyware EULAs altogether. In fact, one of the defined terms is EULA:

"End User License Agreement (EULA): An agreement between a producer and a user of computer software that specifies the parameters of use granted to the user. The software producer specifies these parameters and limitations on use, which can become part of a legally binding contract. Some companies use the EULA as the sole means of disclosure of a program's behaviors or bundling."

In a similar vein, the document's "Anti-Spyware Safety Tips" section for consumers includes a warning to read all the fine print:

"Whenever you install something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes important information such as aggressive installs or the inclusion of unwanted software in a given software installation is documented, but it may be found only in the EULA. The fine print may be the only place consumers can find notice of potentially unwanted technologies. Unfortunately, careful consumers must read all the fine print."

Well, that's true enough, of course, but it's also completely useless advice from the point of view of dealing with spyware. If everyone would read and understand every 10,000-word spyware EULA and privacy policy, there wouldn't be a spyware problem. There wouldn't be much of anything, because we'd all be too busy reading all the EULAs and all the privacy policies that we're confronted with every day. After all, you don't know it's a spyware EULA until you've read it.

Since Microsoft, Symantec, and some other big supporters of the sanctity of the EULA are members of the coalition, I suppose it's not really surprising that the definitions leave the impression that spyware EULAs are perfectly valid. The software industry is conflicted over spyware EULAs because spyware companies aren't the only ones who like to hide the real nature of the deal deep in the fine print. If spyware vendors are required to give real notice and get real consent, so might others in the technology business.

The simple fact is that the sanctity of the EULA is going to have to take a hit if the spyware plague is ever to be brought under control. Consumers can't and won't read all the fine print - they need real notice of what they're dealing with so they can give true consent. And if the Anti-Spyware Coalition is to be any more effective than previous industry-led attempts to curb the spyware menace, it's going to have to start by defining what that really means.

— Ed Foster

Government Focuses on Countering Spyware

THE GOVERNMENT IS SLOWLY JOINING THE BATTLE against spyware as three bills await approval by the U.S. Senate.

In November of 2005, the Senate Commerce, Science and Transportation Committee approved a bill that would outlaw the practice of remotely installing software that collects a computer users' personal information without consent.

In addition to prohibiting spyware, the Spyblock (Software Principles Yielding Better Levels of Consumer Knowledge) Act would also outlaw the installation of adware programs without a computer user's permission.

Spyblock, sponsored by Senator Conrad Burns, a Montana Republican, would prohibit hackers from remotely taking over a computer and prohibit programs that hijack Web browsers. The bill would protect anti-spyware software vendors from being sued by companies whose software they block.

"I am pleased that a majority of the committee agrees with me that Congress must act to protect the right of consumers to know when potentially dangerous Spyware is being downloaded onto their computers," Burns said in a statement. "As the Spyblock Act moves forward to the Senate floor, I hope we can continue making it a stronger bill by making sure the private sector has all the right tools it needs to successfully slow the spread of malicious spyware."

The Spyblock Act would allow the U.S. Federal Trade Commission and state attorneys general to seek civil penalties against spyware and adware distributors.

Also still awaiting approval from the Senate are two bills focusing on spyware, overwhelmingly passed the U.S. House of Representatives last May.

One requires many software programs collecting personal information to get permission before doing so.

The Securely Protect Yourself Against Cyber Trespass Act, or Spy Act, also would outlaw the act of taking over a computer in order to send unauthorized information or code, and diverting a Web browser without the permission of the computer owner.

The bill, which passed the House by a vote of 393-4, prohibits Web advertising that computer users cannot close "without undue effort" or without shutting down the computer, and it prohibits collecting personal information through keystroke logging.

A second bill, the Internet Spyware Prevention Act, or I-Spy Act, sets jail terms of up to five years for a person who uses spyware to access a computer without authorization and uses the computer to commit another federal crime. The I-Spy Act also would allow a jail term of up to two years for a person who uses spyware to obtain someone else's personal information or to defeat security protections on a computer with the intent of defrauding or injuring the computer owner.

The I-Spy Act, sponsored by Virginia Republican Representative Bob Goodlatte, passed the House by a vote of 395-1. Both bills would have to pass the U.S. Senate and be signed by President George Bush to become law. Both bills passed the House in 2004, but failed to make it through the Senate.

The Spy Act, sponsored by California Republican Representative Mary Bono, would allow fines of up to $3 million for spyware-like activity such as delivering unauthorized software to a computer or hijacking a Web browser. Security software updates are exempted from the Spy Act.

Unlike an older Bono bill, this version of the Spy Act doesn't attempt to define spyware, but outlaws several actions commonly associated with spy-ware.

An earlier Bono spyware bill, introduced in July 2003, broadly prohibited and defined spyware. Some software vendors, including those that market antivirus update software, objected that the definition was overly broad and could subject their services to fines.

Microsoft issued a statement praising both new bills as providing "important tools in the battle against spyware and other deceptive software." But Microsoft also called for the Senate to include language that would protect vendors of antispyware software from lawsuits by companies distributing spyware. Two antispyware companies have been sued by firms asking that their software not be removed from users' computers, with Claria, a distributor of pop-up advertising formerly known as Gator, filing a lawsuit against PC Pitstop in September 2003. Last year, Claria also asked Computer Associates International to stop its PestPatrol software from deleting Claria ad-targeting software, but CA refused.

Microsoft released its own Windows AntiSpyware software in 2005. "In its current form, these bills leave companies that are responding to consumer demand for strong antispyware tools vulnerable to frivolous lawsuits brought by the very companies responsible for the proliferation of spyware and other deceptive software," Jack Krumholtz, managing director of federal government affairs for Microsoft, said in a statement.

Others, including the libertarian think-tank Cato Institute, have opposed the spyware legislation, saying it's unneeded because the U.S. Federal Trade Commission (FTC) already has the authority to seek fines for deceptive business practices.

The new version of the Bono bill requires that creators of software that collects personal information get permission from computer users before installing the software. The consent requirement, however, has an exemption for Web sites tracking their own pages visited. The bill also gives the FTC authority to allow some software vendors to ask for permission only once, not every time their programs access a computer.

Bono's bill would also preempt any state spyware laws.

"As this nation continues to push towards a global e-commerce market-place, spyware stands to undermine the security and integrity of e-commerce and data security," Bono said in a statement. "Daily web activities by consumers have become stalking grounds for computer hackers through spyware. Consumers have a right to know and have a right to decide who has access to their highly personal information that spyware can collect."

— Grant Gross

Spyware Threat Changing Online Behavior

SECURITY CONCERNS ARE ERODING INTERNET USERS' confidence and having such a chilling effect on their online behavior that U.S. business-to-consumer sales will grow more slowly than expected in coming years, Gartner warned in a recent report.

Alarmed at the startling rise in phishing attacks, spyware intrusions, virus infections and the compromising of personal data, Internet users are limiting their e-commerce activities and this will slow down U.S. business-to-consumer sales growth between 1 percent and 3 percent in the coming years, according to Gartner.

"This concern is affecting online consumers' behavior and dampening their willingness to use the Internet to transact," said Avivah Litan, author of the study "Increased Phishing and Online Attacks Cause Dip in Consumer Confidence" released in 2005. Consequently, ISPs, financial institutions, online retailers and other companies selling goods and services to consumers via the Internet must address these concerns and put safeguards in place to protect their clients, Litan said.

Consequently, Gartner is warning that the total dollar value of business-to-consumer online sales could grow at a slower pace than the company previously predicted, by anywhere between 0.3 percent to 1 percent each in coming years, Litan said. Without accounting for the possible slower growth resulting from security concerns, Gartner expected the dollar value of business-to-consumer sales to increase 18 percent in 2005, 15 percent in 2006 and 11 percent in 2007, so each of those projected annual growth rates could fall by as much as a percentage point due to consumers' security concerns, Litan said.

Online consumers are increasingly dismayed and frightened over the rising rates of a variety of security threats. A big one is phishing, in which scammers dress up e-mail messages to make them look like they came from a legitimate organization, such as an online store or a bank. Between May 2004 and May 2005, phishing e-mail recipients grew 28 percent and about 1.2 million U.S. consumers suffered phishing-related losses totaling about $929 million, according to Litan.

This type of phishing e-mail message can cause harm in a variety of ways. For example, it can lure consumers to enter sensitive information such as credit card numbers, bank account numbers and passwords into a legitimate-looking Web site set up by scammers. Even if consumers don't enter data into the rogue Web sites, just landing there can trigger an automatic and transparent download of malicious software to their PCs.

Online marketplace eBay and its online payment unit PayPal are the two Web sites phishers most frequently try to spoof, and Citigroup Citibank is the most popular target among banks. But as large banks wise up to the scams, phishers are starting to target smaller, regional banks, according to Litan.

Another security problem frightening consumers is spyware, which is malicious software installed on a user's machine without knowledge or authorization. This type of software comes in different flavors, with some that furtively log users' keystrokes to steal passwords and other sensitive information and others that search hard drives for information and transmits it.

But the security problem online consumers find the spookiest is unauthorized access to their personal and financial information that criminals can use to steal identities and inflict serious damage to their finances and credit, Litan said. Examples of this are recent incidents of lost, misplaced or unsecured data at companies such as CardSystems Solutions, ChoicePoint, Citibank and Wachovia that could potentially affect millions of consumers.

In a recent survey of 5,000 U.S. Internet users done by Gartner, 42 percent said concerns about online attacks have affected their online shopping behavior. Among this 42 percent, three-quarters are more cautious about where they shop online and one-third buy fewer items than they normally would, Litan said.

Online banking activities are also being affected. Among the 5,000 respondents, 28 percent have modified their online banking behavior because of security concerns. Within this 28 percent, three-quarters log into their accounts less frequently, 14 percent have stopped paying bills via online banking and about 4 percent have completely given up on online banking, Litan said.

A major victim of consumers' distrust is commercial e-mail, with a majority of survey respondents saying they delete e-mail from unknown companies or individuals without even opening the messages. This trend is seriously damaging the effectiveness of e-mail as a legitimate tool for bonafide companies to communicate with their clients.

Gartner's survey also found that consumers expect the companies they do business with over the Web to be much more effective than they are now at detecting and preventing fraud. The survey also found consumers are underwhelmed by government initiatives to address online security problems, with about 66 percent of respondents saying they want laws that would let consumers opt out of having their personal data shared with third parties without their consent.

— Juan Carlos Perez