The Cost of Spyware to your Business

We know why writers of Spyware do so; for the money. Hackers, once satisfied with villainy as their reward wrote viruses, which brought them no financial gain. Now, they are going after the money, and it is enormously profitable. Profitability also means that writing malicious code has become attractive to well-financed organized crime, and perpetrators of industrial espionage. If it is not already being used as weaponry, it will be so used, eventually. According to a report by Special Agent Wendi Whitmore, a computer crime and counterintelligence officer with the Air Force Office of Special Investigations, the military has seen a rise in such attacks over the last couple of years.[1]

Because there is so much money to be made, Spyware is here to stay. In the coming years, Spyware techniques will change in nature and increase in technical sophistication, as will the technology to fight it.

Increasingly, enterprise applications are being downloaded. The browser has become the superhighway on which business critical supplies are sent. When the browser is infected, the results are often disastrous.

On June 15, 2006, UPI Business News reported that more than 1,300 people in Oregon may become victims of identity theft because an employee of the Oregon Department of Revenue downloaded data-capturing Spyware. The employee was using an office computer to surf pornographic sites and downloaded a Trojan. According to the report, this Trojan installed itself Jan. 5, 2006 and for the next four months captured Social Security numbers, names and addresses in stealth and relayed them back to its creator.

As a result of this security breach, The Oregon Department of Revenue has banned employees from accessing Web sites for personal use. However, this is not a practical solution in many corporate environments where employees who use the vast resources of the Internet for appropriate purposes are equally vulnerable to Spyware infection. For example, hackers can host bogus blog sites, or create a blog on a legitimate host site and post Trojans or keylogging software to the page. It is only a matter of time before hackers find ways to take advantage of other flaws, which could create risks for all bloggers who subscribe to their RSS feeds.

It is equally impractical to impose Internet access restriction on employees who work long hours and use their break times for online banking, shopping and other personal business that may otherwise be neglected. The cost of lost productivity is less than the cost of preoccupied, anxious employees. Anxiety that diverts workers' focus from

[1] Department of Homeland Security Daily Open Source Infrastructure Report, June 19, 2006

their jobs could compromise throughput far more than a few minutes spent on personal chores.

An obvious question would be, “Why have we not yet found a way to eliminate Spyware?” We are accustomed to hearing is that Spyware and other Malware “exploits security holes” in operating systems. In fact, any application installed on a computer can perform any action the logged-in user is authorized to perform. To paraphrase Dr. Alan Karp research team leader at Hewlett-Packard’s Virus-safe Computing Lab, there is no inherent reason why a Solitaire game needs to be able to search the user’s desktop, or why a spreadsheet program needs to be able to search its host’s disk for secrets or put a Trojan in its startup folder.

This levels of permission inherently granted these applications are much higher than what is required to accomplish their tasks.

This is not to suggest that Solitaire is using its authority for evil purposes, although it could. However, it logically follows that if there were an exploitable hole in Solitaire, a Spyware creator could gain control of this application, and do anything that Solitaire is authorized to do.

Future software, notably Microsoft’s forthcoming Vista operating system, will attempt to address this potential for abuse. Applications could have as much authority as they required just in time to accomplish their tasks; no more and no longer. The balancing act between functionality and security, known as “sandboxing” lies outside the scope of this document. It is noted only in that it helps to explain why Spyware will not be eliminated any time soon, and that network security must take this functionality into account.

Data Theft

Problem: Increasingly, Spyware is being designed specifically for identity theft. It compromises both personal and commercial privacy, with potentially dangerous effects for enterprises needing to protect proprietary information. When a computer is infected with Spyware, all of the sensitive content, trade secrets, data and passwords that reside on that computer are subject to theft. Spyware can be programmed to detect certain file types and then send the data in these files to an unauthorized third party. Keyloggers can read and broadcast everything typed on a keyboard, from a harmless e-mail to credit card account numbers and passwords, or even the administrative login passwords to your network.

Solution: iS3 ANTISpyware Corporate (ASC) locks would-be thieves out of your system before they can access your valuable data. ASC stops all forms of Spyware. When you first clean up your system with ASC, it removes existing Spyware and prevents those threats from reinstalling themselves. With True Real-Time™ protection, you can expand your use of computer technology to serve your company's business goals instead of scaling back out of fear of data theft and fraud.

Loss of Employee Productivity

Problem: The cost of Spyware goes well beyond stolen data. It not only steals your system resources but also your Internet bandwidth. It brings to a crawl the computer on which it is installed, and can slow performance for other computers across a network. It can also cause your system to become unstable and crash. In the corporate environment, cleaning up employee machines loaded with Spyware often accounts for 20% or more of an enterprise's IT Help Desk efforts.

Solution: Your employees are not security experts, nor should they be. Without any time-consuming user intervention, ASC continuously monitors desktops for Spyware activity. Because it operates in true real-time, traditional scans are not needed, and users are not interrupted by a lengthy, ultimately useless scanning process that allows Spyware to reinstall itself when users reboot.

Problem: Adware, although technically not Spyware is most effective when it is driven by Spyware. If you were surfing mortgage sites, an ad for a lender would bring better results than an ad for sports equipment. It is Spyware that causes Adware to deliver ads targeted to the user's surfing. Adware bombards employees with blizzards of Pop-ups, often forcing them to close down. Or worse, unsophisticated users click on appealing ads, games, toolbars or offers, thus downloading even more Spyware. Many pop-up ads are keyed to certain products or services. By covering an entire screen, they can prevent users from navigating to intended sites.

Solution: Pop-ups can be vehicles for one of the most virulent Spyware distribution schemes: the ActiveX drive-by download. iS3 includes advanced Pop-up protection that stops both Adware and browser Pop-ups. It enables workers to use their computers more efficiently, without the risk of inadvertent Spyware installation.

Increased Bandwidth Costs

Problem: Data flow to and from Spyware has a cumulative effect on network performance. Spyware infesting a network uses valuable bandwidth when transmitting data –your data- back to its maker. Spyware transmits data about users' surfing habits to unauthorized third parties. Users' habits and preferences are analyzed and new content is sent back to the ad bank. The more that Spyware infects your system, the more you pay.

BotNets, which are spammers' latest "solution" to junk mail deterrence technologies, can turn your users' machines into zombies, using all available bandwidth and slowing down your entire network.

Solution: By targeting (killing) Spyware and preventing future installations, ASC helps to conserve bandwidth. New ads are no longer downloaded to ad banks on your machines and Spyware reporting is halted. Without malicious Spyware traffic, your bandwidth can be used for the purposes intended.

Poor System Performance

Problem: Spyware is code, and most of it is poorly written, causing it to consume large amounts of memory. This can degrade computer performance drastically or even cause crashes. Unfortunately, many users believe that this compromised performance is a result of an inadequate system, and thus believe they need to invest in upgrading their systems.

Solution: Spyware makers do not care if their products have a harmful effect on their victims' computers. Their goals are to steal data or advertise their clients' products and services, which are at cross purposes with your goals. ASC detects, blocks and quarantines Spyware in true real-time. It eliminates the possibility that unwanted Spyware programs will ruin employees' machines or impair their performance.

The Tangible Cost of Spyware

According to the 2005 FBI computer crime Survey released on 11 January 2006, approximately 79% of all enterprise PCs in the U.S. are infected with some form of Spyware at any given time.

According to the Radicati Group's January 2006 report, the estimated cost of each infected workstation is $265, based on IT services, downtime and re-imaging.

Assuming your business has fifty users, 79% of whom (39.5) have a Spyware infection. At $265 per workstation, your company can expect to spend $10,467.50 to clean all infected machines – per incidence of infection.

Without an effective anti-Spyware solution, users will continue to become infected and Spyware cleanup will be an ongoing expense.

The Intangible Cost of Spyware

How to assess the loss of compromised data, stolen intellectual property, trade secrets and customer data? According to iS3 researchers, various Spyware attacks increased almost fourfold in 2005 and instances of Trojans more than doubled between 2005 and 2006.

By the most conservative estimates, and based on a limited survey, the FBI has determined that about 20% of U.S firms have experienced a cyber attack. The average cost per incident was $24,000 per company.[2]

These estimates are acknowledged to be low because most enterprises are reluctant to report successful breaches of their security. “Most companies that experience computer intrusions or breaches of security do not report the incidents to law enforcement, “FBI Director Robert Mueller said at a Feb. 15 Business Software Alliance town-hall meeting.

Industry may be reticent to report Spyware due to the belief that law enforcement cannot do very much to stop it, and that the attendant bad publicity would affect customer confidence and hence, profitability. Short term, Spyware does affect the bottom line. Long term, Spyware undermines the public’s faith in online commerce of all kinds.

Making the Investment

In a report published by Deloitte Touche Tohmatsu[3] over half of all companies doing business in the technology, media and telecommunications sectors have sustained data breaches that potentially exposed their intellectual property or customer information. Roughly one-third of those incidents directly resulted in financial losses.

Although 74% of survey respondents said that they expect to spend more time and

[2] 2005 FBI computer crime survey of 2,000 businesses in Iowa, Nebraska, New York and Texas. Each had more than five employees and $1 million in annual revenue.

money on improving security in 2006, the average budget increase among those companies was only 9% percent. Fewer than 15% of those increasing their security budgets planned to do so by over 20%.

Regulations such as the Sarbanes-Oxley Act (mandates internal controls over financial reporting), HIPAA (mandates protection for the privacy of personal health information) and the Graham-Leach-Bliley Act (regulates sharing of personal information about individuals who obtain financial products or services from financial institutions) are showing benefits in improved business practices, but many IT professionals are concerned that with a focus on compliance, there are fewer dollars being allocated to robust network security.

Companies' reluctance to increase their spending on new security measures is serving them poorly. With the increasing proliferation and sophistication of Spyware and other online threats, computer security needs to become an enterprise-wide business concern rather than a nuisance problem for IT.

For a cost calculator that generates a customized presentation in PDF on the cost of Spyware to your particular company, **click here.**

[3] DTT's Global Financial Services Industry Annual Security Report, 21 June 2006