PC Tools Software

Essential tools for your PC

Stop the Corporate Spying:

Powerful, clear-cut Spyware Protection for the Enterprise

Stop the Corporate Spying

PC Tools Software
Essential tools for your PC

Introduction

Security threats in the forms of viruses, worms, hackers, corporate sabotage, SPAM and phishers are on the minds of chief security officers around the world as they try to prevent malicious attacks on their corporate IT systems. Collectively, companies spend billions of dollars on security software each year[1] and are making serious headway in the fight against some of the more common and more disruptive attacks. While anti-virus solutions, intrusion detection software and SPAM filters are available on a corporate level, many businesses are still unaware of how much protection their IT systems really need from spyware attacks.

Spyware is software that silently infiltrates and infects a computer system or network and relays information back to advertisers or other interested parties. Over the course of its lifecycle 70-90 percent of corporate desktops will become infected with different forms of malicious spyware. And because threats of spyware go relatively unchecked, businesses end up losing billions of dollars each year in employee productivity, IT maintenance, equipment repair and prevention efforts.

According to an informal poll of its readers, *InformationWeek* reports that 94 percent of U.S. companies regard spyware and its effect on the business as a concern, but only six percent say it is a catastrophic problem and only 42 percent say it is a major problem.[2] The reality is that spyware is a leading cause of employee inefficiency, a major drain on IT resources and a serious threat to corporate security despite flying under the radar. Most companies still do not have a strategic spyware prevention strategy in place to prevent infections.

In this paper, we will investigate:

- the **financial and cultural impact** spyware has on enterprises
- the **best strategy** for combating spyware in the enterprise
- the merits of choosing a **best of breed anti-spyware solution** in conjunction with an existing security software suite
- PC Tool's award-winning **Spyware Doctor Enterprise Edition**

[1] Schroder, Norma. Gartner. Forecast: Security Software, Worldwide, 2005-2009. Mar. 30, 2005

[2] Karpenski, Richard. InformationWeek. Special Report: Readers Take the Offensive Against Spyware. Aug. 9, 2004

Stop the Corporate Spying

PC Tools Software
Essential tools for your PC

Impact of Spyware on Business

It's no secret that spyware is a nuisance. Pop-up ads, inappropriate banners, redirects and unwelcome cookies annoy end users more than anything. However, once you investigate the true impact of spyware on the business, you can start to understand why it ceases to be a personal computing issue and becomes a detriment to business productivity, a drain on IT resources and a major security risk.

> "While some spyware is harmless, at a minimum it can slow the performance of individual machines or frustrate users by altering the way their browsers work. Badly infected computers can cease working altogether. Most important--and problematic--managing spyware can become a full-time task for IT departments, tapping manpower and requiring the development of enterprise-wide policies for reining in its spread and impact."
>
> -*InformationWeek*, August 9, 2004

Employee Productivity

Spyware runs in the background on an infected PC without the user knowing that anything is going on. This additional workload zaps the CPU's ability to run multiple programs, slowing performance, preventing business applications from working properly and even causing the machine to crash. And since the spyware is working in the background without the user's knowledge, simply closing running programs is not an easy fix.

Poor performance on a PC or workstation has a direct negative effect on employee productivity. Business processes like entering sales information into a spreadsheet or simply doing Web-based research all depend on a certain level of application performance. If that performance is not there, productivity suffers. In cases when downtime occurs, which happens when threats of spyware affect a PC to the point where the system crashes, hours, even days of productivity can be lost. In today's high tech world this creates not only frustration but fatal business flaws such as missed deadlines and priority assignments.

Lost productivity does not stop with the user infected by spyware. Today's collaborative work environments have made every employee a key element in the business. If even one person on a team is unable to use their computer, important deadlines can be missed and whole projects put in jeopardy.

Drain on IT Resources

In addition to lost employee productivity, spyware puts strain on the IT staff. In organizations without a robust spyware protection solution, help desk resources are required to fix performance issues that seem to have no obvious cause or viable solution. Since spyware is designed to avoid detection these phantom performance issues are usually not diagnosed right away and help desk personnel spend more time than necessary on infected systems.

Spyware is also a drain on network and application performance. Considering the effect spyware has on a single PC, imagine the harm it could cause on a network with hundreds or thousands of clients. Network resources that normally would be dedicated to business applications like sales software, CAD design or email are misdirected to supporting spyware. Bandwidth is eaten up, causing either a shortage or over-procurement.

Hardware costs can increase as well, as poorly performing PCs are perceived as needing replacement, when they really just need to be thoroughly cleansed of system-draining spyware. Other equipment like Web servers, email servers and network infrastructure can also be wrongly accused of being a bottleneck and mistakenly tagged for replacement.

Security Concerns

According to IDC, IT organizations rate spyware as the second biggest threat to enterprise security, just behind 'Trojans, Viruses and Worms' and before SPAM (#3), hackers (#4), sabotage (#10) and compliance (#16).[3] But despite this concern, most companies are doing little to combat the problem. In reality, spyware makes corporate IT systems more susceptible to viruses, worms and other malicious attacks by finding and exposing holes in the network.

Spyware can also capture keystrokes, sending user habits back to a central depository. While seemingly harmless, internet advertising is especially dangerous. While these advertisers claim they are just capturing key words to use for targeted marketing, companies need to

[3] Burke, Brian. IDC. Security Enterprise Environments Against Spyware. November 2005

be aware of any transfer of information outside of the corporate network. If keystrokes are being captured, others can collect customer data, employee records, user names, passwords, etc. Advertisers claim they are just capturing key words to use for targeted marketing, but who is to say that the data cannot be stolen or sold to another individual or organization. Usernames and passwords can be pulled out and unauthorized users could gain access to the corporate network. A company's customer data, employee records and personal information is at risk.

Some spyware can cause a computer to dial-out to remote servers for software upgrades or new ads, creating another security concern. Any connection to a server outside the corporate network opens up the company to further security breaches.

Compliance and Corporate Reputation

Organizations also need to think about federal and industry compliance. New privacy laws like HIPAA and Sarbanes-Oxley require businesses to keep company and customer data secure, and spyware can seriously hinder a company's ability to either remain in compliance or prove they are compliant.

A company's reputation is also important. Employees continually having to call the help desk because of performance issues can become impatient with the business's lack of support. These employees can grow frustrated or even unhappy and start to spread their discontent with other employees or to people outside the company. For the sake of the company's internal and external reputation, the spyware issue must be faced head on.

What Type of Solution Should You Deploy

Like anti-virus and anti-spam solutions, anti-spyware products need to keep the enterprise one step ahead of the spies. The nature of spyware is continuously changing with new, more elusive technology being developed to remain as invisible as possible and under the radar of most anti-spyware software solutions. It is essential that companies deploy a powerful anti-spyware solution that heads off spyware trying to infiltrate its IT environment. While the

urge to trust your anti-spyware needs to your existing security software vendor is strong, many of those vendors do not have a dedicated solution as part of their security suite. In fact, some of the larger vendors currently try to pass off spyware detection tools that only detect spyware rather than actually remove programs or cleanse the system. Instead, a more cooperative effort that enhances your existing security suite with a best-of-breed anti-spyware solution is the best strategy for securing your corporate IT environment from infection.

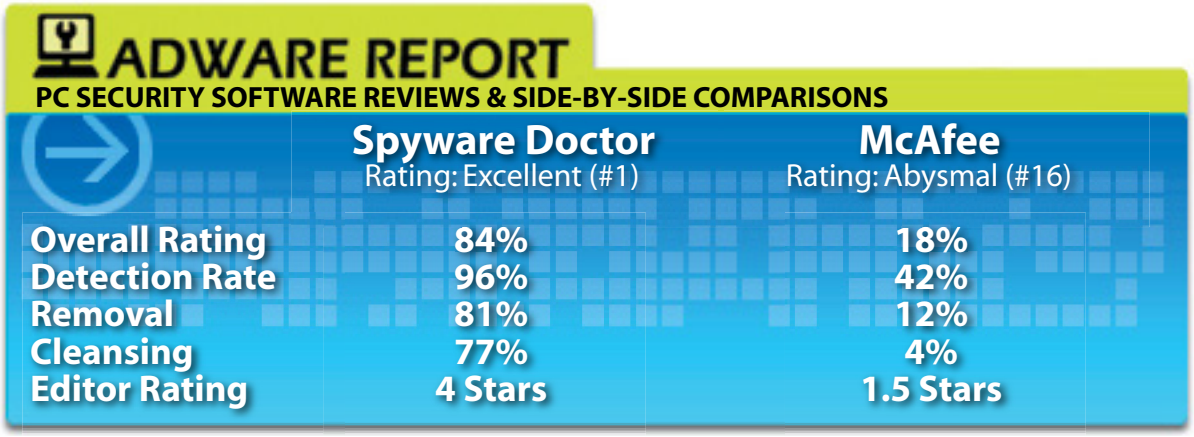
Characteristics of a Solid Anti-Spyware Solution

The paramount criteria when implementing enterprise-grade anti-spyware software is the elimination of spyware from the network, but there are other factors to consider when implementing a solid anti-spyware strategy:

- **While detection is important, cleansing is essential:** There are two parts to spyware protection: detection and removal. A good anti-spyware solution does both while continuing to block further threats. What good is detecting a malicious program when it can't be deleted from the computer?
- **Cover your entire IT environment:** Your anti-spyware solution needs to cover the entire network, including laptop and remote users who only occasionally log on to the network. Typically, these users are the most at risk since they often work outside the firewall.
- **Centralize management for simplicity and consistency:** Managing your spyware centrally (usually through a network-based solution) ensures that your spyware protection strategy remains consistent throughout the entire organization. Most spyware is designed to take advantage of the weakest link, so make sure everyone follows corporate policy. A central management console is also more effective when issuing patches and software upgrades.
- **Ensure your anti-spyware solution is always working:** Nothing is worse than thinking you are protected and finding out that your security software is continuously going down. A solution that is easy to manage, easy to configure and easy to scale is more likely to be always available.
- **Make sure you have the most updated information:** Authors of spyware are sneaky. Once they realize their programs are being detected, it is simple for them to

tweak code or develop entirely new, undetectable spyware. Make sure your anti-spyware solution is updated with new threats every day. Any lag longer than that could put you at risk for infection.

- **Integrate anti-spyware with your existing security strategy:** Any effective anti-spyware strategy needs to integrate with the rest of the company's security strategy to ensure all threats are dealt with consistently and in the best interest of the enterprise.



General Security Software Vendors Can't Effectively Combat Spyware Alone

As you can see from the above chart, most spyware detection solutions bundled with the major security suites do not provide the level of protection that best of breed solutions provide. Only McAfee is ranked in the top 10 while Symantec and Computer Associates are not even listed. The rest of the top 24 are point-product vendors that focus exclusively on spyware detection and cleansing. While these security suite vendors provide top-of-the-line virus, intruder and SPAM protection, companies with more vigorous anti-spyware needs are better served deploying a best of breed solution in conjunction with their existing security portfolio.

The large security software vendors like McAfee, Symantec and Computer Associates are not spyware experts. Admittedly, they are more focused on intrusion-detection, anti-virus and systems management solutions. They don't have the resources to dedicate to developing the most potent anti-spyware tools. These vendors are also under pressure to sell other tools

packaged with anti-spyware solutions, which is something to keep in mind during the sales process. Do they really have your best interests in mind or are they just trying to 'upsell' you?

Best of Breed is the Way to Go

On the other hand, best of breed vendors are better suited to providing the spyware protection enterprises need. They are completely focused on catching the most spyware and eliminating it from corporate networks. They dedicate thousands of man-hours searching for new spyware programs, analyzing trends in the industry and coming up with new, innovative methods of detection, removal, and blocking. For example, PC Tools employs an army of engineers who continuously scour the Web for new threats. Only by keeping a close eye on what the spies are up to can an anti-spyware vendor make sure they are catching everything that is thrown up against them.

While it would be inefficient to cast out your security vendor for best-of-breed products across the board, a combination of the two may be the best fit for an enterprise looking for additional protection. Most anti-spyware solutions integrate seamlessly with the larger security suites and provide more dynamic spyware protection without sacrificing the company's overall security strategy.

PC Tools Spyware Doctor Enterprise Solution

PC Tools Spyware Doctor Enterprise is an industry-leading, multi award-winning anti-spyware solution that provides comprehensive and continuous anti-malware protection for network servers with limited administrative intervention. Spyware Doctor Enterprise builds on the strength of PC Tools' leading consumer anti-spyware product, combining the industry's most powerful detection, removal, and blocking tools with enterprise-level scalability and management. Identified by dozens of third-party media outlets and consumer groups as the most powerful anti-spyware solution available, Spyware Doctor consistently finds and removes more spyware than any other competing solution.

Stop the Corporate Spying

PC Tools Software
Essential tools for your PC

Key Features of PC Tools Spyware Doctor Enterprise include:

- **Best of Breed Performance –** PC Tools provides the most powerful spyware detection and removal functionality in the business with Spyware Doctor
- **Automatic Smart Updates –** PC Tools consistently updates its threat database and automatically passes that information to customers to better stay on top of new spyware threats
- **Gateway versus Desktop –** Spyware Doctor Enterprise sits on the corporate network giving administrators a central point of management while detection tools sit on the client side for more efficient and powerful spyware identification capability
- **Ease of Use and Reporting –** Spyware Doctor Enterprise is easy to install, scale and monitor through a central management console that allows administrators to produce trend analysis reports

Spyware Doctor 4.0
September 2006

January 2005

September 22, 2005
Spyware Doctor

Spyware Doctor 3.5
May 2006

Spyware Doctor 3.5
April 2006

July 20, 2006 December 27, 2005

Powerful

Spyware Doctor is consistently lauded by third parties as having the best ability to locate and remove the most spyware while continuing to block further threats in real time. *PC Magazine* awarded the solution its Editor's Choice award in 2005 and 2006, while CNet gave the product a rare five out of five star ranking. In addition, *PC Pro*, MajorGeeks.com and Shareware.com have given top awards to Spyware Doctor.

Automatic Updates

Spyware Doctor automatically updates its threat database directory, populated by an army of engineers who continuously seek out new spyware threats on the Web. The solution's Smart Update Server

collects the information from PC Tools and makes sure the threat checklist on each client is updated accordingly. The server also handles the task of downloading software updates. This function makes sure that the enterprise is armed with the most up-to-date information and is better prepared to locate and remove spyware on client machines.

Gateway versus Desktop

Spyware Doctor Enterprise Edition is uniquely deployed from a central server to client workstations. This architecture ensures that that software is updated accordingly while keeping key features and commands on the client side for better performance and availability.

Other solutions that are solely client-side do not have the central management capabilities of Spyware Doctor, while solutions that sit exclusively on the network are vulnerable to network outages and suffer in performance over the LAN.

Ease of Use and Reporting

Spyware Doctor Enterprise enables centralized management of your network security protection, including installation and maintenance, threat management, monitoring, real-time reporting analysis and spyware detection/removal from an easy and intuitive central console interface.

The server-side interface manages the processes for automatic scan/fix and scan/report commands. IT administrators are given three options for cleansing schedules, including daily reports, startup reports and weekly fix. The network administrator can also create custom schedules based on desired needs.

Spyware Doctor also includes visual alert notifications of infections detected on the network as well as license expiration alerts. These alerts can also be automatically emailed to the administrator. Spyware Doctor offers central reporting capabilities, including real-time executive summary reports, real-time infected computer reports and a trend summary analysis report.

The console also provides comprehensive logging capabilities for logins, errors and warning events. Each event is assigned a transaction ID, which allow commands to be traced from inception to completion for easy tracking.

> "Spyware Doctor is one of the most aggressive antispyware programs we've tested, going beyond the call of duty by dealing with more than just traditional adware and spyware. With its quick scanning and multiple tools that stop the spread of malware before it starts, Spyware Doctor provides a welcome addition to your anti-spyware arsenal…The program runs scans much more quickly than other popular products, yet turned up much the same results."
>
> – Cnet, February 28, 2006

Conclusion

In this paper we have learned that while today's enterprises are doing what they can to combat viruses, hackers and SPAM, many companies are lacking specialized anti-spyware solutions like Spyware Doctor Enterprise. As a result, spyware has become a major contributor to employee inefficiency, a drain on IT resources and a major security risk. Simply put, spyware costs enterprises billions of dollars each year.

A viable anti-spyware solution protects the enterprise through powerful detection and removal features, coverage of the entire IT environment, central management, automatic updates and integration with existing security solutions. That said, an anti-spyware tool included in your existing security suite may not provide the level of performance or functionality an enterprise may require. Instead, companies are much better off combining a best-of-breed solution to enhance their existing anti-virus, anti-intrusion and anti-SPAM efforts. PC Tools' Spyware Doctor Enterprise is able to guarantee the best spyware protection for your business while not degrading other security features already in place. Spyware Doctor Enterprise's industry-affirmed performance, scalable architecture, simplicity and ease of use make it the best solution for enterprises looking for superior spyware protection.

For more information about the threat of spyware on the enterprise and how Spyware Doctor Enterprise addresses these threats, please go to **www.pctools.com**.