



White Paper



**Combating the
Spyware menace:
Solutions for the
Enterprise**

Contents

Evolution of the Spyware Risk..... 3
The Complex Spyware Fraternity..... 4
The unseen Spyware Attack..... 5
Escalating Costs of Spyware..... 6
Tackling the Spyware Threat..... 8
Evaluating Enterprise-Class AntiSpyware..... 10
About Omniquad AntiSpy Enterprise..... 11

Evolution of the Spyware Risk

Enterprises, Internet Users and Internet Security companies are trying to battle one of the most elusive, complex and established technological threats of all – the Spyware menace. The term *spyware* first came into use in 1995 in a letter that poked fun at a large software company's business strategies. Today spyware is a serious and persistent problem that no known internet-security technologies like firewalls or anti-viruses can address fully. Antispyware technology was first introduced in 2000, but the surge of newer antispyware solutions continues even today – a clear proof of the prevalence of Spyware as an ever growing problem.

There has been a major growth in antispyware technologies over the past couple of years due to two major reasons:

1. Enterprises and internet users were largely unaware of, and slow to wake up to the adverse effects of spyware. Consequently, they treated spyware as a less serious problem than viruses or hackers.
2. Spyware was considered quite simply as any program that captures and sends user information to the remote servers or creators of the program without the user's knowledge, which could easily be prevented with adequate network security.

Spyware makers on the other hand took this slow awakening phase as an opportunity to explore further possibilities of spyware and to diversify the modes of attacks.

Most businesses have tackled viruses, hammering best practices into their users and implementing anti-virus software. However, these enterprises and their users often do not realize spyware's potential for damage, according to a session at a recent SHARE user conference in Boston.¹

Nine out of ten internet users say they have adjusted their online behaviour out of fear of falling victim to software intrusions. Unfortunately, many internet users' fears are grounded in experience - 43%, or about 59 million American adults, say they have had spyware or adware on their home computers. Although most do not know the source of their woes, 68% of home internet users, or about 93 million American adults, have experienced at least one computer problem in the past year that is consistent with problems caused by spyware or viruses.²

The complex Spyware fraternity

Over the last couple of years, the programs that could be termed *spyware* have become more diverse in nature.

Online advertisers, hackers and even makers of file sharing software have joined the bandwagon making the spyware fraternity a very complex one to identify and define. Despite the diversity of spyware generators and their purposes, all of these programs cause inconvenience for internet users.

-- Spyware may track browsing habits to create marketing profiles, or capture confidential user data and divulge it to third parties, or attack system vulnerabilities. -- Eventually there is trouble; enterprise networks become flooded with unexpected system problems that cause bandwidth drain and escalate troubleshooting and repair costs.

With the effects of a spyware attack ranging from identity theft and system degradation to intrusion or invasion of privacy, the term *spyware* had to be redefined.

Thus the fight against spyware widened its spectrum so that it became relevant to all users of the internet. Some of the major spyware categories are adware, malware, keyloggers, browser helper objects, worms, trojans, password hijackers, E-mail flooders, firewall killers, spoofers, hacking tools, dialers, tracking cookies, remote administration tools, backdoors and annoyance tools.

According to an October 2004 study by America Online and the National Cyber-Security Alliance, 80% of surveyed users' computers had some form of spyware, with an average of 93 spyware components per computer. 89% of surveyed users with spyware reported that they did not know of its presence, and 95% reported that they had not given permission for it to be installed.³

The unseen Spyware attack

Today, spyware is best defined as any program that is installed without a user's informed consent to perform any undesired activity.

With the line between legitimate and illegitimate programs fast fading, the term *spyware* now encompasses a wide range of programs. As forms of spyware diversify, they get more elusive than their precursors; and their distribution methods have become more devious.

Spyware now can come packaged with legitimate P2P file sharing programs. The more insidious spyware that comes bundled with various other programs seem not to be mentioned anywhere in the setup installation screens, leaving users dumbfounded as to how unknown programs came to be installed. Spyware often exploits the fact that users usually don't bother to read license agreements when installing software

There are sinister spyware programs that trick users to click *Yes* or *No* on the browser when accessing certain websites. Users click hastily, without thinking, as it hinders their work or browsing time. In the process of choosing "Yes" or "OK", the spyware is surreptitiously invited to install itself. These BHOs (Browser Helper Objects like Toolbars and ActiveX Control plug-ins) are often unsolicited and affect the user's PC in unforeseen ways.

It is now known that even spammers use the confidential information gathered by spyware to unleash spam mails and flood mail boxes.

Some jurisdictions, such as the U.S. state of Washington, have passed laws criminalizing forms of spyware. The Washington law makes it illegal for anyone other than the owner or operator of a computer to install software that alters Web-browser settings, monitors keystrokes, or disables computer security software.⁴

Lack of knowledge about internet viruses and malicious software is putting computer users at risk from online identity fraud, according to research.

Just 16 per cent of the public have heard of key-logging software, which criminals use to steal confidential internet password and banking details, says research firm Mori.⁵

Escalating Costs of Spyware

Recently, a Trojan named Backdoor.Nibu (a variant of a family of Trojans called *Dumaru* or *Srv.SSA-KeyLogger*) wreaked havoc by stealing data from compromised computers. The Trojan attack succeeded in collecting passwords of online accounts from 50 banks, Ebay, Paypal login names and hundreds of credit card numbers. This virus had the capability to disable most antispyware software in the affected PCs, edit the Windows host file, grab all text stored on clipboard and typed in Internet Explorer forms. No known Antivirus application was capable of removing this threat, and antispyware vendors had to come up with customized signatures to root out this spyware.

Public awareness of spyware reached a peak when a New York Times editorial called for legislation, and was followed by a *Federal Trade Commission* discussion of potential regulations to combat this pervasive IT security issue.

"The *Forrester* report says that, on average, 7% of all help desk calls are made in response to spyware infections; Dell's (Profile, Products, Articles) own estimate is 20%. As an exercise, take 7% 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.)"⁶

'According to The DTI's *'Information Security Breaches Survey,'* two thirds of UK businesses have had a security breach in the last year compared to

A recent survey indicates that 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.⁷

Earlier this year Sumitomo Mitsui bank almost lost over \$396 million due to a very well targeted Spyware attack.⁸

18% six years ago. It states that large organizations are likely to experience one attack per week with the average cost being \$18,000, or for a large organization, running up to \$216,000!

An IDC survey of 600 corporate IT managers revealed that Spyware ranks fourth on the list of biggest security risks. For home users, information and identity theft by spyware remains serious, but can usually be stopped and losses recovered in a relatively short period of time.

The risks that different types of spyware pose today makes it necessary for corporate networks to address and curtail escalating costs with sound cost-effective solutions. New and complex procedures of Spyware distribution also mean that antispymware vendors have to come up with behaviour-specific spyware removal methods.

Specific behaviours that have changed in the wake of spyware threats include more cautiousness about opening e-mail attachments. 81 percent of those surveyed said they have stopped opening e-mail attachments unless they are sure the documents are safe.⁹

Tackling the Spyware Threat

Evolved spyware behavior invariably meant that antispware solutions had to come up with a multi-pronged approach to tackle the threat. It also has become increasingly clear that conventional anti-virus engines and firewall technologies, with their standard pattern recognition techniques, cannot adequately encompass the full gamut of Spyware threats.

A case in question is the about:blank Web search hijacker. This hijacker, also referred to as the HomeOldSP hijacker, redirects users to itself every time they try to access a website. The spyware installs a random file in the Windows system folder which makes it difficult to fix manually. The various effects of this Spyware include – replacing your home page with a new one titled "about:blank". It installs a browser helper object into Internet Explorer that consumes system resources and slows down the internet connection. It restores itself after its file directory is deleted, restores its registry settings once they have been deleted, is difficult to remove from memory and starts with the operating system. If it is removed from the auto-start settings, it will then restore itself there. Later versions change their executable to avoid detection by the simple hash recognition algorithms that most antispware products use and may also store executable code in your temporary internet explorer files. No single method of detecting and removal can work for this spyware.

While most businesses know spyware is a problem, far fewer have the right systems in place to protect themselves. The average company may not be at risk from commercial espionage and organized crime, but can lose time and money to adware that slows down PCs and clogs up networks. Relying on free detection software designed for home use isn't the best way to protect hundreds of desktop PCs.¹⁰

The most common methods employed by antispymware solutions are:

Real-time Installation Blocking – Blocking spyware this way is as good as stopping it at the Internet gateway level so your network will be free of spyware most of the time.

Blocking File Execution – This important layer of defense prevents spyware files from loading before execution so that data security is not compromised, but it leaves removal for a later stage.

Search and Destroy - Most antispymware vendors include this method in their design, and most free antispymware applications use this method almost exclusively. Search and Destroy solutions scan the computer's hard drive for known spyware applications and once identified, removes them. When used along with a paid antispymware subscription, which should also include regular threat file updates and real-time monitoring, Search and Destroy is an effective and necessary method for spyware removal.

Evaluating Enterprise Class AntiSpyware

Selecting the best enterprise product suited to meet your spyware risks and network vulnerabilities requires considerable attention and informed decision making. For a long time there were hardly any antispyware solutions designed to address the needs of big or small enterprises in the war against spyware.

While evaluating Enterprise AntiSpyware solutions some basic points need to be kept in mind.

1. Whether Spyware detection/removal can be centrally managed
2. The methods of Spyware detection and removal that the product employs
3. The level of protection it offers
4. The quality of the Spyware signature database the product delivers
5. The frequency of Spyware signature updates that are dispatched
6. The Spyware reporting capabilities
7. The cost-effectiveness of the solution
8. Whether the product is compliant with other software and security tools used at your site

Since there are new and unknown spyware releases everyday, no product can truly claim to solve all Spyware issues at the customers site by default. There will be cases where urgent troubleshooting and follow up is required. It will therefore be beneficial to look at the quality of support offered for the product and the turn around time when issues are reported. Support for customer feedback is therefore an important feature.

One thing to note when evaluating antispyware tools: spyware labelled as a single program by one antispyware tool can show up as 30 different products with a different one. A program that claims to detect 60,000 types of spyware may not protect you any better than one that is only capable of covering 20,000.¹¹



Omniquad AntiSpy Enterprise

Omniquad AntiSpy Enterprise is an integrated Internet Management solution that can be used exclusively for spyware detection and removal. Built within the robust and proven Enterprise Manager framework, this award winning product offers multi layered security to protect corporate LANs/WANs against malicious Spyware.

Omniquad AntiSpy Enterprise offers the following features for network administrators to effortlessly administer Spyware protection:

- Centralized management of spyware detection and removal
- Automated deployment of agent software across enterprise networks of any size
- Fully compatible with Windows Active Directory
- Comprehensive spyware database
- Automated and daily spyware signature updates
- Centralized spyware reporting with complete spyware details
- Security policy application on mobile Internet user laptops
- Customizable policy application for users, computers and organizational units
- Scheduled scan policies
- Fully customizable spyware scan options
- Enhanced browser security



About Omniquad

Based in London, United Kingdom, Omniquad (Pvt) Ltd. specializes in Internet Security Solutions for home and enterprise users. Omniquad's security software spectrum ranges from privacy protection, Internet management, intrusion detection, firewall and anti-virus software to managed email security services. Omniquad continues to provide services to millions of home users, educational institutions, corporations, government institutions and small to large enterprises across the globe. Omniquad takes pride in careful listening to customers, in innovation and in providing dedicated support for its clientele. Omniquad has also received several accolades and awards for several of its niche product suites.

To know more about Omniquad, please visit www.omniquad.com



Omniquad Ltd

72 Crestway
London SW15 5DD

Tel: +44 (0) 208 743 8093
Fax: +44 (0) 870 458 2866
General/Media Enquiries: info@omniquad.com

Distributors

United Kingdom

Caretower IT Solutions

Triangle House,
305-313 Green Lanes,
Palmers Green, London,
N13 4YB
TEL: 020 8372 1000
FAX: 020 8372 1001
SUPPORT: 020 8372 9272

North, Central and South America

Tech Assist, Inc.

2058 Bayshore Blvd. Suite 1
Dunedin, FL 34698
Tel (800) 274-3785 or (727) 547-0499
<http://www.toolsthatwork.com>
sales@toolsthatwork.com

Rest of the World

Omniquad Ltd.

72 Crestway
London SW15 5DD

Tel: +44 (0) 208 743 8093
Fax: +44 (0) 870 458 2866
www.omniquad.com
General Enquiries: info@omniquad.com

¹ <http://www.adtmag.com/article.asp?id=11726>

² Pew Internet and American Life Project – Reports: Public Policy Spyware: The threat of unwanted software programs is changing the way people use the internet-Susannah Fox July 6th 2005 http://www.pewinternet.org/PPF/r/160/report_display.asp

³ "[AOL/NCSA Online Safety Study](#)". America Online & The National Cyber Security Alliance. October 2004

⁴ Wikipedia – The free Encyclopedia

⁵ <http://www.vnunet.com/computing/news/2141693/ignorance-increases-online>

⁶ Info World February 18, 2005

⁷ Info World August 25, 2005

⁸ Morgan Stanley May 25, 2005

⁹ Info World July 07, 2005

¹⁰ <http://www.guardian.co.uk/online/story/0,3605,1541766,00.html>

¹¹ <http://www.guardian.co.uk/online/story/0,3605,1541766,00.html>