

## **Spyware:** Securing gateway and endpoint against data theft

The explosion in spyware has presented businesses with increasing concerns about security issues, from data theft and network damage to reputation loss and exposure to potential litigation. This paper examines how spyware infiltrates and affects organizations and describes how to protect against it.

# Spyware:

## Securing gateway and endpoint against data theft

### Spyware defined

Spyware poses a constant and significant security risk to organizations, stealing or damaging confidential corporate information and opening up networks to further attack. Its intent is malicious. It installs itself onto a user's computer by stealth, subterfuge and/or social engineering and sends information from that computer to a third party without the user's permission or knowledge.

*Spyware comes in many guises, and although outnumbered by downloaders in 2006, Sophos expects this to result in even more spyware being installed on the computers of unsuspecting users.*

Organizations also need to manage the associated problem of adware, which delivers targeted advertising, such as pop-up messages, to users' computers, and is increasingly seen as a nuisance. However, while adware and other potentially unwanted applications (PUAs) can affect user productivity and system efficiency, they may actually be required by some users. Commercial remote administration tools, such as Azrael, are an example. So although the distinction between spyware and adware is sometimes blurred, this paper focuses on the threat posed by spyware.

### A growing and diverse threat

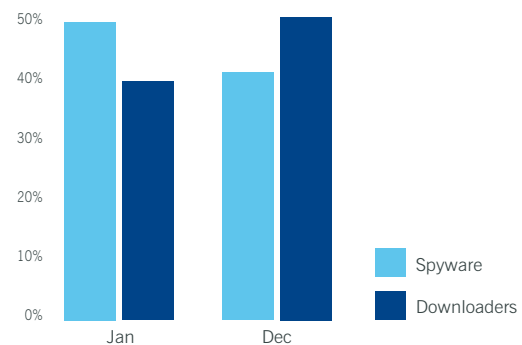


Figure 1: Spyware and downloaders in 2006

The problem of spyware is an evolving one, and is now the second largest security concern for organizations.<sup>1</sup> Although the growth in immediately identifiable spyware has slowed, the increasing use of Trojan downloaders is expected to provide more versatile and devious ways to deliver spyware to unsuspecting users. Figure 1 shows the percentage of email that contained spyware and the percentage of email that linked to websites from which spyware is downloaded at the beginning and end of 2006. The rise of Instant Messaging (IM) and peer-to-peer (P2P) file-sharing applications in particular has also added to potential delivery mechanisms available to users and distributors of spyware. However, Sophos research shows that businesses are demonstrating a heightened awareness of the spyware problem.

Of those responding to a Sophos web poll, an overwhelming majority – 95% – indicated that they expect their anti-virus software to provide simultaneous protection against spyware.<sup>2</sup> As well as growing in volume, the spyware threat is diversifying, with new techniques appearing all the time.

*In early 2006, the Haephrati couple – managers of the firm Target-Eya – developed and marketed a Trojan specifically aimed at private investigators for commercial espionage.<sup>3</sup>*

Spyware threats include:

- Password and information stealers – steal passwords and other sensitive personal information.
- Keyloggers – monitor keystrokes with the intention of stealing information such as passwords.
- Banking Trojans – monitor information entered into banking applications and banking web forms.
- Backdoor Trojans – can contain any of the above functionality, including the ability to allow hackers unrestricted remote access to a computer system when it is online.
- Botnet worms – create a network of infected computers, configured remotely to work together to carry out any of the above functionality.
- Browser hijackers – reduce browser security settings and/or modify browser settings with the intention of redirecting users to automatic download sites.

The threat posed by spyware has been increased by the ready availability of spyware kits on the internet for as little as US\$15. In 2006 SophosLabs™ discovered a Russian website where potential hackers can cheaply obtain scripts that simplify the task of infecting computers. Such kits are also attractive to opportunists who lack the skills but have malicious intentions.<sup>4</sup>

### How spyware attacks businesses

Spyware is a real threat to organizations, affecting business continuity in a number of ways.

#### Data theft

Spyware can steal important or confidential information, as in the example of Troj/BankAsh-A, a password stealer and keylogger. Once installed, the software starts reporting the next time the computer is online. This kind of spyware can also steal financial data, spreadsheets, personnel records, bank account numbers, passwords, or any other information typed into the affected computer. Over 33% of all threats analyzed by SophosLabs are designed to steal information, while 16% contain keylogger functionality. A damaged reputation, the loss of money or competitive advantage, and an increased risk of litigation can all result from data theft.

#### Hacking

As well as capturing data, spyware can leave corporate computers vulnerable to espionage by hackers – more than 40% of all threats seen by Sophos allow others access to infected systems. Backdoor Trojans, such as Troj/Feutel-L, enable hackers to take control of a computer and steal any information stored on it. For the IT administrator this kind of attack is potentially worse than a virus, since the behavior of any hacker accessing the network is unpredictable.

### Zombie attack

Spyware such as botnet worms can also be a very effective tool for spammers. Using a botnet worm or a Trojan such as Mytob – the top family of threats identified by Sophos during 2006 – spammers can take over a vulnerable computer or web server and force it to send out their emails for them, thus making the email appear to be from a legitimate source. The hijacked computer can also be used for other malicious purposes, such as forming part of a denial of service attack. In such an attack, thousands of computers access a website at once, overloading its servers and causing it to shut down. Computers that have been hijacked and linked to other infected machines in this way are known as botnets or “zombie” networks.

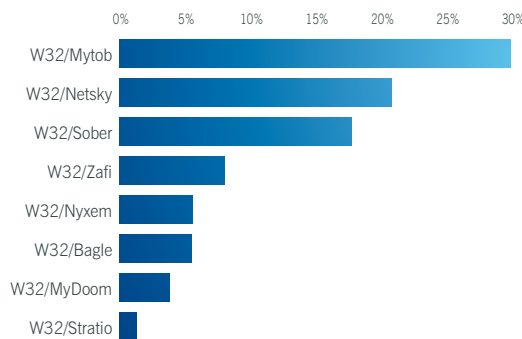


Figure 2: Zombie-creating Mytob family tops the 2006 malware chart

Sophos estimates that over 60% of spam is being sent from zombie computers. While it is often home users who are most at risk, the problem also affects organizations. At the beginning of 2006, a man in California was indicted on charges of launching a zombie attack which infected 150 computers at Northwest Hospital and Medical Center in Seattle, US.<sup>5</sup>

In May 2006 in South Korea, the third most prolific host of spam sources according to SophosLabs,<sup>6</sup> authorities arrested a man suspected of running a network of 16,000 zombie computers that were responsible for sending 18 million spam emails every day to 133 countries.<sup>7</sup>

### Network damage

Network performance can also suffer as a result of a spyware attack, as the software places extra demands on the system. For a business, this can mean disruption and decreased productivity while the software remains undetected, and extra resources being spent on finding and clearing up the problem.

### How spyware becomes installed

Spyware can be installed by a virus, or when a user clicks on a weblink or opens an attachment in an email. As mentioned earlier, the increased use of web 2.0 technologies such as IM provides spyware writers with yet another vehicle for attachments containing malicious payloads. Most spyware requires some user action for it to be installed on a computer, such as downloading an ostensibly useful or desirable piece of software (a P2P file-sharing program, for example) which may carry the spyware hidden within it. Users may also be duped into downloading spyware through pop-up messages that prompt them to download a software utility they “need”. Security vulnerabilities, such as those in some web browsers, are also exploited to install spyware. A user only has to visit a certain website or view an HTML email message for spyware to install itself onto their computer. This kind of secret installation is known as a “drive-by download”.

## Protecting against spyware

### The basic steps

As with any security threat, the basic steps an organization needs to take to protect itself against spyware involve the effective combination of:

- Education – ensuring that all users understand the need to be cautious when opening attachments and downloading and installing software.
- Policy – enforcing a robust, company-wide internet policy to prevent unauthorized downloads, and implementing passwords to prevent unauthorized access to desktop computers.
- Security – installing the latest browser and operating system patches, ensuring that browser security settings are set correctly, and deploying up-to-date endpoint and gateway threat protection.
- Control – ensuring that the control of applications such as IM, VoIP (Voice over Internet Protocol) and P2P file sharing is integrated into the existing anti-malware detection and management infrastructure.

### Security and control

Beyond these basic steps, businesses should implement an integrated security solution, which protects both the endpoint and the gateway. As well as safeguarding against viruses, Trojans, phishing attacks, zombie attacks, and spam, organizations need to prevent policy abuse, the use of unauthorized applications, and unauthorized access to the network – managing the increasing complexity of threats as a whole, not as separate problems.

In summary, businesses need to be proactive in their approach to spyware protection, through a combination of user education, policy enforcement, and technology. A solution from a trusted vendor that enables both security and control is a key component in overcoming the threats that spyware and associated applications present. ◆

---

## The Sophos solution

Sophos provides effective protection against spyware at all levels – from gateway to endpoint.

**Sophos Web Security Appliance** blocks spyware, malware and unwanted applications at the gateway and enables comprehensive web access control for safe, productive web browsing.

**Sophos Email Security Appliances** protect the email gateway from inbound and outbound threats, delivering high-capacity, high-availability security against spyware, viruses, spam, and phishing.

**Sophos PureMessage®** uniquely integrates anti-spyware, anti-virus, anti-spam and policy enforcement capabilities to protect the email gateway.

**Sophos Endpoint Security** provides integrated protection against spyware, viruses, adware, unwanted applications, and hackers, as well as preventing the use of unauthorized applications.

**Sophos NAC** blocks unauthorized users, controls guest access, and ensures that legitimate users comply with security policy – so that administrators know who and what is connecting to the network.

**Sophos ZombieAlert™ Service** immediately warns organizations of spam originating from their networks as the result of spyware infecting their computers.

**To find out more about Sophos products and how to evaluate them, please visit [www.sophos.com](http://www.sophos.com)**

## Sources

- 1 Worldwide Secure Content Management 2005-2009 forecast update and 2004 vendor shares: spyware, spam, and malicious code continue to wreak havoc. IDC. September 2005
- 2 95% say anti-virus software should also stop spyware, Sophos  
[www.sophos.com/pressoffice/news/articles/2005/07/va\\_pollspyav.html](http://www.sophos.com/pressoffice/news/articles/2005/07/va_pollspyav.html)
- 3 Married couple formally charged over spyware Trojan horse, Sophos  
[www.sophos.com/pressoffice/news/articles/2006/03/israeliesp2.html](http://www.sophos.com/pressoffice/news/articles/2006/03/israeliesp2.html)
- 4 Spyware kits sold for fifteen dollars available on the web, Sophos  
[www.sophos.com/pressoffice/news/articles/2006/03/russianspykits.html](http://www.sophos.com/pressoffice/news/articles/2006/03/russianspykits.html)
- 5 Man accused of hospital zombie attack that brought down computers, Sophos  
[www.sophos.com/pressoffice/news/articles/2006/02/nwhospital.html](http://www.sophos.com/pressoffice/news/articles/2006/02/nwhospital.html)
- 6 Security threat report 2007, Sophos  
[www.sophos.com/security/whitepapers/sophos-security-threats-2007\\_wsrus](http://www.sophos.com/security/whitepapers/sophos-security-threats-2007_wsrus)
- 7 Zombie king suspect alleged to have sent 18 million spams per day, Sophos  
[www.sophos.com/pressoffice/news/articles/2006/05/krzombie.html](http://www.sophos.com/pressoffice/news/articles/2006/05/krzombie.html)



Sophos: 100%  
spyware detection

## About Sophos

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. With over 20 years' experience and a global network of threat analysis centers, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, MA., and Oxford, UK.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France  
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2007. Sophos Plc.

All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

**SOPHOS**  
WWW.SOPHOS.COM