

# Solving the spyware problem

A Sophos positioning paper

February 2006

The explosion in spyware has presented businesses with increasing concerns about security issues, from data theft and network damage to reputation loss. This paper examines how spyware infiltrates and affects organizations and describes how to protect against it. The paper also shows how Sophos's 20 years' experience in dealing with malicious content uniquely places us to provide reliable, Checkmark-certified protection against spyware – alongside a host of other security threats including viruses, Trojans, worms, phishing attacks, spam and email policy abuse.

## 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.

Adware is distinct from spyware in that it delivers targeted advertising, such as pop-up messages, to users' computers. While adware and other potentially unwanted applications (PUAs) affect user productivity and system efficiency, they may actually be required by some users.

---

*"Spyware threatens security and is malicious. Adware and other potentially unwanted applications compromise productivity and can be an irritant. Sophos protects against spyware today and will integrate adware and PUA detection in the next major release of Sophos Anti-Virus."*

*Richard Jacobs, Chief Technology Officer, Sophos*

---

## A growing and diverse threat

The problem of spyware is widespread and continues to grow rapidly, with spyware now forming the majority of new threats. Figure 1 shows the number of spyware threats reported to Sophos during 2005 as a proportion of the total

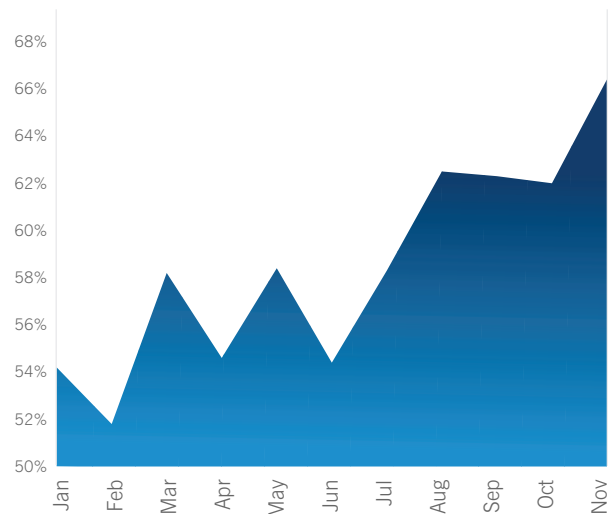


Figure 1: Spyware as a proportion of all new threats (2005)

malware analyzed by SophosLabs™ – a global network of threat analysis centers – and how that proportion has increased. In January, only 54.2% of threats were spyware, but by November this had risen to 66.4%. Sophos research also 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>1</sup>. As well as growing in volume, the spyware threat is diversifying, with new techniques appearing all the time.

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.
- Downloaders – install other, potentially malicious, programs without the user’s knowledge.
- Dialers – dial a premium rate phone line, normally with the intent of generating large phone bills.

## 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/Progent-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.

---

*Over 33% of all threats analyzed by SophosLabs are designed to steal information, while 16% contain keylogger functionality.*

---

### Hacking

As well as capturing data, spyware can leave computers vulnerable to hackers – more than 41% 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 Troj/Sober-Q, 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. 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. Recently, 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>2</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. 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 peer-to-peer 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, for example in 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.
- Technology – installing the latest browser and operating system patches, ensuring that browser security settings are set correctly, and deploying up-to-date security software.

## Integrated threat management from Sophos

Beyond these basic steps, businesses should implement an integrated security solution, which protects both the endpoint and the gateway. Businesses also need to manage the increasing complexity of threats – from viruses, Trojans, phishing attacks, zombie attacks, spam and policy abuse – as a whole, not as separate problems. Sophos ZombieAlert™ Service provides organizations with immediate warning of spam originating from their networks as the result of spyware infecting their computers.

---

*WestCoast Labs Checkmark –  
confirming Sophos detects  
100% of spyware, with no  
false alarms.*

---



Spyware detection is an integral feature of Sophos's award-winning anti-virus software. Sophos Anti-Virus provides organizations with reliable, manageable, and effective protection against spyware in just the same way as it protects against other threats.

## About Sophos

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. Our reliably engineered, easy-to-operate products protect over 35 million users in over 150 countries. Through 20 years' experience, combined in-house anti-virus and anti-spam expertise, and a global network of threat analysis centers, we respond rapidly to emerging threats – no matter how complex – and achieve the highest levels of customer satisfaction in the industry.

In addition, the ability for businesses to block or selectively allow adware and other potentially unwanted applications will be integrated into the next release of Sophos Anti-Virus, which all customers will automatically receive at no extra cost.

This level of reliable, integrated protection is part of Sophos's continuous commitment to providing businesses with the best integrated solution to threat management. It is backed up by 24/7 technical support and by the expertise in SophosLabs™ which carries out round-the-clock analysis of new and emerging threats.

*To find out more about how Sophos can protect your network, visit [www.sophos.com](http://www.sophos.com).*

## Sources

- 1 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)
- 2 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)

---

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

© Copyright 2006. 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**