

Wiping out spyware through integrated threat management

A Sophos positioning paper

August 2005

The explosion in spyware over recent months has presented businesses with new 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 threats including viruses, Trojans, worms, phishing attacks, spam and email policy abuse.

What is spyware?

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 this affects user productivity and system efficiency, it may actually be required by some users.

"Spyware threatens security and is illegitimate. Adware compromises productivity and is an irritant. Sophos protects 100% against spyware and will integrate optional adware detection in the next major release of Sophos Anti-Virus."

Richard Jacobs, Chief Technology Officer, Sophos

An exploding problem

The problem of spyware is widespread and continues to grow rapidly, 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 – a network of backdoor Trojans, configured remotely to work together to carry out any of the above functionality, which may also be used to create zombie networks from which spam can be sent out.
- Browser hijackers – modify browser settings with the intention of redirecting users to automatic download sites and/or reduce browser security settings.
- Dialers – dial a premium rate phone line, normally with the intent of gaining access to pornographic material.
- Downloaders – install other, potentially malicious programs without the user's knowledge.

The threat to organizations

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. 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 computers vulnerable to hackers. Backdoor Trojans, such as Troj/Feutel-L, enable hackers to take control of a computer and delete project plans, alter stock records, download porn, or control the user's mouse and keyboard. 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.

"It is estimated that 67% of all computers are infected with some form of spyware, with multiple spyware variants on most infected machines."

IDC, Worldwide Spyware 2004 - 2008 Forecast and Analysis, November 2004

Zombie attack

Spyware such as botnets can also be a very effective tool for spammers. Using 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. Computers that have been hijacked in this way are known as "zombies". Sophos estimates that as much as 50% of spam is being sent from zombie computers, many within the networks of legitimate organizations.

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 used 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 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 need to implement an integrated security solution, which protects both the endpoint and the gateway. It needs to manage the increasingly complex blended threats – from viruses, worms, Trojans, spam, phishing attacks and policy abuse – as a whole, not as separate problems.

*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 (not a discrete application). It provides organizations with reliable, manageable, and effective protection against spyware in just the same way as it protects against other threats. In addition, the ability for businesses to block or selectively allow adware applications will be

integrated into Sophos Anti-Virus, version 6.0, which all users will automatically receive at no extra cost.

This level of reliable, integrated protection is part of our 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™, our global network of threat analysis centers 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.

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.

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

© Copyright 2005. 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