

The spying game: how spyware threatens corporate security

A Sophos white paper

May 2005

SUMMARY

This paper defines spyware, investigating what it can do and why it threatens the network security of businesses. The prevalence of spyware is highlighted and the ways in which it can install itself are described. Methods for protecting computers and networks are also discussed

Spyware defined

Opinion is divided on the definition of spyware, since it is often used as an umbrella term for a whole range of malicious and non-malicious software. Examples include joke programs, adware, Trojans, internet cookies, homepage re-set programs and dialers (software that connects computers to premium-

Unlike spyware, some adware informs the user of its intended function before installation, but this information is often hidden amongst hundreds of lines of text.

rate phone lines). Some malicious spyware presents a security threat because of its ability to secretly record and steal confidential information, or maliciously alter an affected computer – by opening a backdoor to allow access to hackers, for example. Other kinds of spyware are more of a threat to productivity than security. One example of this is adware – software that can collect information on users' surfing habits and displays advertisements while another program is running. Adware usually informs users of its intended function before it is installed, but since this information is often hidden amongst hundreds of lines of dense legal text, some adware sits on the border of being legitimate.

However, it is malicious spyware that threatens corporate security, mainly through data theft, hacking and network damage. Examples of malicious spyware include Trojans and system monitors such as keystroke loggers, which can steal data such as passwords typed into a keyboard. Other programs can turn on webcams and microphones, allowing hackers to spy on computer users. In the context of this paper, all discussion of spyware relates to malicious spyware, i.e. that which is installed secretly, without consent, and threatens the security of networks.

A widespread problem

Although spyware has been around for some time, the actual number of affected computers is not known. However, evidence suggests that the problem has become widespread. A SpyAudit report conducted by ISP Earthlink and Webroot Software performed 2.07 million scans in the first six months of 2004, finding 332,809 system monitors and 366,961 Trojan horses.¹

Spyware is certainly recognized as an increasing security threat. In a survey of 600 North American businesses by IDC, spyware was ranked as the fourth greatest threat – ahead of spam, hackers and cyberterrorism. The only areas viewed as bigger threats than spyware were viruses, internet worms and damage through employee errors.²

The threat to business

The fact that spyware can become installed and active on a computer or network without the user's permission or knowledge makes it a particular threat to businesses, since it can cause harm in a variety of ways if left undetected.

Spyware can steal confidential business information, leaving companies vulnerable in several ways.

Data theft

One of the main security threats is the ability of spyware to steal important or confidential information. A type of spyware – known as a system monitor – does this by running in the background, recording what is typed into a keyboard and sending the information to another location. Once installed, the software starts reporting the next time the computer is

online. This kind of spyware can 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 this data theft.

Hacking

As well as capturing data, spyware can download other malicious programs or leave computers vulnerable to hackers. Backdoor Trojans can allow hackers unrestricted access to a computer system when it is online, and are a particular risk for computers with broadband internet access. These Trojans can enable hackers to take control of a computer in a variety of ways, such as deleting project plans, altering stock records, downloading porn or controlling the user's mouse and keyboard. Some other Trojans can capture screenshots or turn on webcams, allowing hackers to spy on computer users. For the IT administrator this kind of attack is potentially worse than a virus, since viruses are at least limited by the set commands in their code and will behave predictably. Humans, who have assumed control of a computer system, can react to the information they find and change tactics accordingly, making the threat unpredictable.

Zombie attack

Spyware can also be a very effective tool for spammers, who can use it to gather email addresses or take information and customize spam emails (for example, by using the names of colleagues found on a user's hard disk) thereby increasing response rates. Using a backdoor Trojan as described above, spammers can also 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 40% of spam is being sent from zombie computers without the user's knowledge.

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 spent on finding and clearing up the problem.

How spyware becomes installed

There are several ways in which spyware can become installed on a computer. It 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 to install it 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

By exploiting security vulnerabilities, spyware can secretly install itself when a user visits a certain website or views an email message.

in other ways, for example a pop-up message might appear which prompts them to download a software utility they "need". Once the user agrees, usually by clicking "OK" on an agreement box, the spyware is installed.

In some cases spyware can become secretly installed by exploiting security vulnerabilities in a web browser such as Internet Explorer. In this case 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". It can happen if the security settings on a computer are set too low or if an unpatched version of a web browser is being used.

Finally, if security regarding passwords or physical access to desktop computers is lax, spyware can be loaded onto a computer by a person using a CD or USB drive.

How to protect against spyware

There are some basic measures that can be taken to protect a network, such as educating users to be cautious when opening attachments and downloading and installing software. Enforcing a sensible company-wide internet policy will help prevent accidental downloads, and making sure passwords are kept secret will help prevent unauthorized access to desktop computers. It is useful to deploy technology such as personal firewalls to control unwanted communication with the internet. Ensuring that the security settings on web browsers are turned on and kept to a high setting will also provide a measure of protection. Spyware and other kinds of malicious code are often designed to exploit security vulnerabilities. Whenever these are discovered in software, the manufacturers issue security patches for users to download. It is important to keep up to date with the latest patches for whichever browser is being used.

However, the most effective way to protect against spyware is to use an integrated security solution to stop malicious spyware both at the email gateway and on individual computers. Sophos Anti-Virus™ provides protection from all malicious spyware. It does not currently block non-malicious software – such as adware – that seeks permission for installation and discloses if it is going to pass information

(albeit usually not very openly) in case users do actually want to allow this communication. This policy of blocking all malicious software while allowing users to judge whether they want the non-malicious applications, enables Sophos to provide 100% protection against real harm, while minimizing

There are several ways to stop spyware, but the most effective is to protect both the email gateway and desktop with an integrated software solution.

the impact on legitimate business use of software. Sophos Anti-Virus provides award-winning protection against malicious software of all kinds on desktops, remote laptops and file servers in companies of any size, while Sophos PureMessage™ guards the email gateway, giving combined protection from malicious spyware, viruses and spam. PureMessage and Sophos Anti-Virus employ Genotype™ spam and virus detection technology respectively, giving proactive protection against variants of spam campaigns, spyware threats and other malware. With policy enforcement from PureMessage, organizations also gain liability protection, meet regulatory compliance, and increase productivity. A suite of management tools enables both Sophos Anti-Virus and PureMessage to be easily installed and updated, and both come with 24-hour technical support. In addition SophosLabs™, a global network of threat analysis centers, ensures a rapid response to any new virus or spam threat anywhere in the world, 24 hours a day.

Incorporated in 1985, Sophos protects 35 million business users from organizations of all sizes in more than 150 countries. For more information on how Sophos can protect your business, visit www.sophos.com, email nasales@sophos.com, or call toll-free 1-866-866-2802.

Sources

- 1 <http://publications.mediapost.com>["Spyware Report Raises Broader Questions". By Larry Dobrow, 5 August 2004.]
- 2 Brian E Burke, "Worldwide Secure Content Management 2004-2008 Forecast Update and 2003 Vendor Shares: a Holistic View of Antivirus, Web Filtering, and Messaging Security" IDC, 2004.

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