

...SPYWARE, THE HIDDEN THREAT

The explosion of spyware threats in recent years is a result of the growing financial gain from stealing corporate and personal information. Spyware is now one of the biggest security concerns for businesses and Gartner predicts that by the end of 2007, 75% of enterprises will be infected with undetected, financially motivated, targeted malware*.

1 What's causing the problem?

Criminal organizations

The upsurge in spyware has been driven by criminal organizations and individuals around the world making money by selling to, defrauding, or stealing from computer users.

Spyware survival kits

Spyware kits that provide potential hackers with the scripts for writing malicious code are available to buy on the internet for as little as \$15. Not only do these kits simplify the task of harvesting confidential data for existing spyware writers, but they also attract opportunists with malicious intent.

2 What exactly ARE the problems?

Theft of information, hacking and zombie attacks

Spyware installs itself on computers by stealth, subterfuge and/or social engineering, and steals or damages confidential information and opens up networks to further attack without the user's permission or knowledge. Keyloggers can recognize user ID, password, or bank account information. Backdoor Trojans allow hackers to remotely take control of a computer and steal any information stored on it. Botnet worms hijack computers on a network to create "zombies", many of which are used to install spyware or mail out spam campaigns.

Variety of delivery methods

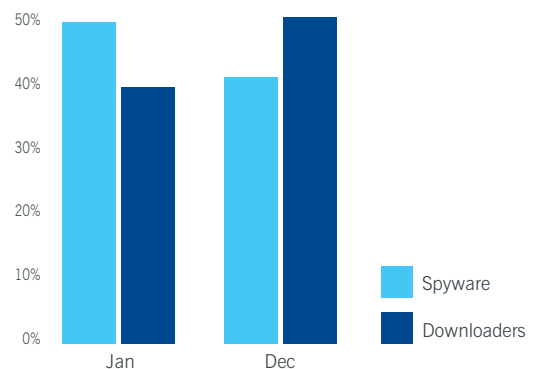
Businesses can be exposed to spyware in a variety of ways. Spyware can be installed by visiting certain websites or by viewing an infected HTML email message. It can arrive in an email attachment, via a weblink or by instant messaging. Users may be tricked into downloading spyware through pop-up messages offering free software, and security vulnerabilities in web browsers are also exploited to install spyware on endpoint computers.

Spyware is a growing and diversifying problem

As the problem of spyware continues to grow, it is evolving and new strategies for infecting the computers of unsuspecting users are being developed. For example, spammed out emails containing Trojan downloaders are being used more often as a devious strategy to pull spyware down from infected websites – as the graph on the right illustrates.

Network and workforce overheads

Spyware poses a significant threat not just to IT security but also to business resources and productivity. By surreptitiously running malicious software on corporate networks, spyware eats up network bandwidth and drains staff resources while the problem is cleared up.



Spyware and downloaders in 2006

3 What are businesses currently doing to fix the problems?

Relying on endpoint anti-spyware protection

Pro There's a very good chance it's already installed.

Con Spyware's ultimate destination is the endpoint, so relying on endpoint anti-virus protection means the network has already been exposed to the threat. Further problems arise if the anti-spyware protection has not been updated or if the endpoint belongs to an outsider connecting to the network.

In 2007, a gang of international hackers was arrested for using banking usernames and passwords stolen through spyware to hack into online bank accounts and steal \$300,000 from internet users.

www.sophos.com/hackergang

Relying on gateway anti-spyware protection

Pro At the gateway, the most common solution is URL filtering, which blocks access to URLs that are known to distribute spyware and other malware.

Con This approach cannot always respond quickly enough to the rapid shift in domains and URLs used by today's sophisticated spyware authors. URL filters only block outbound page requests and not inbound content, so if spyware is coming from a new source, URL filters won't be able to block it until they discover the source and publish an update.

4 What should you do now to fix the problems?

Use a multi-tiered approach

In order to protect against spyware, a multi-tiered solution is required to secure every potential entry point of the network.

Secure endpoint computers

Infection can occur from many sources such as remote workers connecting to your network from home. Make sure your anti-malware solution is frequently updated, and includes central monitoring to avoid lapses in protection.

Secure the gateway

Stop threats before they infiltrate your network. Use a web security solution that blocks access to malicious websites and scans inbound content quickly and thoroughly to keep new spyware and other malware out. Use an email security solution that can detect and block emails containing links to malicious spyware-hosting URLs, and can block emails from known malware writers and spammers.

Secure the network

Acceptable computer-use policies and disabling local administrator privileges can only go so far. However good your best practice, visitors to your company will not be aware of internal policy. Prevent lapses in employee policy compliance, or visitors logging in with inadequate computer security using Network Access Control (NAC).

Sophos provides effective protection against spyware at all levels – from gateway to endpoint thanks to Sophos Web Security Appliance, Sophos Email Security Appliances, Sophos PureMessage, Sophos Endpoint Security and Sophos NAC. To find out more about Sophos products and how to evaluate them, please visit www.sophos.com.

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 rights reserved. All trademarks are the property of their respective owners.

tt/070425

SOPHOS
secured.