

# The growing scale of the threat problem

A Sophos white paper

February 2006

The growth in malware has continued unabated during the 20 years since Sophos entered the computer security industry, despite repeated speculation that it would eventually slow down. This paper examines the history of viruses and spam and looks at how collaboration between virus writers and spammers is impacting enterprises. It also looks at future developments, and how the expertise of SophosLabs™ is applied to providing continuous protection against evolving threats.

## A brief history of viruses

Following the development by Bell Labs in the 1950s of an experimental game in which players used malicious programs to attack each other's computers, the idea of viruses and worms infecting and spreading across networks was floated in both academic circles and the sci-fi world. However, it took until 1986 for the first recognizable PC virus to emerge: Brain was allegedly written by two brothers in Pakistan, and was activated when booting up from floppy disks.

Recognizing the increasing threat of viruses, the emerging anti-virus industry developed signature files to identify the unique strings of code in known viruses. In response, virus writers began to develop polymorphic viruses which mutated as they spread, making detection and disinfection more difficult. For a brief period, there were also attempts to evade detection by making virus code sequences very short.

However, the development of the internet opened up the whole world to virus writers around 1995, so that viruses were no

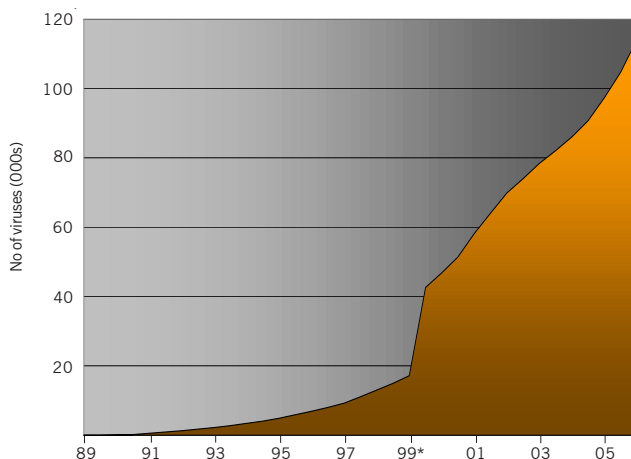


Figure 1: The growth in virus numbers 1989-2005

longer constrained to spreading simply via the exchange of floppy disks. Together with the development of worms – a type of malicious code that self-replicates without the need for a host program – viruses could propagate rapidly via email and the web, with the result that outbreaks often became global phenomena. By the end of the 1990s, viruses were capable of attacking the functioning of computer hardware, with Chernobyl being the first virus to affect the BIOS of a computer.

---

*The most prolific malware is email-aware, distributing itself automatically by email. Internet worms increase the risk to computer users, as they do not rely on email being opened.*

---

Melissa, Bubbleboy and the Love Bug were high-profile harbingers of the escalating email threat. Millions of recipients naively opened the latter's "love letter" attachment, causing the collapse of email systems worldwide. In 1999, Bubbleboy confirmed the absolute vulnerability of email, with another step change in virus delivery techniques. It was the first virus to infect a computer when email was simply viewed, rather than relying on the opening of an attachment to launch its payload.

For two decades, the number of viruses has continued to grow relentlessly, passing the 50,000 mark in 2000. As can be seen in Figure 1, since July 2002 the number of known viruses has increased from 75,000 to more than 115,000 by December 2005. During this latter period virus writers, such as the creators of the Bagle and Netsky series of worms, competed to see who could have the maximum impact. This type of cyber vandalism has had a significant effect on business productivity, providing a springboard for more overtly criminally motivated activities involving theft and fraud.

\* Growth in 1999, caused by the release of 15,000 viruses from one source, did not result in a commensurate increase in the threat to computer security.

## Evolution of the threat landscape

New issues for email users and administrators extending way beyond reduced productivity were created by the advent of unsolicited commercial email, or spam. The electronic equivalent of junk mail, spam was originally just an irritant in the shape of unwanted, or possibly offensive, advertising that cluttered inboxes. In the 21st century, spam began to evolve into more elaborate scams and threats to network security.

---

*The methods used by spammers have become more sophisticated, and spam is now increasingly combined with malware and used as a tool for online fraud or theft, or to propagate malicious code.*

---

As organizations deployed anti-spam solutions to reduce the impact on productivity, spammers changed their tactics. Their simple money-making schemes progressed from just sending unsolicited email, promoting their own products or dubious services, to something much more sinister. By joining forces with virus writers and hackers, spammers were able to develop a whole underground economy geared to outwitting anti-spam defenses and increasing the effectiveness of spam delivery systems. Campaigns that coordinate virus, spam, phishing, and spyware attacks have succeeded in generating more revenue and further compromising business productivity and confidentiality. The escalating nature of these assaults on computer users is plotted in Figure 2.

### Malware used as malicious tools

The term malware is now used to include viruses, worms, Trojans and spyware. Worms can exploit weaknesses in a computer's operating system and spread rapidly via the internet, and Trojans pose as legitimate software but actually carry out hidden, harmful functions. Backdoor Trojans add a further level of sophistication, incorporating themselves into a computer's startup routine, thereby allowing hackers to monitor keystrokes and steal confidential information from the computer without the user's knowledge. Virus writers have found it easier to deliver malicious code via Trojans, cooperating with spammers by using their lists to deliver Trojans via email attachments.

This development has ramped up both the volume and speed of propagation of malware. The alliance between the virus-writing and spamming communities has also spawned a widening range of increasingly complex threats.

### Multiple, or "blended", threats

The emergence of "blended" threats and financially or politically motivated attacks has blurred the distinction between viruses and spam. Simultaneously, the computer security debate has moved from the realms of cybergraffiti and vandalism to the more obviously criminal. Blended threats typically use spam containing malware to deliver a malicious payload. This highly efficient and stealthy means of propagation can be used to distribute high volumes to the maximum number of computers, or to target a smaller group more selectively. Either strategy can yield illicit access to confidential information.

### Denial of service and zombie attacks

Spammers and hackers have also found ways of hijacking computers for attacks that can be politically or commercially driven. In a denial of service (DoS) attack, hackers bombard email or web servers with unusual or excessive messages and attachments with the intention of crashing an organization's system, thereby denying the service to legitimate users. In a variant, known as a distributed denial of service (DDoS) attack, a hacker exploits a vulnerability in one computer system, from which a multitude of compromised systems can be triggered to mount a coordinated attack on a single target. The hacker is able to use the first computer to identify and compromise perhaps thousands of others, triggering one of many coordinated attacks with a single command.

---

*In DDoS and zombie attacks, the final target is not the only victim – the business systems controlled by the intruder are also compromised and could potentially be blocklisted as spam sources.*

---

Organizations are under further threat by spammers aiming to conceal the origins of spam and increase capacity at little or no cost. In a "zombie" attack, spammers hijack a vulnerable

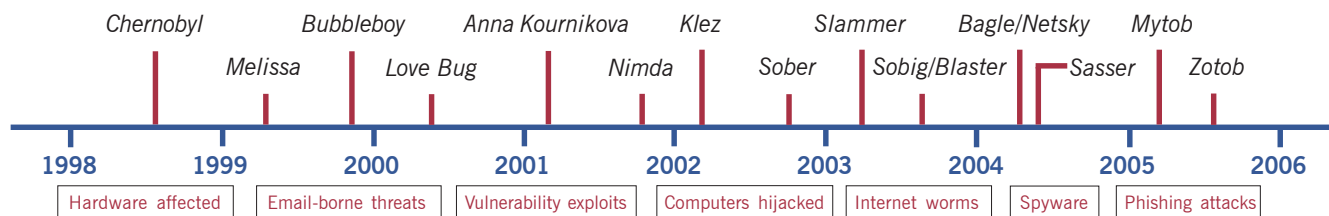


Figure 2: The complexities of the evolving threat landscape

computer or web server and use it to send out their emails for them, thus making the email appear to be from a legitimate source. Organizations with diverse networks and flexible connectivity policies, such as educational institutions, government bodies, and ISPs, are particularly attractive targets. Sophos estimates that over 60% of spam is being sent from computers hijacked in this way, many of which reside undetected within the networks of otherwise innocent organizations. Compromised systems can cause serious damage to reputation, threaten the delivery of outbound mail and act as the launch point for additional malicious attacks on the network.

## Increasing complexity

Virus complexity has reached new heights in the last two years. New types of malware, such as EXE packers, have emerged which are difficult to detect and disinfect. The hacking community has hijacked these legitimate compression programs to deliver malicious code while remaining undetected. The unique property exploited by hackers is that EXE packers are designed to keep an executable program permanently in compressed format – unpacking on the fly for execution only. Detection is therefore dependent on the ability of anti-virus software to penetrate the compressed file.

## The spy within

Another insidious development in recent years has been the increasing infection of computers with spyware – programs that steal information. Installed by a virus, or when a user clicks on a weblink or pop-up message, or opens an attachment in an email, spyware sends information from a computer to a third party without the user's permission or knowledge.

---

*Organizations infected with spyware can suffer damage to reputation, financial loss, and increased risk of litigation – as well as network disruption and decreased productivity.*

---

Spyware comes in many guises. Two of the most high-profile forms are:

- Keyloggers and backdoor Trojans, which can steal passwords and other confidential information.
- Dialers, which can surreptitiously dial a premium rate phone line and create revenue that is billed through the infected user's telephone service provider.

In addition to risking data theft, organizations infected with spyware are more vulnerable to hackers and further attacks.

## Phishing and its variants

Phishing is an increasingly common form of online theft, and represents another aspect of the increasingly complex and converging security threats facing individuals and businesses today. Unchecked, it could undermine confidence in the rapidly-growing e-commerce sector. In a phishing attack, computer users are spammed with authentic-looking emails that claim to come from well-known financial or e-commerce institutions, and are asked to click on a link contained within the message. The link takes them to what appears to be a legitimate website, which acts as the "bait". Here, they are tricked into handing over control of their online accounts by entering their passwords and other confidential data. Phishers are also placing Trojans on computers that are activated when the user visits the website.

---

*Confidence in e-commerce could be undermined by increasingly successful phishing attacks.*

---

It is extremely difficult for computer users – and even computer experts – to detect these exploits. According to the Anti-Phishing Working Group (APWG), up to 5% of recipients are successfully hoodwinked. The answer is effective spam protection and keylogger detection combined with a responsible attitude to unsolicited or unexpected email.

Variants of phishing include "pharming" and "spear phishing". Pharming involves poisoning a DNS server so that large numbers of users are redirected from genuine websites to spoof sites. Users suspect nothing because their browsers show the legitimate web address. Spear phishing is a recent development that focuses on a single organization. Employees at a company or government agency are sent emails that appear to come from a powerful person within the organization. In environments where authority is rarely questioned, it is relatively easy to trick employees into giving up passwords, so that the phisher can install Trojans or other malicious programs to find and steal intellectual property and confidential information.

APWG claims phishing attacks are rapidly increasing in both sophistication and volume: attacks more than doubled in the year to October 2005, when almost 16,000 were reported. Over 100 brands were hijacked in the previous month – a 65% increase since the beginning of the year.<sup>1</sup>

## Future threat developments

Nowadays, multiple variants of the same threat are relentlessly created and rapidly distributed, with the aim of defeating traditional signature-based virus protection and existing spam

rules. Recent events indicate the development of malware with increasingly sophisticated means of concealment, such as:

- Trojans that infiltrate Windows by integrating with the winlogon process – once installed here, these viruses stay live even if Windows is started in safe mode, making them very difficult to remove.
- Versions of the mass-mailing worm, Bagle – variants of which have been in circulation since the beginning of 2004 – that are able to split functionality between several files in an attempt to avoid detection.

However, there is a risk that high-profile worm outbreaks, such as Blaster and Bagle during 2005, distract attention from a more significant underlying problem – undiscovered or undisclosed vulnerabilities in software already running on business-critical systems.

### Web browsing risks

Many Sophos customers now claim that web browsing is the biggest threat to security and productivity, introducing spyware and adware to their computers. Organizations that patch their installed software rigorously and operate best practice policies<sup>2</sup> will be able to minimize the problem. However, the incidence of bots – malicious versions of web robots, originally designed to carry out automatic routines such as building databases for search engines – is increasing. A bot can be used to install spyware or even to create zombie networks – enabling spammers to use the bandwidth of thousands of computers to send junk email. SophosLabs estimates that the average time for infection of an unprotected Windows XP computer connected to the internet is just 12 minutes.

### Risks of flexible connectivity

Although boot sector viruses are more an historical artifact than a real threat today, the method which they originally used to spread – via removable floppy disks – has a modern equivalent. The increasing popularity of removable media with USB connectivity, including devices such as memory sticks and portable hard disks, has reintroduced a high-risk route to infection. The trend towards working at home and downloading multi-media files is also conspiring with the rapidly evolving connectivity of mobile non-computer devices via USB and Wi-Fi to create a minefield for IT administrators. However, the outbreaks of mobile phone and PDA viruses predicted by some security vendors have yet to materialize.

### Sophos's response to the growing threat

For 20 years, Sophos has responded authoritatively to new threats, and provided advice on best practice to maintain protection. Our innovative solutions offer rapid and proactive protection on multiple platforms against all forms of malware.

Expertise and technology is delivered through SophosLabs, a network of threat analysis centers that provides 24/7 protection via labs in three continents, ensuring the earliest possible detection of emerging threats. Genotype™ technology in our core anti-virus and anti-spam engines recognizes families of viruses and spam campaigns, providing pre-emptive detection against emerging threats.

---

*Sophos was first with a UNIX-based anti-virus solution and on-access scanning on Windows NT, and was the first major vendor to protect its customers against the Love Bug virus.*

---

Sophos Anti-Virus protects against spyware installing itself on computers, and version 6.0 will give businesses the ability to block or control adware and other non-malicious, but unwanted, applications. A network of spam traps around the world enables us to offer customers the Sophos ZombieAlert™ Service, which provides them with immediate warnings about spam originating from their networks. Similarly, organizations subscribing to the Sophos PhishAlert™ Service receive rapid notification of phishing attacks targeting their customers within minutes of being picked up by Sophos's threat detection network.

Sophos experts believe that the greatest danger to organizations currently remains with malware infecting desktop computers and servers. However, SophosLabs continues its research and development of technology to fight potential future threats from mobile devices and evolving connectivity.

### Summary

The network security threats faced by enterprises today are much more complex than 20 years ago. The exponential growth in malware is compounded by its speed of propagation and the complexity of blended threats, changing the nature of the risks. The behavior of network users is also changing rapidly: a key part of risk reduction is for organizations to implement an integrated security solution and actively manage their policies relating to email, web browsing, removable media, and connectivity. From the early boot sector viruses right through to the most complex blended threats, Sophos has provided robust protection. Our integrated solutions now protect against all types of threat, including viruses, spyware, spam, and policy abuse – proactively detecting malware before it can do any damage.

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

---

---

## Sources

- 1 Phishing Activity Trends Report, Anti-Phishing Working Group, July 2005 ([http://antiphishing.org/apwg\\_phishing\\_activity\\_report\\_sept\\_05.pdf](http://antiphishing.org/apwg_phishing_activity_report_sept_05.pdf))
- 2 [www.sophos.com/virusinfo/bestpractice](http://www.sophos.com/virusinfo/bestpractice) and [www.sophos.com/spaminfo/bestpractice](http://www.sophos.com/spaminfo/bestpractice)

## 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 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**