



# Sophos Security Threat Management Report

## Update July 2006

### Reviewing the first six months

In this update to our December 2005 annual security threat management report, we look at how the threat landscape has changed in the first six months of 2006 and what the likely trends are for the rest of the year.

Once again we have seen those responsible for securing an organization's network challenged in new and inventive ways. The demands being placed on IT have continued to be challenging as cybercriminals invent new ways to exploit human and computer vulnerabilities to steal and extort money from computer users and companies.

The numbers of malware increased, and the growing emphasis on secrecy and stealth that we saw at the end of last year has continued to spiral upwards. Spyware and phishing remain two of the biggest threats that businesses now face, and malware attacks are almost universally targeted on a small number of victims compared to the mass-mailing worms of the past, in an attempt to avoid drawing unnecessary attention to themselves.

The Global Security Survey released in June 2006 by the Financial Services Industry and conducted by Deloitte Touche Tohmatsu reported that more than three-quarters (78%, up from 26% in 2005) of respondents confirmed a security breach from outside the organization.<sup>1</sup> The survey called identity theft the "crime of the 21st century".

#### 6 months at a glance

Over 180,000 threats detected by Sophos  
Viral emails down to 1 in 91  
New Trojans outweigh viruses and worms 4:1  
Ransomware demands money with menace

### Growth rates

The number of threats has continued to grow. By June 2005 the number of different pieces of malware protected against by Sophos Anti-Virus stood at 140,118\*. A year later, by June 2006, Sophos Anti-Virus was identifying and protecting against 180,292\* different viruses, spyware, worms, Trojan horses and other malware, as well as adware and other potentially unwanted applications (PUAs).

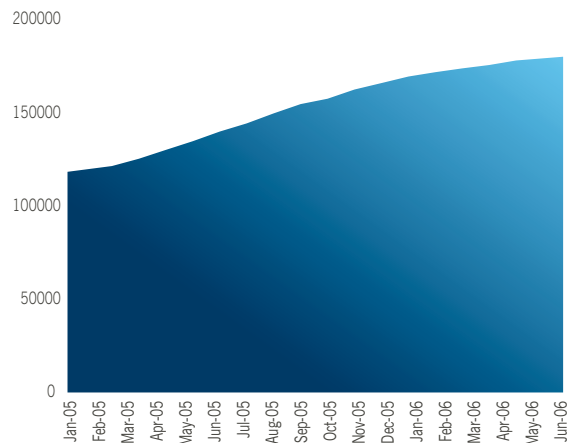


Figure 1: Growth in malware

Malware authors are increasingly turning away from email-aware worms to other methods of infection in their search for victims. Financially motivated hackers do not want to infect millions of emails as it draws attention to their malware, and increases the chance that users will take efforts to protect themselves.

Similarly, the number of computers targeted by each spam attack was reduced so that the threat would sneak under the radar of anti-spam techniques that measure email volume.

Sophos research reveals that only 1 in every 91 of all emails were viral so far this year, compared with one in every 35 for the same period in 2005 – further proof that email worm

\*Note that we have changed the way we calculate and report the threats that we protect against so that we more accurately reflect the number of individual threats detected by our proactive Genotype technology.

attacks have dropped off in favor of other methods of malicious attack.

### Top ten malware threats

Sophos has a global network of tens of thousands of monitoring stations capturing data about the latest viruses spreading via email, giving it a unique insight into the health of email systems and early warning of emerging virus outbreaks.

Interestingly, the top ten chart (seen in Figure 2) is dominated by viruses which have been around for a considerable time, as can be seen in the graph below.

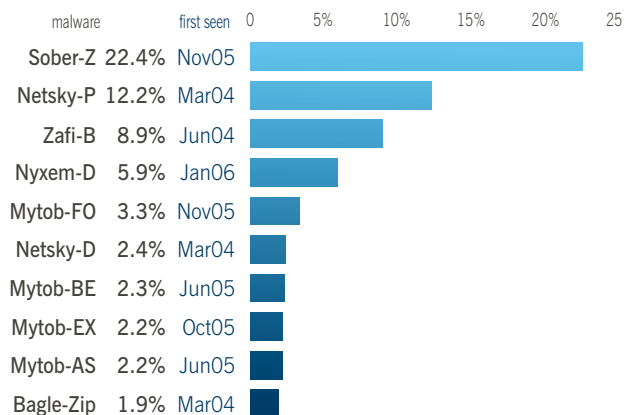


Figure 2: Top ten threats and their longevity

The hardest hitting threat from January to June 2006 was the Sober-Z worm, which, at its peak, accounted for one in every 13 emails.<sup>2</sup> The worm, which masqueraded as an email from the FBI or CIA claiming that the recipient is believed to have accessed illegal websites,<sup>3</sup> dominates the charts despite being programmed to stop spreading from 6 January 2006.

The only new worm to have broken into the top ten list of malware is the Nyxem-D worm (also known as Kama Sutra), which spread via email posing as obscene pictures and sex movies.<sup>4</sup> This data underlines that more recent attacks have been more insidious, subtly infecting smaller groups of people in an attempt to avoid drawing attention to themselves.

### Trojans

The first six months of 2006 showed that virus authors continue to prefer infecting Windows machines with Trojans over viruses and worms.

In 2005, Trojans outnumbered viruses and worms almost 2 to 1; today, computer users are four times more likely to be hit by a Trojan than by a virus or worm.

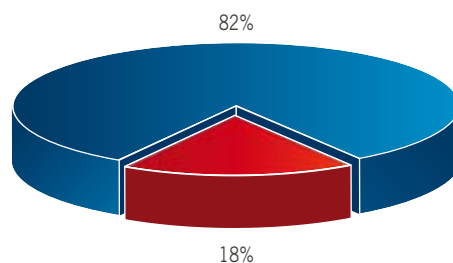


Figure 3: New Trojans (82%) and viruses (18%) threats

1 in every 2 Trojans in the first six months of the year has contained spyware components – performing activities such as logging key strokes, stealing information like user names, passwords or credit card details, and giving third-party access to infected computers.

As Trojans cannot spread on their own, the author must consider ways to entice computer users to download or run the malware. Email is exploited because it is a cheap and immediate method of communication. Rather than having a message contain an infected attachment, spam messages today will often display a link to a website. Should the recipient visit the webpage, malicious code hidden on it will attempt to gain access to the machine via a vulnerability on the Windows machine – this could be a software bug or insufficient firewall or anti-virus defenses - in order to download itself without alerting the user.

### New threats

#### Ransomware

This year has seen Trojans being used to bring old-fashioned blackmail into the digital age, and highlights more than anything the view that malware authors are turning more towards focused attacks against specific small groups of people rather than a mass-bombardment of internet users.

Ransomware is malicious software, often Trojan horses, that stops users accessing their files – usually by encrypting them – and then demands money with menaces. We have seen several examples of this at SophosLabs. Zippo, for example, which arrived on the scene in March 2006 encrypted files and demanded \$300.<sup>5</sup>

Ransom-A prevented victims from accessing their computer data until a ransom of \$10.99 was paid via Western Union.<sup>6</sup> It threatened to delete one file every 30 minutes until the ransom was paid. It also displayed pornographic images and an unsavoury message. If the user tried using CTRL+ALT+DEL to stop the Trojan running, they were subjected to a taunting message.

Arhiveus (shown in Figure 4) demanded that the victim buy goods from an online drugstore.<sup>7</sup>

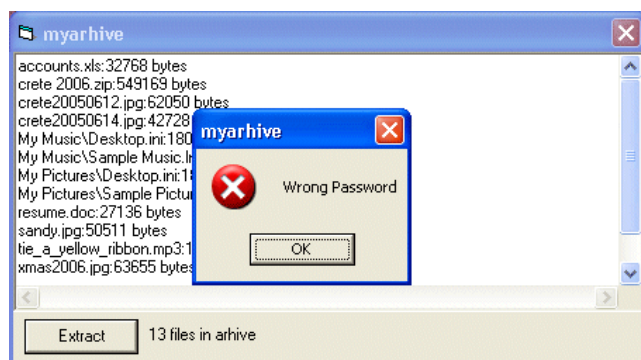


Figure 4: Held to ransom – the Arhiveus Trojan

## Rootkits

A rootkit is a set of software tools placed on a computer by a third party and intended to conceal running processes, files or system data. The concept came to prominence at the end of 2005 when Sony used one on its music CDs to protect its copyright. However, it opened up a vulnerability that was exploited by a number of Trojan horses. Sony has accepted that this cost users and businesses money and inconvenience and has offered them their money back.<sup>8</sup>

The threat, though, still exists with bespoke Trojans often employing rootkits, and installing themselves on a small number of systems to call very little attention to themselves. It is likely that we will see increasing sophistication in this tactic over the coming months. They are, however, difficult to write and so we tend to see variants of existing rootkits. Whether they will work under Vista – Microsoft's new operating system to be released in 2007 – remains to be seen.

## Spammers

Medical-related spam (which primarily covers medication which claims to assist in sexual performance, weight loss, or human growth hormones), and spam containing adult content remain prolific. And stock-related spam, continues to remain hugely successful for unscrupulous spammers.

In mid-June 2006, there was a widespread spam campaign detected by Sophos experts that encouraged users to buy stock in a company called Southern Cosmetics.<sup>9</sup> The spammed emails, which consisted of an embedded graphic in an attempt to avoid detection by anti-spam filters, told recipients that savvy investors would be wise to buy stock in the company because of business deals it was making with Naomi LLC, a cosmetics firm endorsed by country music singer Naomi Judd.

Southern Cosmetics' stock price rose dramatically following the spam email. An examination of the company's share price shows that there was a marked increase in trading in the stock, with the share price rising to a high of 6.6 cents from its pre-spam campaign low of less than one cent per share.

## What lies ahead?

### Mobile

Since the late 1990s some anti-virus companies have predicted the imminent arrival of a major mobile phone virus outbreak, but this has still not emerged. To date, there have been no large-scale incidents involving mobile phone or PDA viruses and the overall threat to mobile devices is tiny compared to viruses affecting Microsoft Windows computers.

One of the reasons why mobile viruses have not become a problem is that the organized criminal gangs responsible for much malware written today see no benefit in targeting the devices, compared to the larger number and more vulnerable population of Windows computers. Viruses can spread successfully, and quickly, on the common Windows platform without having to worry about the different operating systems and differences seen in the varied cell phone market.

As mobile devices become more ubiquitous, and common operating systems come into widespread use, we are likely to see more malware being written for the platforms.

Despite the present extremely low threat posed by mobile malware, security vendors are building technology to protect mobile devices from malware, and we can expect to see more announcements regarding protection solutions in 2006.

### Windows Vista

In March 2006 Microsoft announced that the release of the next version of their operating system, Windows Vista, is being delayed until at least 2007.

The delay in Vista's launch is bad news for security-conscious computer users as it incorporates a number of new features which should harden the operating system against attack.

One feature of Vista is the inclusion of Defender, an anti-spyware tool designed for home users. Attacks against consumers have allowed hackers to make significant profits through zombie computers.

Windows Vista will also probably force malware writers to re-assess the techniques they are using for both regular malware and rootkits. Existing rootkits will most likely not work simply because of changes in the underlying operating system. However, it may just be a matter of time before the bad guys learn enough about Vista to build rootkits or other malware with the equivalent degree of stealth capability.

### Macintosh

Although the first malware for Mac OS X was seen in February 2006, it has not spread in the wild and not heralded an avalanche of new malicious code for Apple's operating system. Hackers remain happy to primarily target Microsoft Windows users and not spread their wings to other platforms. It seems likely that Macintosh will continue to be a safer place for computer users to be for some time to come.

Figure 5 shows another company being monitored by Sophos. The campaign email was spammed out on 21 April rocketing the volume of shares sold to nearly 400,000 and more than hiking the share price by 74%. A week later, a followup spam saw prices go even higher.

This sort of spam is usually sent at the weekend because most vendors – unlike Sophos – do not have researchers analyzing new spam and distributing new rules to block it at the weekend

It uses exactly the same techniques of a pre-internet, centuries-old con. The spammer (often part of an organized crime ring) buys the stock at low prices, talks up the stock (via spammed emails), sees the share price rise, and then sells. The spammer makes a small fortune, the buyer is left with overpriced stock and the company financial strategies are left in disarray.

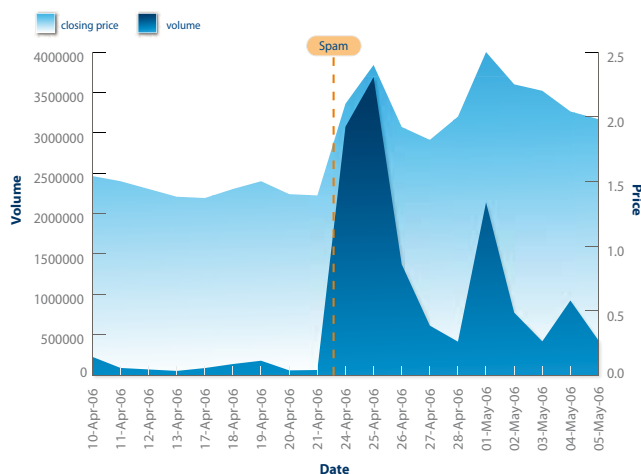


Figure 5: The effect of pump-and-dump on company shares

### Social engineering

Most people have wised up to the fact that if they click on an attachment purporting to be of a semi-clad celebrity they will end up with more than a cheap thrill. So the social engineering has moved on and become more subtle. Political issues, topical news events and tugging at the heartstrings have made recognizing the trap more difficult for users, and put a big onus on organizations to have watertight security in place.

Sophos has continued to intercept a wide variety of this type of email scam. In June 2006, a version of the Stinx Trojan claimed that George W Bush and Tony Blair were involved in a Middle East oil price cover-up,<sup>10</sup> while the Sixern worm lured victims in the run-up to the World Cup soccer tournament by claiming to contain pictures of football fans engaged in a naked match.<sup>11</sup>

### The top spam relaying countries

Spam is increasingly a worldwide problem, benefiting from the fact that wherever the spammer is based, they can take advantage of insecure broadband home computer connections anywhere in the world to send their unwanted marketing messages.

The United States continues to head the list of the “dirty dozen” countries from which spam is sent (23.4%) but is continuing to relay less of the world’s spam than it did during 2004 due to a number of factors, including jail sentences for spammers, tighter legislation and better system security.

The US is followed by China (20.5%) and South Korea (8.7%). However, as Figure 6 shows, Asia as a whole is responsible for relaying more spam than the US.

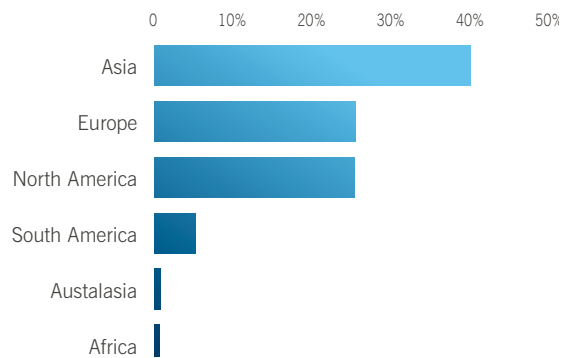


Figure 6: Regional relaying of spam

### Need for protection

Insufficiently protected computers continue to come under attack in shorter timescales than ever before. Exploits, taking advantage of software flaws, can spread without human intervention. Hackers are increasingly releasing malware before users have been able to apply the security patch from Microsoft, or even – in some instances – before a patch has been published. The Oscan-B Trojan horse, for example, exploits a day-zero vulnerability in Microsoft Word, allowing it to infect computers when infected Word documents are opened.<sup>12</sup>

### Summary

The growing quantity of new threats, the speed with which they spread, and the hugely complex task of protecting networks against them are going to have significant implications for businesses throughout the second half of 2006. As cybercriminals become more cunning and use increasingly inventive methods to try to avoid their malware being detected, organizations will look to single vendors with cross-threat expertise and consolidated product solutions to protect their systems, their data and their business continuity.

## Sources

- 1 Global Security Survey, Financial Services Industry and Deloitte Touche Tohmatsu, June 2006
- 2 The latest news on the Sober-Z worm outbreak, 1 in 13 emails are now infected by the Sober worm  
[www.sophos.com/pressoffice/news/articles/2005/11/soberz.html](http://www.sophos.com/pressoffice/news/articles/2005/11/soberz.html)
- 3 Sober-Z worm poses as bogus messages from FBI or CIA  
[www.sophos.com/pressoffice/news/articles/2005/11/soberfbi.html](http://www.sophos.com/pressoffice/news/articles/2005/11/soberfbi.html)
- 4 Obscene Kama Sutra worm spreads via email  
[www.sophos.com/pressoffice/news/articles/2006/01/nyxemd.html](http://www.sophos.com/pressoffice/news/articles/2006/01/nyxemd.html)
- 5 Zippo Trojan horse demands \$300 ransom for victims' encrypted data  
[www.sophos.com/pressoffice/news/articles/2006/03/zippo.html](http://www.sophos.com/pressoffice/news/articles/2006/03/zippo.html)
- 6 Ransom Trojan horse demands money with menaces  
[www.sophos.com/pressoffice/news/articles/2006/04/ransom.html](http://www.sophos.com/pressoffice/news/articles/2006/04/ransom.html)
- 7 Devious Arhiveus ransomware kidnaps data from victims' computers  
[www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html](http://www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html)
- 8 Refunds for music fans hit by Sony DRM rootkit  
[www.sophos.com/pressoffice/news/articles/2006/05/sonysettlement.html](http://www.sophos.com/pressoffice/news/articles/2006/05/sonysettlement.html)
- 9 Cosmetics company's stock price rises sharply following spam campaign  
[www.sophos.com/pressoffice/news/articles/2006/06/stockspam.html](http://www.sophos.com/pressoffice/news/articles/2006/06/stockspam.html)
- 10 Spammed Trojan claims Bush/Blair Middle East oil cover-up  
[www.sophos.com/pressoffice/news/articles/2006/06/stinxw.html](http://www.sophos.com/pressoffice/news/articles/2006/06/stinxw.html)
- 11 Nude World Cup worm spreads via email  
[www.sophos.com/pressoffice/news/articles/2006/06/sixem.html](http://www.sophos.com/pressoffice/news/articles/2006/06/sixem.html)
- 12 Trojan horse exploits zero day Microsoft Word vulnerability  
[www.sophos.com/pressoffice/news/articles/2006/05/oscorb.html](http://www.sophos.com/pressoffice/news/articles/2006/05/oscorb.html)

---

Sophos is a world leader in integrated threat management solutions purpose-built for business, education and government. With 20 years' experience and consolidated anti-virus, anti-spyware and anti-spam expertise SophosLabs protects even the most complex networks from known and unknown threats. Our reliably engineered, easy-to-operate products protect over 35 million users in more than 150 countries from viruses, spyware, intrusions, unwanted applications, phishing, spam and email policy abuse. Round-the-clock vigilance has resulted in our increasingly rapid international growth, expanding user base and continuous profitability. Our instant response to new threats is matched by business-focused, 24/7 technical support, and has led to 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