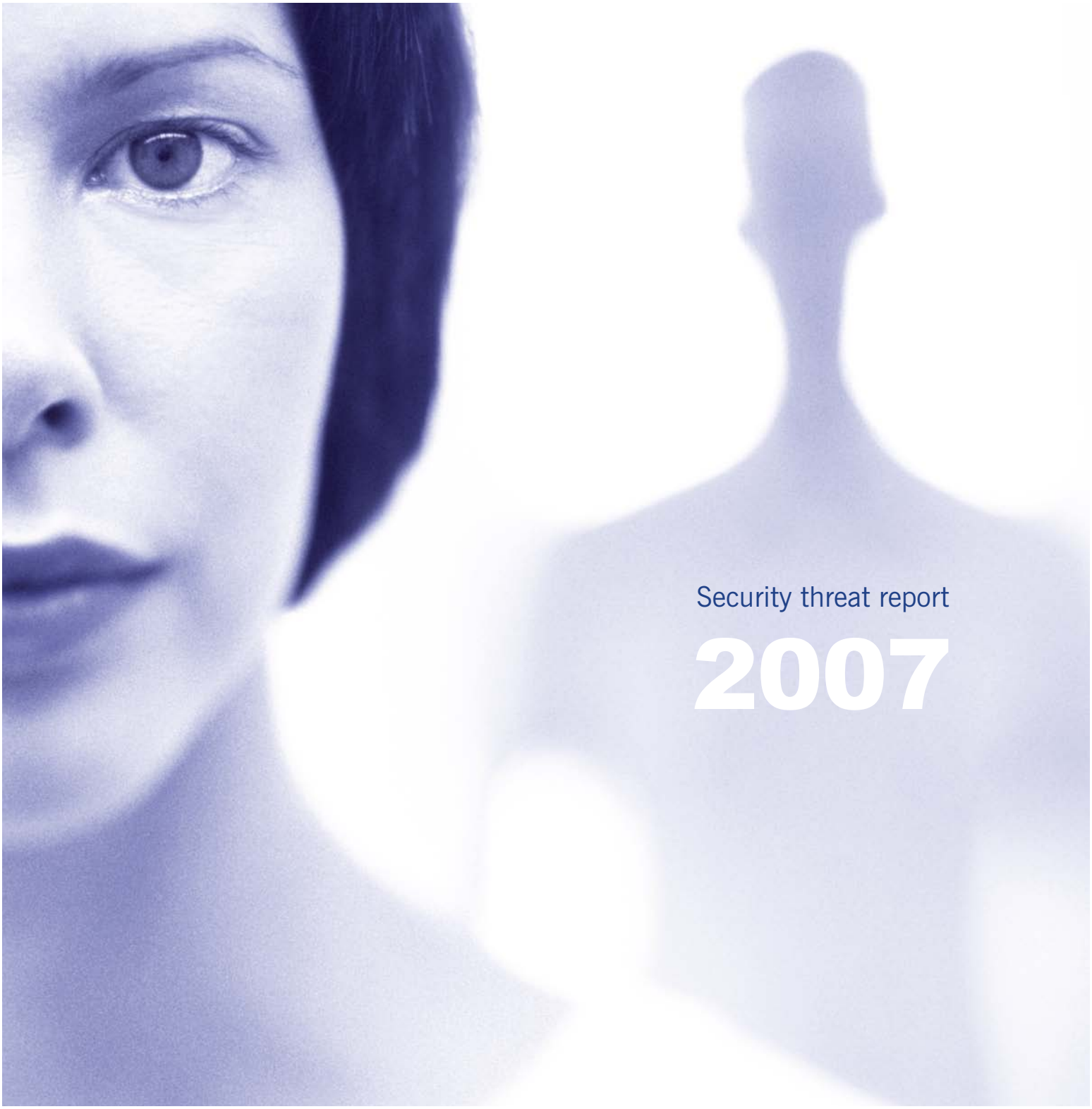


Security threat report

2007

SOPHOS

secured.

SOPHOS

Security threat report **2007**

Overview

2006 saw increasingly surreptitious behavior on the part of cybercriminals who have found more cunning ways to hide their activities. Copycat websites that only the keenest eye can detect as fake, spam campaigns that mutate in a matter of seconds in order to evade detection, phishers replicating voicemail systems to duplicate the switchboards of legitimate companies – these are just three examples of the rapidly changing nature of the threat.

The total number of different malware threats protected against by Sophos was 207,684, with Mytob at the top of the list of malware families. Malware continued to spread via spam, instant messages, hacked websites, email, and network shares. In addition, the web became a significant source of threats, being overrun by spyware, adware, potentially unwanted applications and undesirable websites. The motivation, as with all other spreading methods, was financial gain, with perpetrators trying to steal confidential information or generate income through compromised PCs.

As malware writers continued to attempt to use malicious code in a covert fashion to evade detection, the trend away from infected email that we saw in 2005 persisted. The proportion of infected email was down from 1 in 44 in 2005 to just 1 in 337 in 2006.

Increasingly complex ways of getting private information from users and businesses has seen more rapidly evolving spam campaigns, complex operational methods, and a raft of new scams. These have been met with new laws and an increased vigor in applying them, but the threat landscape remains challenging for the year ahead.

2006 at a glance

- Malware authors continuing to turn their backs on large-scale attacks in favor of more focused attacks
- Explosive growth of web-based downloaders to spy on users
- Total number of different malware threats protected against – 207,684
- 41,536 new pieces of malware detected by Sophos
- Trojans outnumbering Windows viruses and worms 4:1
- New mass-mailing worm, Stratio had over 1000 unique variants in November
- Email containing infected attachments – down to 1 in 337
- Most spam continuing to be relayed by poorly protected US computers

Only 34% of businesses think 2007 will be a better year for security than 2006.

Source: Sophos online poll, December 2006

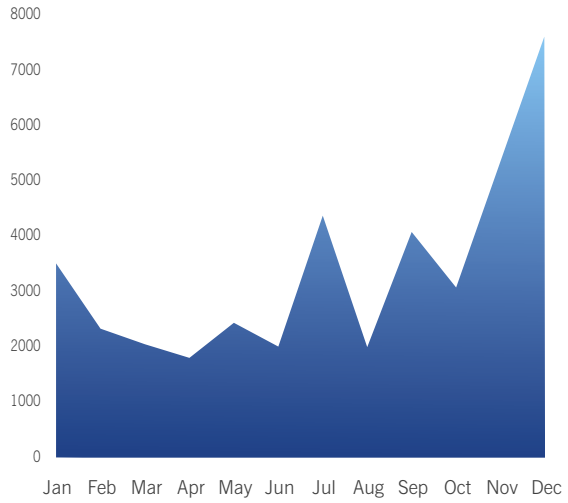
Malware

Malware growth rates

In 2006, Sophos detected 41,536 new threats. Malware writers continued to find new ways of infecting computers and duping users into handing over confidential information throughout the year. There was a particular surge at the end of the year, with November seeing 7612 new threats – nearly four times November 2005's number of 1940.

Sophos does not expect the growth in malware to taper off in 2007. If anything, we expect to see even more devious attempts to steal information with the end goal of financial gain.

The spike in the graph above is attributable to the emergence in 2006 of a family of malware called Stratio, also known as Stration or Warezov. This mass-mailing worm saw major growth and over one thousand unique variants of it were spammed out in November. (Stratio is described in more detail on page 4.)



New malware threats each month in 2006

Top ten email threats

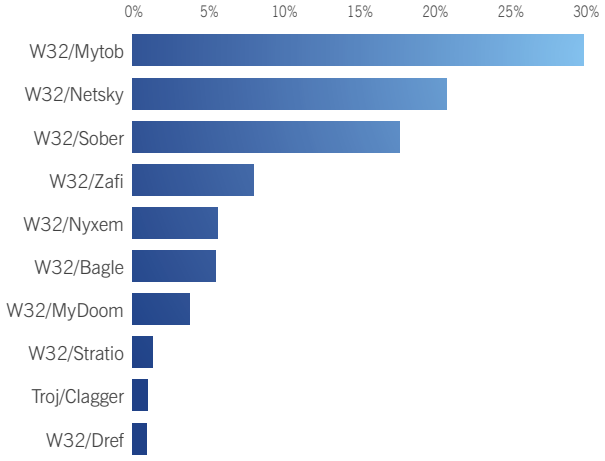
Sophos has a global network of tens of thousands of monitoring stations capturing data on the latest viruses spreading via email.

Although the proportion of infected email fell from 1 in 44 in 2005 to just 1 in 337 (0.3%) in 2006, there was nevertheless some high-profile malware dropping into users' inboxes. Worms such as Mytob, Netsky and Sober spread widely via email in 2006.

1 Mytob

The list of top ten malware families reveals that variants of the Mytob worm continue to plague insufficiently protected users around the globe. Mytob first emerged in March 2005, yet people are still being infected by this email-aware worm. 18-year-old Farid Essebar, a Russian-born resident of Morocco, known as the owner of the online handle "DiablO", was sentenced to two years in jail for spreading the Zotob worm.[1] Evidence found within some Mytob variants suggests that he was also involved in their creation.

With thousands of different variants of Mytob, many of which are hidden within bespoke compression code, it is likely to continue to hit unprotected computer users in 2007.



Top ten malware families 2006

2 Netsky

On 8 May 2004, the German teenager, Sven Jaschan, was arrested in connection with the widespread Netsky and Sasser worm outbreaks. In July 2005, he was sentenced to one year and nine months on probation and 30 hours community service.[2]* Despite this sentencing, the Netsky family, in particular variants Netsky-P and Netsky-D, continue to make a significant impact on the charts.

An additional worry is that Netsky-D can run on a default installation of Windows Vista, Microsoft's recently released operating system.[3] Although Vista includes additional security features which will help lock down a computer from attack, this threat again demonstrates the importance of up-to-date virus protection.

3 Sober

Sober also continues to be a widespread threat. Having first emerged in October 2003, it continues to present itself in Sophos's top ten lists. Its most widespread variant, Sober-Z, first seen in late 2005, sent itself as an email attachment pretending to be an email from the FBI, CIA or German authorities, and attempted to turn off security software on the user's computer. It stopped spreading on January 6, 2006 but despite spreading for only a few days at the beginning of the year, it still managed to secure the Sober family third place in the list of the most prolific malware families of 2006.**

4 Zafi

Another old-timer, Zafi was first seen in April 2004, and spread by harvesting email addresses. The fourth version of this code, Zafi-D, is the most widespread of this family.[5] Posing as a Christmas greeting, it used social engineering techniques to fool users into launching the attachment. At its height, it accounted for 1 in every 10 emails travelling across the internet and claimed number one position in the 2005 virus chart.

* Two years ago, in a blaze of publicity, Jaschan was hired by a German security firm, sending out a dangerous message that virus writers might be able to gain hasty employment in the industry despite their malicious behavior.

**In an odd twist, an unnamed 20-year-old German man, who had a number of pornographic pictures of children on his computer, turned himself in to the authorities, believing a message sent by Sober-Z which claimed he was being investigated by Germany's Federal Crime Office (known as the BKA) for visiting illegal websites[4].

5 Nyxem

This mass-mailing malware, most commonly known as the Kama Sutra worm because it uses a variety of pornographic disguises, caused panic for infected computers' users in early 2006.[6] Its payload was destructive, destroying DOC, XLS, MDB, MDE, PPT, PPS, ZIP, RAR, PDF, PSD and DMP files on the third day of any month.

6 Bagle

The Bagle family was first seen and protected against in January 2004. Despite its maturity, computer users are still being infected by this threat. Several more recent variants spread widely in February 2006: Bagle-CM posed as a message offering free tickets to the Winter Olympic games in Turin,[7] while Bagle-CO carried the words of love in a fake Valentine greeting.

The success of these threats is a result of too many computers running today without appropriate protection. Variants of Bagle will continue to spread via email until affected computer users install anti-virus against these threats.

Microsoft Windows Vista

Microsoft launched Windows Vista, its successor for Windows XP, in November 2006. Vista boasts a number of security settings, including User Access Control, which allows the user to make choices on what is allowed to run on a case-by-case basis and offers better protection against malware. Its Windows Mail email client has a number of default settings which can help stop malware from being executed. This is good news for computer users. Having an operating system that can offer better protection against threats will certainly compliment their security policy.

However, it is important that users do not rely solely on the security improvements in Windows Vista to protect their systems from malware attacks. Sophos tested Microsoft Vista in its default settings and found that three high profile and widespread email-aware worms would run on Vista: Stratio-Zip, Netsky-D and MyDoom-O. These three variants represented almost 40% of all the threats that were circulating during the month of November 2006.

Microsoft has an additional challenge to face in the coming year. With Microsoft comfortably retaining the largest portion of market share in the operating system business, they will continue to be targeted by malware authors searching for vulnerabilities in Vista code. Although Microsoft has made great improvements in issuing patches for known security holes in the code, exploits are regularly used in malware to bypass security on computers.

7 MyDoom

The MyDoom family of worms has been widespread for a number of years. First seen in January 2004, MyDoom has attracted a lot of attention, not least because software company SCO announced that it was offering a $250,000 reward for information leading to the successful arrest and conviction of its author.[8]

An additional worry is that the most prevalent variant – MyDoom-O – can, like Netsky described on page 3, infect Vista computers and again demonstrates the importance of up-to-date virus protection.[9]

8 Stratio

Stratio was a new mass-mailing worm which emerged in August 2006 and its aggressive distribution led to its position in the top ten malware threats.[10] It spreads via email using a variety of disguises, including one which ironically poses as a warning that the recipient's computer has been infected by a worm. At the end of the year Stratio-Zip was one of the three high-profile worms discovered to be capable of infecting Vista computers.

Several thousand variants of the Stratio worm were widely spammed out, on some days accounting for more than 50% of all reported malware. The purpose of the Stratio worm is to spread image spam, incorporating random pixels to act as "noise" to try and avoid detection by simpler anti-spam filters. It does this by pulling down an array of additional downloader components from the web. It caused a notable increase in the amount of spam being sent across the internet in late 2006. The messages sent by the malware typically advertise online pharmaceutical drug stores.

9 Clagger

Clagger is the only Trojan that appears in the top ten. Since Trojans cannot spread on their own, Clagger must have been spammed to millions of email addresses in order to enter the chart, which demonstrates just how successful rapidly evolving spam campaigns can be. By trying to exploit a list of known vulnerabilities, the Trojan turns off security settings once it installs itself on a PC. The purpose is to download spyware applications to steal sensitive information. For example, it was distributed as an attachment in emails that claimed to be from PayPal and Amazon in the early part of 2006.[11] Clagger was also highlighted in the top ten of Sophos's mid-2006 report where it held eighth position – further indication of the relentless spamming of this Trojan.

10 Dref

First seen in mid-2005, early versions of Dref spread via an IRC channel and by attaching themselves to outgoing emails. This mass-mailing Windows worm turns off anti-virus applications, sends itself to email addresses found on the infected computer and drops more malware onto users' PCs. Later versions, such as Dref-N, attempted to fool recipients into opening the infected file, for example by posing as bogus breaking news stories, including the outbreak of a nuclear war and the announcement of President George Bush's demise.[12] The intention was that, by using this type of story, informed computer users, aware of the risks of infected attachments, were more likely to fall victim to the attack.

A later variant, Dref-V, accounted for a staggering 93.7% of all virus reports in the last 48 hours of 2006, posing as a Happy New Year message.[13] The success of this piece of malware took advantage of users coming back to their workstations after the holiday period, rushing through their email and clicking on attachments.

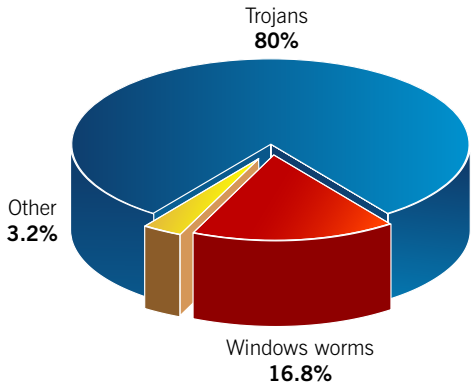
Email threats in 2007

Email will continue to be an important vector for malware authors when they distribute their malware, but Sophos expects to see the number of mass-mailing worms using infected attachments to continue to decline. Replacing this trend will be spam messages with images and links to infected websites. The reason for this shift is twofold. By not having an infected executable attached to the email, the email stands a better chance of being delivered to the recipient. Second, worms are difficult to control – their spread affects all vulnerable computers. The more viruses and worms are distributed, and the more widespread they become, the more attention they receive. By infecting websites with Trojans in the forms of downloaders and spyware applications, malicious code writers can better target specific audiences, which means their malware is better able to sneak onto a computer undetected.

Trojan horses

Even though viral attacks, such as those from Dref and Stratio worms were widespread, and therefore appear in the list of top ten malware threats of 2006, they are, in fact, far outnumbered by Trojan attacks, which are spammed out in small targeted campaigns but in vast numbers.

Trojans represented more or less the same proportion of the threat throughout 2006, averaging around 80% of malware detected throughout the year. This continued the trend of 2005 where Trojans outnumbered Windows worms every month, although the percentage of the threat then was only 62%.



Trojans versus Windows viruses and worms 2006

Spyware and downloaders

Spyware continues to present organizations with a serious headache and has raised the profile of web security significantly. Spyware is now the second largest security concern for organizations.[14] It sits secretly on computers, logging keystrokes, and stealing and sending confidential, financial and personal information from the computer to a third party without the user's permission or knowledge. It also opens up networks to further attack.

In their efforts to steal information, malware writers have become increasingly devious. They continue to place "traditional" spyware code on individual computers. However, they are also moving strongly towards a new method in which they spam out emails offering, for example, a plug-in to view videos or pornography or even offering free bogus security applications. The link in reality takes the duped user to an infected website from which a backdoor or data-stealing Trojan is downloaded. In its simplest form, as soon as the web page loads, malware on the website infects the visiting computer.

This type of Trojan downloader is not actually new, but downloaders are playing an increasingly important role in malware creation and what we are increasingly seeing, are more complex routes to infection, where the infected site first attempts to assess the security in place on the computer: it looks for vulnerabilities to exploit, out-of-date virus protection or a way to bypass a firewall. The idea is to find any means of downloading security-disabling code onto the visiting computer and then to download further malicious code. In order to obfuscate the intent, several downloaders will be used: one downloader pulls down another downloader on a different site which pulls down another on yet another site and so on. The last downloader in the series has the job of pulling down the spyware which will be used to steal sensitive information or give access to an unauthorized third party. Because security has been suspended, this spyware has a better chance of installing itself without being detected.

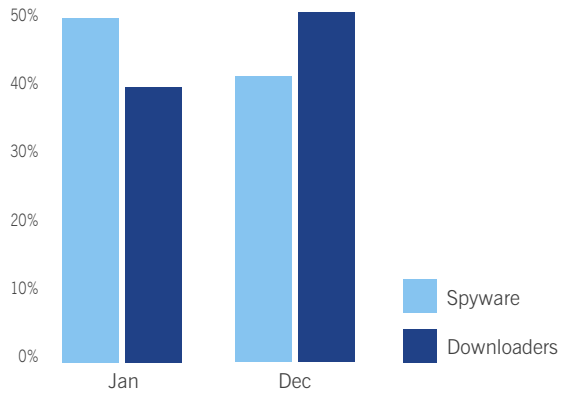
High-profile families have used Trojan downloaders to great effect (for example Bagle[15]) and many threats that spread via IRC are equipped with "download and execute" backdoors. Another example is Zlob, also known as Popupper or Puper.[16] This family of Trojans encompasses a whole variety of different components, and the extent to which it causes problems is made evident by the mass of postings within online forums. Zlob primarily uses pornographic websites to entice its users into downloading and running a file pertaining to be a video codec installer required to view a specific adult movie, or a password management tool, purported to be needed to access restricted sites. In some instances, the sound from an adult film is heard, but no image can be seen – this acts as a further trick to encourage users to download files that they are told are necessary.

As Trojan downloaders have come of age – their versatility making them more attractive and their use in malware increasing dramatically – Sophos expects their use alongside spyware to continue. Victims, particularly those who have visited pornographic sites, are unlikely to come forward in droves. Additionally, by complicating the route between the initial downloader and the eventual spyware installation, it makes it difficult for smaller security vendors who lack an overview of the entire picture to be able to adequately protect their users. As a result, smaller companies might want to replace existing security measures with a one-stop

solution, so that the software solutions that are blocking malware, spam, spyware, adware and hackers can all communicate and be managed centrally.

The graph on the right shows the percentage of email that contained spyware and the percentage of email that linked to websites from which spyware is downloaded at the beginning and end of the year. The shift towards downloaders is clear.

Meanwhile, the malicious code planted on websites ready for the Trojan downloaders to pull down is being changed frequently by hackers in an attempt to evade detection. In some instances, Sophos has seen malicious code on websites being altered on average seven times a day. Some of the more commonly encountered adware is also changed and repackaged frequently by its authors in order to evade detection by security products.



Spyware and downloaders in 2006

Malware – its origins and haunts

Aside from producing protection against new and unknown malware, experts at SophosLabs conduct research into which countries are responsible for writing malicious code, and which nations are hosting websites that deliver viruses and Trojans to innocent users' computers.

Where malware is written

Forensic analysis by SophosLabs to determine where malware has been written has revealed some interesting differences in the motives and tactics used by different hacking groups around the globe.

For instance, 30% of all malware is written in China. Most of it takes the form of backdoors, but a surprising proportion (17%) of the malicious software originating from the country is designed to steal passwords from online gamers.[17]

Brazil accounts for 14.2% of the malware that has been analysed by SophosLabs. The majority of the code written in the South American country is Trojan horses, designed to steal information from online bankers.

Russian and Swedish hackers (responsible for 4.1% and 3.8% of the malware respectively) mostly create backdoors that allow hackers to gain access to compromised computers. For example, the Bifrose family of Trojans makes up 15% of the malware written in Sweden and is designed to stealthily open backdoors.

Ukraine also appears to be a hotbed for the creation of backdoors and bots, with 3.4% of all malware studied by SophosLabs established as having originated in the Eastern European country.

Knowing that China's malware authors are largely interested in stealing information from gamers and Brazil's authors want to steal banking information, helps security experts and authorities strengthen their profiles. Sophos expects hackers in China, Russia and Brazil to continue in similar vein in 2007, and it will be interesting to see which other countries crop up in the list and which particular type of malware they will lean towards.

Countries hosting malware on the web

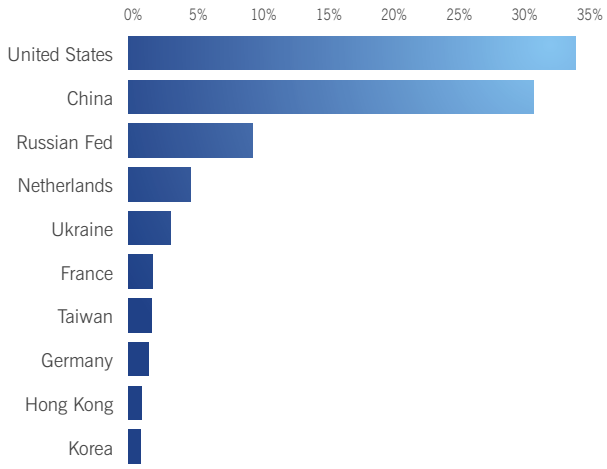
The graph on the right shows the proportion of unique URLs of websites containing malware that were seen by SophosLabs during 2006. They are grouped by the country in which the web server was hosted.

The enormous number of computers based in North America probably makes it no surprise that the US heads the list, and is hosting over a third of all websites containing malicious code.

One country which is of interest, however, is the Netherlands. The country's appearance in fourth place in the chart at 4.7%, may be explained by some web hosting companies based there having adopted a history of turning a blind eye to their users' activities, protecting their activities under the banner of freedom of speech. In fact, the country hosts numerous sites with information and code dedicated to crackers and hackers.

Sophos believes that web hosting companies need to act responsibly as members of the global internet community, policing content published on customers' web space more closely, and liaising with the authorities to ensure that malicious code found on a public site is quickly removed.

It will be interesting to see how these trends develop in the coming year. It is difficult to make predictions on this particular aspect of the report because it is very much based on the dedication of governments to crack down on sites that host malware. In many instances, websites are attacked and the administrators of the sites do not have enough countermeasures in place to prevent hackers from breaking in. With today's malware being so covert, administrators without adequate protection might not even be aware that a threat is lurking on their site, ready to infect their visitors' computers.



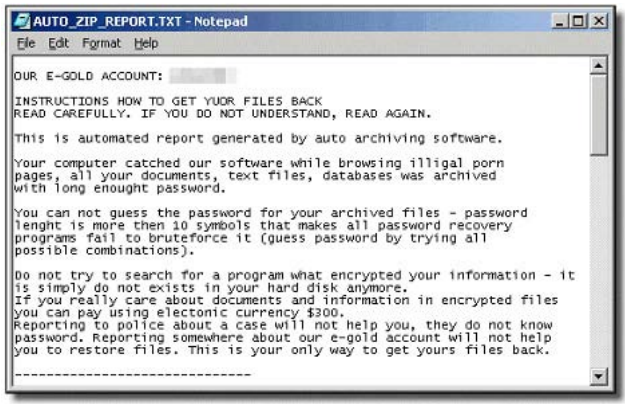
Top ten countries hosting web-based malware 2006

Ransomware

Ransomware is malware designed to "kidnap" data by encrypting it, only providing the password once the ransom has been paid. More aggressive examples even threaten to permanently delete files every 30 minutes until the ransom is paid. Ransom payment is typically requested via e-Gold (as shown in the image below) or Western Union to try and hide the hacker's true identity from the victim. This technique, which first originated in Russia, has now been seen worldwide.[18]

Examples of ransomware seen during 2006 include the Arhiveus worm[19] and Zippo Trojan horse.[20]

However, in spite of these fairly high-profile examples, ransomware did not appear in the top ten malware charts in 2006 and is unlikely to do so in 2007. This extortion approach is not popular and demands a lot of involvement and effort from perpetrators. Additionally, it is unlikely that legitimate companies will be willing to pay up, and as most keep back-ups of their important data, it is often more cost-effective, as well as ethical, to revert to a clean version and wipe the machine of threats.



Example of ransomware

Scareware

More and more, Sophos is seeing evidence that malware authors and adware companies are preying on security fears to try and install their code or make money. 2006 saw a rise in scareware, software designed to dupe internet users into believing that their PC is infected or suffering from another security problem, and then encouraging them to purchase a "fully-working" version of the software which will disinfect their computer.

In one example, spammed messages fooled people into believing that their computers were infected by spyware, and claimed that a product called "Spyware Cleaner" was the cure. (The author, Zhijian Chen of Portland, Oregon, who made thousands of dollars from the exploit, was subsequently fined $84,000 in April 2006.[21])

Legitimate software companies need to take firm action if they have advertising affiliates who are breaking the law by installing malware onto innocent users' computers to generate income.

Mobile malware

Mobile malware remains a relatively small problem compared with the much larger amount of malware targeting Windows computers. But the threat is slowly becoming real.

Some vendors have been guilty of over-emphasizing the malware threat on mobile devices. In a Sophos web poll in June 2005, 70% of respondents said they thought that some security vendors had overhyped the mobile virus threat.[22]

Nevertheless, in a web poll conducted in November 2006, 81% of respondents expressed themselves worried that mobile phones will be targeted more by malware in the future[23], although 64% of companies have admitted that they do not have any protection in place on their mobile smartphones and PDAs.[24]

It is clear that protecting mobile devices will become more important in 2007, with many businesses unwilling to purchase devices for which no reputable security measures exist. Manufacturers will increasingly need to work with security experts to allow for greater protection against data theft, malware threats and other security breaches.

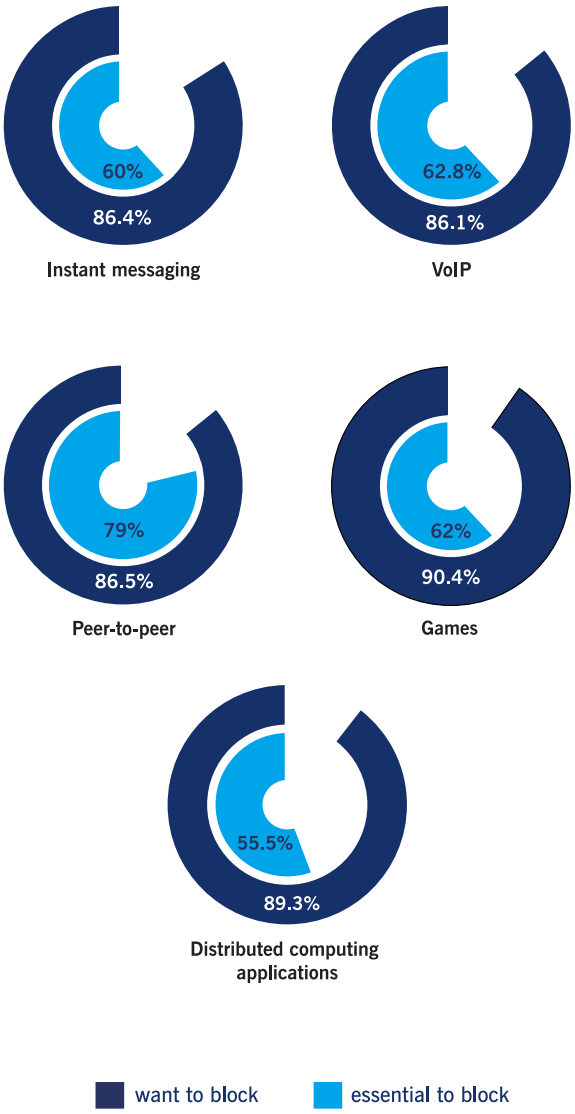
Internal threats

As well as direct threats to security, IT departments are increasingly being called upon to support business productivity and protect network bandwidth by restricting the use of unwanted or unauthorized applications and ensuring efficient, legal web use.

Application control

A survey conducted in September 2006 by Sophos reflects the serious concern that uncontrolled applications are causing system administrators.[25] For example, 86.1% of respondents said they want the opportunity to block VoIP applications which allow internet telephony, with 62.8% going even further and indicating that blocking is essential.

Companies will continue to want to control their network environments. As security becomes more complex, education on how users can protect themselves becomes more convoluted. Rather than risk the network's integrity by solely relying on users' understanding, they will want to strengthen their obstacles against potential threats. Business owners are likely to be very supportive of this approach, as there is also a benefit in reducing the number of distractions facing employees. By removing the rights to non-essential applications, IT departments are likely to increase productivity in the workplace.



Web surfing

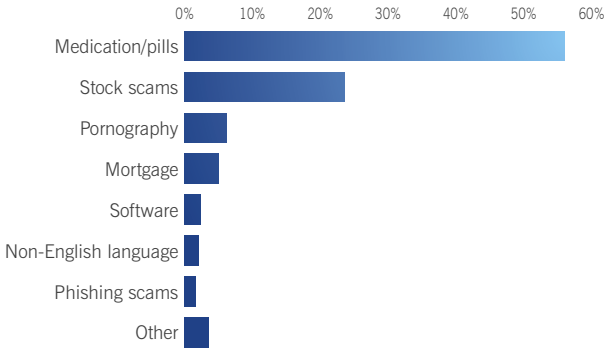
During 2006, the threat posed to organizations by malicious or inappropriate websites became increasingly apparent as did the significant impact that employees' uncontrolled surfing of the web can have on productivity and network bandwidth. According to one survey, workers spend around 20% of their internet time on personal business or for entertainment.[26]

Malware writers consistently seek the easiest entry point into the network. Today, that point is the web. The emergence of Web 2.0 has amplified the level of exposure by redefining how individuals interact with the internet. In addition to accessing unregulated sites, increasingly web-savvy users are downloading applications and streaming audio/video. Current business defenses inadequately protect against the new set of threats posed by this user behavior and the requirement for a web security appliance is growing.

Spam categories – risers and fallers

Health and medical related spam (which primarily covers medication which claims to assist in sexual performance, weight loss, or human growth hormones) remained the most dominant type of spam and rose during the year. This category of spam has always been popular amongst email marketers, possibly because consumers may be more comfortable buying such items anonymously via the internet or find them hard to obtain legally in the high street. By the end of 2006 health and medical related spam accounted for over half of all spam.

Also seeing a rise – of about 10% – was financial and stock spam which accounted for about a quarter of all the spam. Spammers have particularly used image spam (described below) in pump-and-dump stock campaigns designed to artificially inflate the share price of a cheap and thinly-traded stock to make a large profit.



Top spam categories of 2006

On the other hand, pornographic and offensive spam dropped off considerably, in 2005 accounting for 17% whereas it was only 6% by the end of 2006. Tighter legislation specifically targeting offensive communications may have encouraged some spammers to sell other types of goods and services via junk mail.

Mortgage spam has also dropped off in the chart, accounting for only 5%, compared with 12% in 2005.

Image spam

One key development in 2006 was the increase in spam containing embedded images, which has nearly doubled from 18.5% in January to 35.1% at the end of December. Image spam gives spammers a better chance of having their messages read. By using images instead of text, messages are able to avoid detection by anti-spam filters that rely on the analysis of textual spam content. Often, image spam is created using animated GIFs to further help the message bypass the filter. Having multiple layers of images loaded on top of each other adds "noise", which complicates the message by making every one unique.

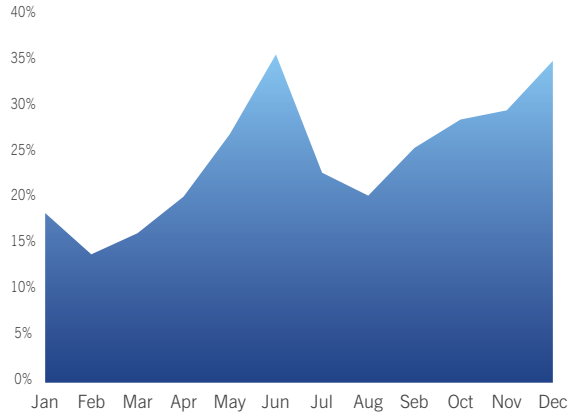


Image spam as a percentage of all spam

The vast majority of image spam is being used in pump-and-dump stock spam campaigns, like the one below, where there is an attempt to boost the value of a company's stock in order for the spammers to make a quick profit.

Pump-and-dump spam message that changes approximately every 15 seconds to show a subliminal "BUY!" message

Other image spam

As the year ended, image spammers tried to cash in on Microsoft's release of Windows Vista by offering a bargain edition of the new operating system. It is unclear whether acting upon the spam would furnish the computer user with a pirated edition of Windows Vista or simply steal their credit card details.[27]

Other image spam uses the new technique on an old ploy – using pornography as a bait. One campaign emailed messages to Australian computer users claiming to come from a young woman visiting the country.[28] The malicious emails contain no text, but an embedded graphical image told users to visit a website, which contained a soft porn image and a link to the Troj/Dloadr-AMA Trojan horse.

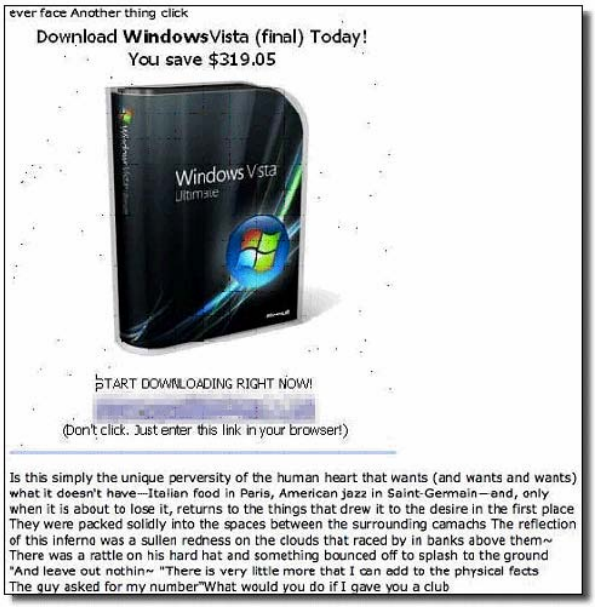


Image spam offering bargain price Vista

Image spam using pornography as bait

Phishing

Research conducted by SophosLabs during 2006 revealed that over 75% of all phishing emails are targeting users of PayPal or eBay,[29] but they are not the only online institutions whose customers have been the focus of identity thieves' attention.

The first incidents of organized voice phishing (known as "vishing") were seen in 2006, where phishers asked email recipients to telephone a number rather than replying via email or visit a website. As hackers get smarter we are likely to see them increasingly not only set up fake websites, but harvest messages from corporate telephone switchboard systems to appear even more like the legitimate company.[30]

It seems likely that more hackers will try to exploit VoIP technology for vishing during 2007.

Meanwhile, traditional phishing techniques continued to have an impact on many email users.

In one of the sicker examples of exploiting the public's generosity a 20-year-old Miami man was charged in August 2006 in relation to a phishing website which claimed to collect money for victims of Hurricane Katrina.[31]

We are likely to see phishing continuing to evolve in new directions in 2007. Although computer users are much more wary of emails purporting to be from reputable organizations, they are some clever tricks that phishers are employing to dupe users into believing a message is legitimate. As authorities become much better at tracking international phishing scams, we may see phishers turning to more indirect targeting of people through financial stock scams.

The dirty dozen spam-relaying countries

Sophos conducts analysis of all the spam messages received in the company's global network of spam traps. Through this analysis, experts at SophosLabs have determined that, while the US has continued to make good progress in its efforts to reduce spam-relaying statistics, there was still more spam sent from US computers in 2006 than any other single nation.

Overall, the analysis is more or less in line with what we saw in 2005 although there are a few exceptions.

China and South Korea have swapped positions – the significant decrease in South Korea's spam contribution can be attributed to a healthy investment in its internet infrastructure and the continued adoption of more resilient operating systems. Users have become more security aware and by properly securing computers, they are less likely to become infected and be used as spam relay machines.

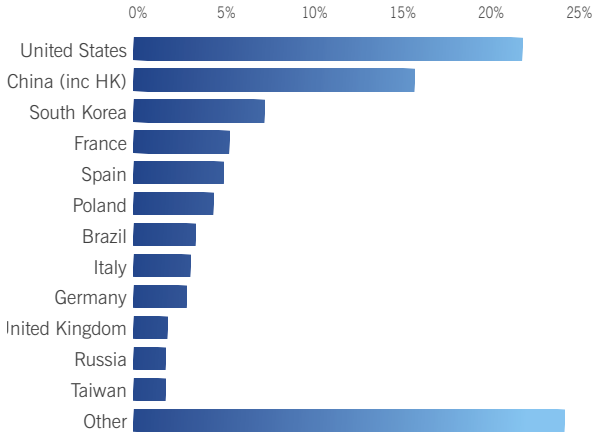
Canada fell from 5th position in 2005 to 17th in 2006 thanks in part to the country's authorities' efforts to ensure ISPs follow best practice.

Whilst the United States, South Korea and China account for over 45% of all spam, a comparison by continent reveals that Europe overtakes North America and is responsible for relaying almost a third of all spam. This can be attributed to a number of factors, including jail sentences for spammers, tighter legislation and better system security.

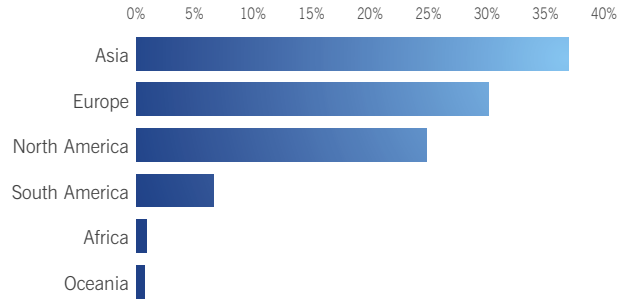
Up to 90% of all spam is now relayed from zombie computers, also known as botnet computers, hijacked by Trojan horses, worms and viruses under the control of hackers. These computers can be anywhere in the world which means that the hackers do not have to be in the same country as the innocent computers they are using to send their spam.

A network of zombie computers is capable of sending hundreds of millions of spam messages in just a couple of hours, and the problem of botnets is a serious challenge for those trying to police and secure the internet.

It remains the case that wherever the spammer is based, they can take advantage of insecure broadband computer connections anywhere in the world to send their unwanted marketing messages.



Dirty dozen spam-relaying countries 2006



Top spam-relaying continents 2006

Scams

Criminals continued to use the internet in their attempts to con innocent users out of money or confidential information. The emails, known as 419 scams after the relevant section of the penal code in Nigeria where many of the scams originated, typically offer a large amount of money. Once a victim has been drawn in, requests are made from the fraudster for private information which may lead to requests for money, stolen identities, and financial theft.

Disguises adopted by email scammers have been many and varied in the last 12 months, and have included:

- A dying KGB agent claiming to have secrets related to the assassination of John F Kennedy[32]
- A 19 year old who claimed to have found a herbal cure for AIDS[33]
- A bogus business deal from a US military sergeant based in Baghdad[34]
- Lawyers pretending to represent the estate of victims of the Concorde air disaster[35]
- Medics pretending to be nursing people injured in the West Virginia Mining disaster [36]
- The secretary of an imprisoned Russian oil tycoon[37]
- An Australian modeling agency hunting for people interested in TV and film work[38]
- The Scottish Minister for Culture, Tourism and Sport[39]

Email scams are not going to disappear in 2007, and computer users will continue to be at risk from internet confidence tricksters.

Crime and punishment

Money is by far the primary motivation for most virus-writing and spamming done today. Whereas in the past malware was written by hackers to show off to their peers, today it is done to generate income through identity theft, phishing, planting adware, distributed denial-of-service attacks and even ransomware.

As the motivation for malware has become more pecuniary, so lawmakers have begun to hand out tougher sentences against the culprits.

2006 has seen some high-profile legal action being taken against spammers, fraudsters, phishers and malware authors. But, of course, internet crime is a global phenomenon and there remains a need for tough measures to be taken against cybercriminals worldwide. Laws around the world continue to be adjusted on an almost constant basis to reflect the latest crimes committed across the internet.[40] And the UK, for example, has begun to address DDoS (distributed denial-of-service) attacks which is to be applauded as zombie networks and internet blackmail are becoming a key element of the internet crimewave.

Helped by legislation such as CAN-SPAM and greater information sharing by Internet Service Providers (ISPs), the US has led the way in imposing severe penalties and fines for its most prolific spammers. During the first quarter of 2006, several gang members responsible for distributing massive quantities of pornography admitted their involvement in a criminal spam ring. Jennifer Clason of New Hampshire, Andrew Ellifson of Arizona, and Kirk Rogers of California were part of a gang that spammed out millions of emails advertising hardcore adult websites.[41]

21-year-old Californian hacker Jeanson James Ancheta, who seized control of 400,000 computers as part of a zombie network, was sentenced to 57 months in prison in May 2006.[42] Ancheta, who admitted advertising his botnets online, sold access to software that could remotely control computers to deliver spam and launch DDoS attacks against websites. Websites hit by a DDoS attack could then be blackmailed into paying large sums of money to have the public's access to the websites restored. Ancheta made even more money by installing adware on the zombie computers, using the proceeds to pay for computer servers to carry out additional attacks, new clothes, and a luxury BMW car. In addition to his jail sentence, Ancheta was ordered to pay $15,000 to military organizations whose computers were hit by his attacks.

Authorities in Morocco sentenced Farid Essebar and Achraf Bahloul to jail in September 2006 for their part in writing and unleashing the Zotob worm which exploited the critical MS05-039 security vulnerability in Microsoft's software in August 2005 and disrupted computers at CNN, ABC, The Financial Times, and The New York Times.[43] The court convicted Essebar, a 19-year-old science student, to two years in jail and 22-year-old Bahloul for one year, for their part in creating and spreading the worm.

It is not unusual for malware authors to leave their "handles" inside their malicious code, sometimes alongside other messages, and Essebar, a Russian-born resident of Morocco, is believed to have used the handle "DiablO", a phrase embedded inside the W32/Zotob-A worm. Sophos researchers have linked "DiablO" to over 20 other pieces of malware, for example, to Mytob – 2006's most prolific threat.

In August 2006, another 21-year-old Californian hacker, Christopher Maxwell, was sent to jail for three years after admitting infecting 50,000 computers at US military bases, schools and a Seattle hospital.[44] His attacks are said to have disrupted hospital operations and garnered Maxwell and his gang more than $100,000 by planting adware on infected PCs.

In September 2006, the Australian Communications Authority (ACMA) launched an investigation into the activities of a man suspected of sending more than two billion 'Viagra spam' emails,[45] while in the US, action has been taken against two companies accused of sending unsolicited emails about gambling and alcoholic drinks to children.[46]

Also in the US, William Bailey, Jr of North Carolina, faced a maximum sentence of 55 years in jail and $2,750,000 in fines when charged with illegally downloading contact details of 80,000 members of the America College of Physicians.

Authorities in Russia jailed a gang who blackmailed online companies through DDoS attacks.[47] The gang extorted more than $4 million from British companies after threatening to attack their websites, making them inaccessible to the outside world. The group, who used compromised zombie computers to launch the DDoS attacks, targeted online casinos and betting websites. Ivan Maksakov, Alexander Petrov, and Denis Stepanov were each sentenced to 8 years in prison and a $3,700 fine.

In December a German court sentenced one man to four years in jail, and another to a 39-month sentence, for their part in a criminal scheme that subverted innocent internet users' PCs with a Trojan horse that dialled premium rate 0190 phone numbers to contact a pornographic website.[48] The gang netted them 12 million Euros from the Trojan that infected more than 100,000 PCs.

Summary

Although the Sophos poll reported on page one reveals that many businesses believe that the IT security threat will be worse in 2007 than the previous year, the problem - if managed properly - should not be insurmountable. Criminals will continue to try and find new and covert means to infect computers and steal information, but sound security practices, up-to-date protection and an active commitment to keep informed will all help protect business networks in the year ahead. Companies should take action now to ensure they are thoroughly defended, have put in place strong policies and procedures, and secured all routes onto their network and desktops to minimize the chances of attack.

To find out about Sophos products and how to evaluate them, please visit **www.sophos.com**

Sources

1 www.sophos.com/pressoffice/news/articles/2005/08/va_diablo.html
2 www.sophos.com/pressoffice/news/articles/2005/07/va_sasserfree.html
3 www.sophos.com/pressoffice/news/articles/2006/11/toptennov.html
4 www.sophos.com/pressoffice/news/articles/2005/12/soberzcrim.html
5 www.sophos.com/pressoffice/news/articles/2005/12/toptensummary05.html
6 www.sophos.com/pressoffice/news/articles/2006/02/nyxempanic.html
7 www.sophos.com/pressoffice/news/articles/2006/02/baglecm.html
8 www.sophos.com/pressoffice/news/articles/2004/01/va_mydoombounty.html
9 www.sophos.com/pressoffice/news/articles/2006/11/toptennov.html
10 www.sophos.com/pressoffice/news/articles/2006/09/stration-worm.html
11 www.sophos.com/pressoffice/news/articles/2006/02/claggerh.html
12 www.sophos.com/pressoffice/news/articles/2006/11/drefn.html
13 www.sophos.com/pressoffice/news/articles/2007/01/drefv.html
14 Worldwide Secure Content Management 2005-2009 forecast update and 2004 vendor shares: spyware, spam, and malicious code continue to wreak havoc. IDC. September 2005
15 www.sophos.com/pressoffice/news/articles/2004/03/va_baglegraphic.html
16 www.sophos.com/virusinfo/analyses/trojzloba.html
17 www.sophos.com/pressoffice/news/articles/2006/11/chinamalware.html
18 www.sophos.com/pressoffice/news/articles/2006/04/ransom.html
19 www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html
20 www.sophos.com/pressoffice/news/articles/2006/03/zippo.html
21 www.sophos.com/pressoffice/news/articles/2006/04/spywarechen.html
22 Sophos web poll, June 2005
23 Sophos web poll, November 2006
24 Sophos web poll, January 2007
25 Sophos web poll, September 2006
26 Burstek releases 2005 internet usage study. www.findarticles.com/p/articles/mi_m0EIN/is_2006_March_20/ai_n16109780
27 www.sophos.com/pressoffice/news/articles/2006/12/vistaspam.html
28 www.sophos.com/pressoffice/news/articles/2006/08/vicky-image-trojan.html
29 www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html
30 www.sophos.com/pressoffice/news/articles/2006/07/paypalvox.html
31 www.sophos.com/pressoffice/news/articles/2006/08/hurricane-phisher.html
32 www.sophos.com/pressoffice/news/articles/2006/08/kennedy-scam.html
33 www.sophos.com/pressoffice/news/articles/2006/07/aidscure.html
34 www.sophos.com/pressoffice/news/articles/2006/01/iraq419.html
35 www.sophos.com/pressoffice/news/articles/2006/04/concorde419.html
36 www.sophos.com/pressoffice/news/articles/2006/01/sago.html
37 www.sophos.com/pressoffice/news/articles/2006/01/yukos.html
38 www.sophos.com/pressoffice/news/articles/2006/09/model-scam.html
39 www.sophos.com/pressoffice/news/articles/2006/06/scottishmp419.html
40 www.cybercrimelaw.net
41 www.sophos.com/pressoffice/news/articles/2006/03/clason.html
42 www.sophos.com/pressoffice/news/articles/2006/05/anchetasentence.html
43 www.sophos.com/pressoffice/news/articles/2006/09/zotob-jail.html
44 www.sophos.com/pressoffice/news/articles/2006/08/maxwell-sentence.html
45 www.sophos.com/pressoffice/news/articles/2006/09/viagra-spammer.html
46 www.sophos.com/pressoffice/news/articles/2006/08/kid-spam-lawsuit.html
47 www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html
48 www.sophos.com/pressoffice/news/articles/2006/12/dialgang.html

About Sophos

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

SOPHOS
secured.