

# SOPHOS

Sophos Security Threat Management Report

2005





# Sophos Security Threat Management Report 2005

## The year in review

The last 12 months saw those responsible for securing an organization's network challenged in new and inventive ways.

The increasing complexity of demands being placed on IT systems – for mobility, flexibility, and interoperability between different hardware and software – has led to an explosive growth in the variety of communication routes exploited by threats.

Over the last year the numbers and different types of malware increased, techniques that hijack computers and turn them into zombies became a cornerstone of many attacks, and new threats became commonplace almost more quickly than the media could come up with terms to describe them (phishing, pharming, spear phishing). The distinction between different types of threat also became more blurred. Overall, there was an increasing emphasis on secrecy and stealth, and spyware has become one of the biggest threats that businesses now face.

## New threats and trends

A report published in November 2005 by Financial Insights, an IDC company, estimates that global financial institutions alone

lost \$400 million or more in 2004 due to phishing schemes.<sup>1</sup> The financially motivated collusion of virus writers, spammers and hackers for criminal gain has developed into an art form in the last year. In a continuously evolving threat environment, criminals have joined forces to produce campaigns that coordinate virus, spam, phishing, and spyware attacks, blurring the distinction between them.

The random vandalism of earlier generations has been replaced by more purposeful criminal activity in which multiple variants of the same threat are relentlessly created and rapidly distributed with the aim of slipping past traditional signature-based virus protection and existing spam rules.

Malware attacks have typically become more focused, aiming at a small number of victims compared to the mass-mailing worms of the past, in an attempt to avoid drawing unnecessary attention to 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.

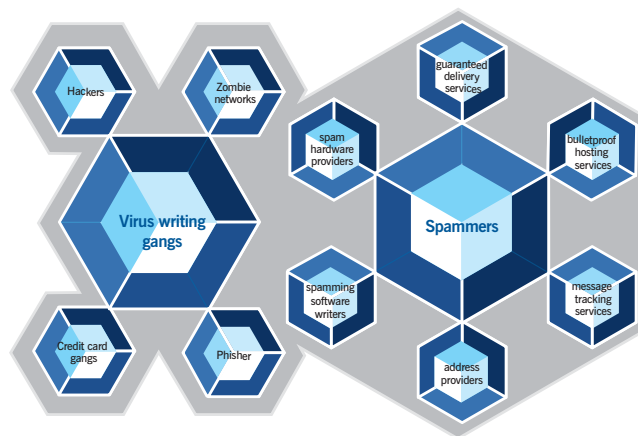


Figure 1: The threat ecosystem

## 2005 at a glance

- 48% increase in new malware threats over previous year
- 1 in 44 of all emails is viral
- New Trojans outweigh Windows worms almost 2:1
- Medical-related spam remains the most common, but pornographic content and pump-and-dump scams have surged
- Cybercriminals joining forces, and attacking using combined technology

### Growth rates

The number of new threats has continued to grow at rates once thought by some to be unsustainable. By December 2005, Sophos Anti-Virus was identifying and protecting against over 114,000 different viruses, worms, Trojan horses and other malware.

Over the period January – November 2005, the number of new virus, worm, Trojan horse and spyware threats rose by 48% as follows:

- 2004: 10,724 new threats
- 2005: 15,907 new threats

What is most significant is the month-by-month increase in the number of new malware threats discovered. In November 2005 alone, there were 1,940 new malware threats – the biggest monthly increase in threats protected against by Sophos products since records began. Figure 2 shows how this rate compares with last year.

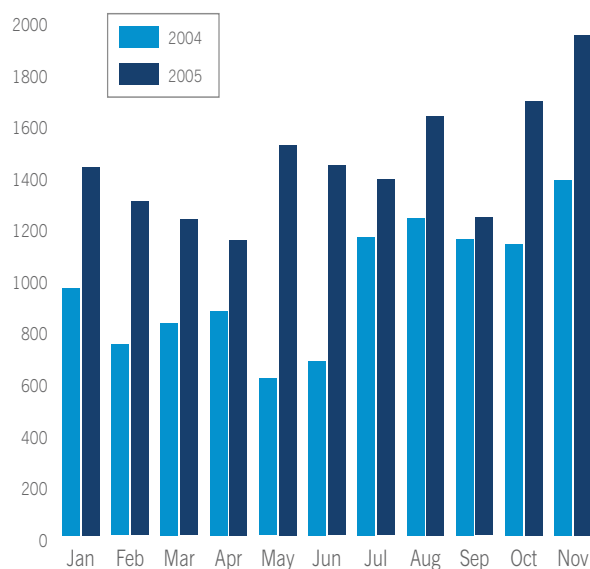


Figure 2: New malware threats - 2004 and 2005 compared

This increase can be attributed to the growing interest in authoring malware shown by criminal gangs. The financial incentive has driven them to write more viruses, worms and Trojan horses as they seek to steal and extort money from innocent computer users and companies.

Not only are the quantity and variety of threats on the rise, but also the speed with which new attacks emerge and spread has increased.

On average, throughout the year, 1 in 44 of all emails were virus infected. However, in times of a major outbreak (such as during the Sober-Z outbreak of late November 2005) this figure could rise to as high as 1 in 12 emails<sup>2</sup>. In this way, mass-mailing email worms can seriously disrupt internet communications as home users, companies and ISPs find they are flooded with unwanted, dangerous content.

In addition, malware authors have tried to make the lives of anti-virus researchers difficult by “blasting” out multiple new versions of their viruses and Trojan horses in a very short period of time<sup>3</sup>. By “packaging” their malicious code in different disguises, they aim to avoid detection by anti-virus vendors, quickly replacing older versions of the worm or Trojan horse with a new version as soon as they realize it is no longer capable of working effectively because defenses are in place.

As a result of these issues, more and more businesses are adopting pro-active defenses against the virus threat, blocking as much potentially dangerous content from entering their organization as possible even before anti-virus updates are available. Sophos has complemented this approach by introducing powerful Genotype™ technology which can determine that a new piece of malware is related to earlier members of the same virus family and preventing it from breaching a company’s defenses.

### 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.

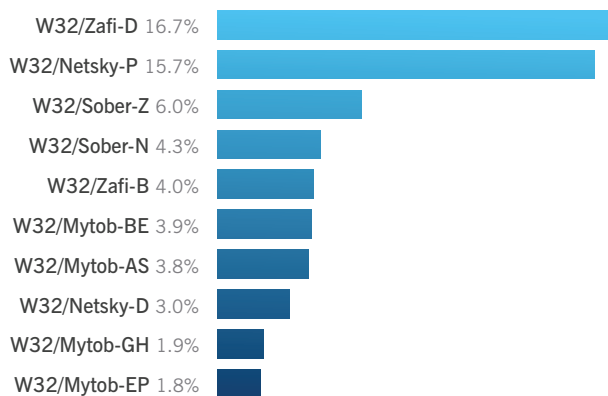


Figure 3: Top ten viruses reported to Sophos in 2005

Although hackers are increasingly using spam techniques to distribute Trojan horses, they are not having the same impact as worms and viruses which have the capability to propagate via email systems.

For many computer users and businesses, the malware in this chart is the most visible because it appears in their email inboxes or is blocked at their enterprise email gateways.

Interestingly, the top ten chart (seen in Figure 3) is dominated by viruses which have been around for a considerable time. This underlines that more recent attacks have been more insidious, subtly infecting smaller groups of people in an attempt to avoid drawing attention to themselves.

The long-standing Zafi-D worm accounts for more than 16.7% of all viruses reported to Sophos in the last 12 months. This Hungarian worm uses the guise of a Christmas greeting to trick users into opening its infected attachment<sup>4</sup>.

Another old-timer, Netsky-P, which was the hardest-hitting virus of 2004<sup>5</sup>, has enjoyed an extremely long reign near the top of the virus chart. German teenager Sven Jaschan, who admitted writing the Netsky and Sasser worms, walked free from court with 30 hours community service and a probationary sentence<sup>6</sup>. It is interesting to note that the author of the Sober worm is also believed to be based in Germany, and it could be speculated that Jaschan's sentence has not worked as a deterrent.

Given more time the Sober-Z worm would have dominated the chart, but its emergence in late November 2005 prevented it from taking pole position. The worm used a number of disguises, including posing as a message from an FBI or CIA investigator accusing the recipient of visiting illegal websites, in an attempt to get users to launch the malicious attachment.

The bilingual Sober-N worm first emerged in May. Posing as tickets to the 2006 World Cup in Germany, Sober-N compromised thousands of PCs in 40 countries<sup>7</sup>.

Sober-N waited silently in the background of infected PCs, before upgrading itself to a newer version in order to churn out German nationalistic spam from the compromised, zombie computers.

### *Trojan horses*

In every month during 2005, there were more Trojan horses being written than Windows worms. Indeed, Trojan horses account for nearly two-thirds of all malware analyzed by Sophos as shown in Figure 4.

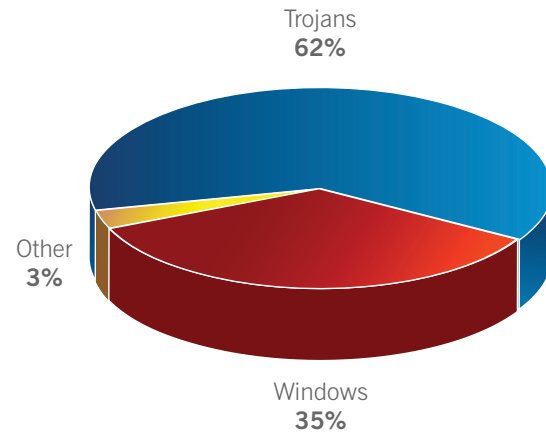


Figure 4: Types of new malware threats in 2005

This underlines 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.

Internet criminals may be turning their back on large scale attacks not only because they do not wish to draw attention to their efforts, but also because they cannot practically handle the amount of stolen data they might receive if they infected hundreds of thousands of computers in one day.

It is much simpler for the criminals to steal money from 200 bank accounts than 200,000, so they pace themselves in their attacks and use Trojan horses to ensure that they are stealing from a manageable group of people rather than the unknown and uncontrollable number of victims that a worm may bring them.

The distinguishing feature of a Trojan is that, unlike a virus or worm, it does not replicate on its own. So in order to spread it needs to be mass-spammed from other computers, which is one of the main uses made of zombies (the top threat characteristic of all malware reported to Sophos last year) as described below.

### Top threat characteristics

The last 12 months have seen cybercriminals looking for more and more cunning ways to infect computers and get what they want.

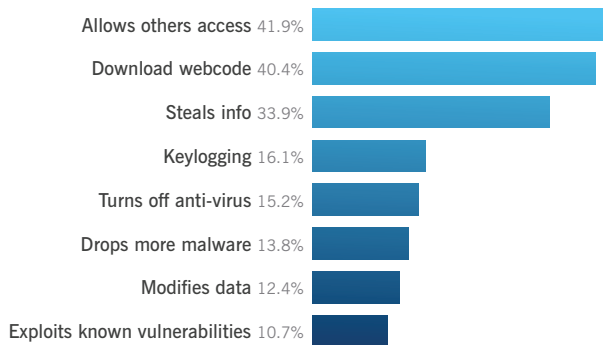


Figure 5: Top threat characteristics

As Figure 5 shows, this includes stealing information, turning off a computer's anti-virus software, and dropping malicious code which can then be used for a variety of tasks. Almost as big a threat as zombies are those threats which download webcode, highlighting the need for firewalls at the endpoint (desktops and laptops). The need for network-wide security is obvious as most malware incorporates more than one of the above characteristics.

### Zombies

A computer becomes a zombie when a bot, or automated program, is installed on it, giving a hacker access and control and making the computer part of a zombie network, or botnet. One of the most high profile botnets of the year was created by the Zotob worm which achieved worldwide notoriety in August when leading media organizations<sup>8</sup>, including ABC, The Financial Times and The New York Times, fell prey to it. CNN, another victim of the Zotob worm, was infected live on air, disrupting its TV schedule and making headline news.

Most of the top ten viruses reported to Sophos in January – November 2005 had the ability to allow third-party access to infected computers, i.e. to create zombies.

Sophos research has found that over 60% of all spam originates from hijacked computers, which are then used to commit a wide range of crimes, as well as launching DDoS attacks on web servers, using http, or on email servers, using SMTP. This real threat to business reputation led Sophos to launch its ZombieAlert™ Service in July 2005, which alerts businesses as soon as any of their computers starts sending out spam<sup>9</sup>.

A significant amount of malware also attempts to download malicious code from the web, highlighting the need for firewalls, not just at the network boundaries, but at the endpoint where they can help secure desktop and laptop computers.

### Spyware

The stand-out new threat is, of course, spyware. The growth in spyware – which sits secretly on computers, logging keystrokes, stealing information, and opening up networks to further attack – has presented businesses with new concerns about security issues. Installing itself onto a user's computer by stealth, subterfuge and/or social engineering, it sends information from that computer to a third party without the user's permission or knowledge.

Figure 6 shows the level of spyware threats reported to Sophos during 2005 as a percentage of the total malware analyzed by SophosLabs™, and how that proportion has increased. In January, only 54.2% of threats were spyware, but by November this had risen to 66.4%.

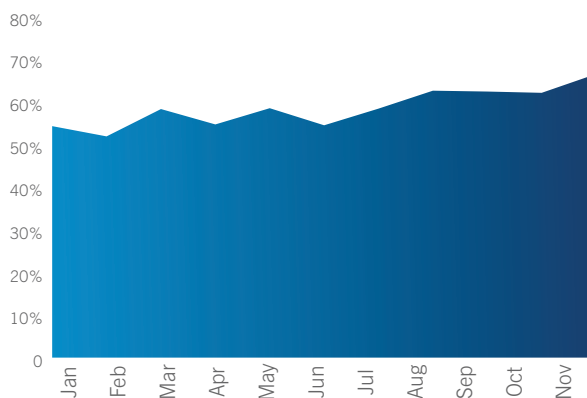
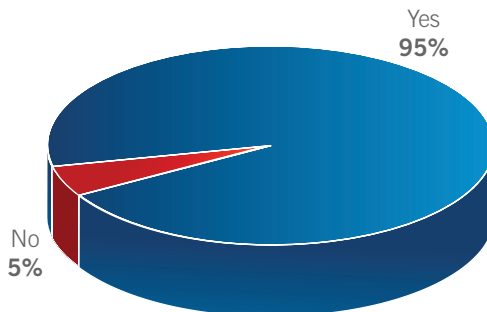


Figure 6: Spyware as a proportion of all new threats

Businesses are demonstrating a heightened awareness of the spyware problem with an overwhelming majority of those responding to a Sophos web poll<sup>10</sup> indicating that they expect their anti-virus software to provide simultaneous protection against spyware, as Figure 7 shows:



Source: Sophos web poll

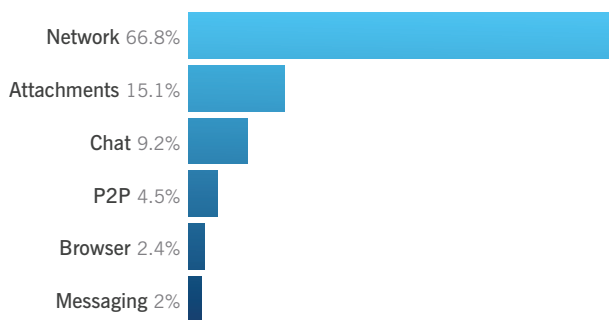
Figure 7: Respondents who say anti-virus software should also protect against spyware

During 2006, Sophos expects that vendors who provide only anti-spyware protection will find the market increasingly competitive, unless they can join forces with a security company which protects against viruses. The likelihood is that the market will consolidate, and some companies who can only protect against spyware will find it next to impossible to maintain their market share.

## Spreading methods

Malware uses a variety of methods to spread itself. It is quite usual today for viruses and worms to use a combination of different techniques to increase their chances of successful distribution and infection.

Figure 8 shows the different techniques used by malware, and what percentage of threats use them. The chart does not necessarily reflect the success of each method, merely that malware authors are building it into their code. It also does not include Trojans as they do not have any built-in spreading technology.



*Figure 8: Spreading methods*

Much emphasis continues to be placed on blocking threats at the email gateway. While this remains a key part of any protection strategy, it offers no defense against threats that use other communication routes.

Organizations are also vulnerable to a host of other threats which bypass the gateway altogether. Network-aware worms represent a real internal threat to organizations and today's malicious content is just as capable of entering an organization through web browsers, chat protocols and instant messaging (IM) applications like AIM and MSN Messenger.

In addition, controlling every CD, USB storage device, memory card, smartphone and MP3 player that comes near corporate computers, wherever they are, is almost impossible, yet these are all potential entry points for malicious content, and highlight the need to protect the desktop as well as other tiers in the IT infrastructure.

In November 2005, this point was brought home strongly when it was discovered that some music CDs from Sony were introducing, via their copy protection software, a vulnerability that was exploited by a number of Trojan horses<sup>11</sup>.

The variety of tactics used by hackers to spread their viral code makes the need for best practice more critical than ever before and highlights the importance of user education, security policies, systematic vulnerability patching, and a multi-tiered approach to virus defense.

## The motive

In the past, the motive of most virus writers was similar to those who daubed graffiti on subway walls. Virus writers, who were predominantly teenage or ethically immature, would write malware to boost their self esteem or impress their peers. Some virus writers even left messages and other clues in their code which could act as a useful lead to investigators.

Such viruses were not harmless (they still used up system resources and caused problems for businesses and home users) but they lacked a clear purpose.

Today, more and more malware is found to be written with the ultimate motivation of making money. Organized criminals are recognizing how the internet can be used in a variety of ways to steal from others.

Ways in which money can be made include phishing, spam, denial-of-service blackmail threats, scams, spyware, and pharming.

In addition, side industries have sprouted up in the threat ecosystem so, for example, there will be some who make money by selling software that helps spammers coordinate zombie computers to launch their campaigns.

There have also been alleged cases of legitimate adware affiliates abusing guidelines set down by the adware companies and illegally installing adware onto thousands of innocent compromised computers, in order to make a slice of money from every click.

We have even seen a growth in the number of worms and Trojan horses that steal credentials from players of Massively Multiplayer Online Role Playing Games (MMORPGs) in a bid to steal and sell virtual items which can make a real world profit. Even though the items do not exist, they can be sold, and such cases have resulted in some arrests<sup>12</sup>.

This move into the theft of virtual goods is hardly surprising when you consider the sums of money changing hands for virtual items in these virtual worlds. For instance, a man in Miami recently spent \$100,000 buying a virtual space station<sup>13</sup>.

However, most of the criminal activity remains in the area of spyware, phishing and internet fraud. Internet criminals are joining forces, sharing expertise, and working closely together in an attempt to make money from innocent computer users.

### Spammers

Medical-related spam (which primarily covers medication which claims to assist in sexual performance, weight loss, or human growth hormones) remains the most dominant type of spam seen. Spam campaigns were seen during the year which exploited concerns about avian flu by marketing drugs online which claimed to be able to protect people<sup>14</sup>. This spam category has remained steady throughout the year and has shown no significant growth, as Figure 9 shows.

Spam containing adult content surged from August 2005 onwards, although part of this climb reflects improved classification of this spam category by Sophos's monitoring stations in the last third of the year. Adult and sexual spam has long stood in second place to medication in the roll call of most prevalent type of spam.

One category of spam which saw considerable growth was stock-related spam, which by November 2005 stood at 13.5% of all spam from a year-start low of 0.8%.

Examples of "pump-and-dump" stock scams seen spammed in the last year include emails claiming that firms have developed effective medication against avian flu<sup>15</sup>.

Meanwhile, the categories of products and software have seen a significant drop-off. Less and less legitimate products are being advertised by spammers. There was a rise, however, in the amount of spam related to Rolex watches during the year, although it is impossible to know if these were legitimate goods or fakes.

### Phishing

One of the most lucrative forms of spamming, and an increasingly common form of online theft, is phishing. Sophos sees more phishing emails related to PayPal than any other organization, followed by eBay and Amazon. But well-known financial institutions also regularly appear.

Only a few recipients need to be lured into clicking on a link to a forged website for the scam to be profitable.

Some phishing scams are particularly devious. For instance, in August 2005 phishers pretended to be a wheelchair-bound elderly lady hunting for an item on eBay, in an attempt to steal from good samaritans<sup>16</sup>.

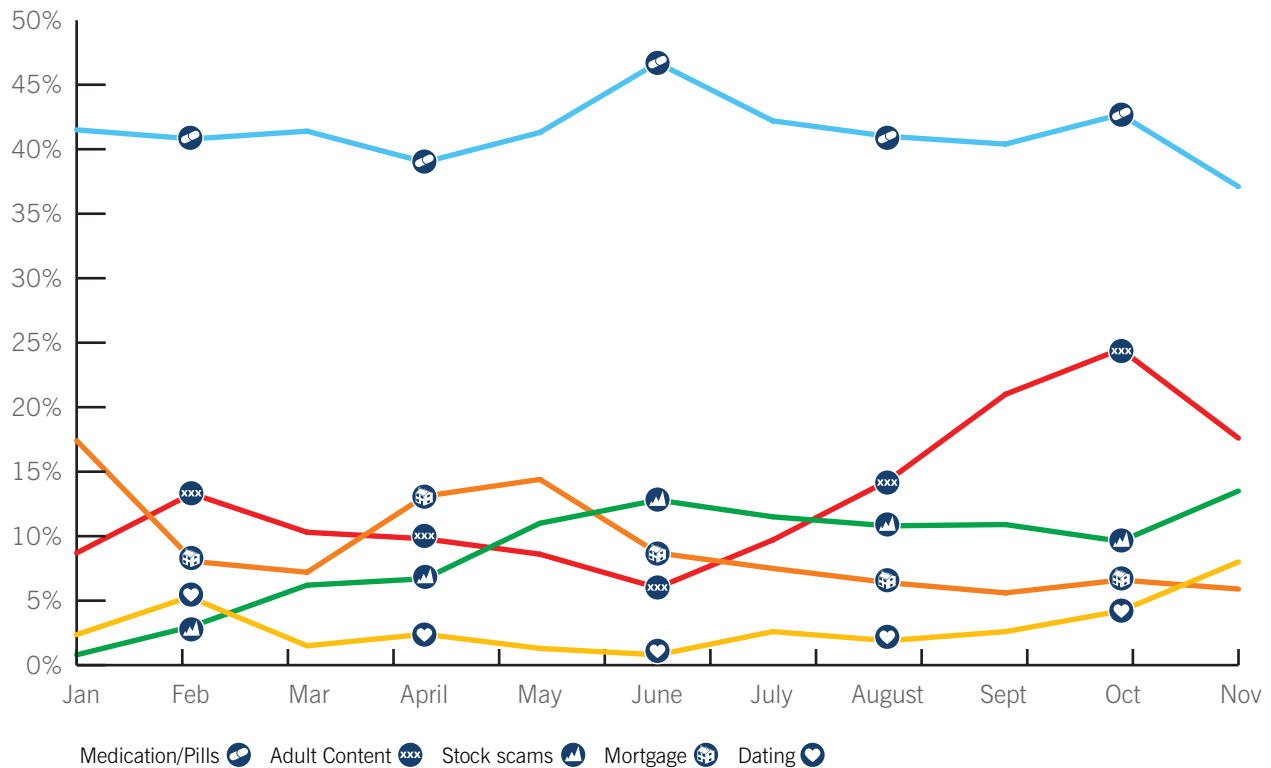


Figure 9: Spam categories

The latest development in this area is “spear phishing”. This is where a phishing campaign is deliberately focused on a small number of users, for instance the employees of a particular company, with the aim of gaining unauthorized access to confidential data. By using social engineering tactics, and forging the email address used in the spear phish to appear to come from someone that the recipient knows, the opportunities for the crime successfully being committed are increased.

### Scams

419 scams (also known as Advanced Fee Fraud, or Letters from Nigeria) are well known, and continue to spread amongst regular spam. During the last 12 months Sophos has intercepted a wide variety of email scams, spammed out to large numbers of people. These have included emails claiming to come from victims of the Indian Ocean tsunami disaster<sup>17</sup>, supposed relatives of a man killed at the July 2005 London terrorist bombings<sup>18</sup>, and even a bogus Liverpool Football Club lottery<sup>19</sup>.

### The “dirty dozen” spam relaying countries

Figure 10 reveals the country of origin of those computers sending spam. The United States remains the worst offender, but is relaying substantially less of the world’s spam than it did during 2004<sup>20</sup>. Sophos has determined that over 60% of all spam is now generated from zombie computers – hijacked PCs infected by malware.

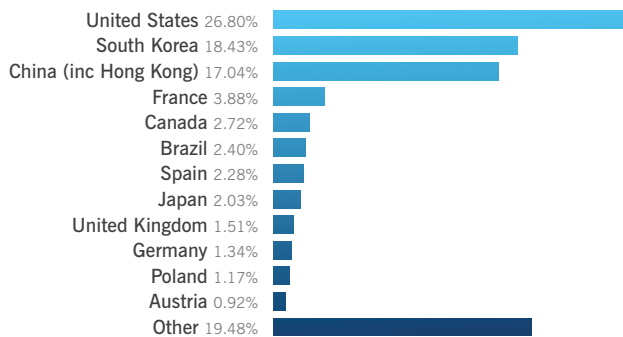


Figure 10: “Dirty dozen” countries

This technique means that the culprits do not have to be in the same country as the innocent computers they are using to send their spam. Whilst the United States, South Korea and China still account for over 50% of all spam, the USA and Canada have done well to reduce their contribution to the problem. Sophos has seen a sharp drop in the percentage of spam sent from North American computers due to a number of factors, including jail sentences for spammers, tighter legislation and better system security.

## 2006 and beyond

### Spyware and adware

Spyware looks set to rise in 2006 and we are now seeing hackers beginning to use zombies to install adware and potentially unwanted software across the network. While adware is not necessarily always illegal, the legal status is being subverted and exploited to create revenue streams<sup>21</sup>. As the threat from spyware and adware continues to grow, 2006 is likely to see businesses looking for integrated, centrally controllable solutions rather than home-user software.

### No end in sight for spam

On January 24 2004, Bill Gates predicted that spam would be “a thing of the past” within two years<sup>22</sup>. However, as January 24 2006 approaches Sophos believes that the rumors of spam’s death have been greatly exaggerated. The threat remains alive and kicking despite the increased action against spammers and constantly improving anti-spam software.

### Host Intrusion Prevention Systems (HIPS)

HIPS covers a wide array of security approaches including behavioral containment and application inspection along with traditional approaches such as virus protection and a personal firewall. Sophos believes that customers should consider carefully what mix of protection they need to defend their enterprises, rather than pick a product because it purports to solve all security needs.

### Mobile viruses

Although there has been an increase in the number of mobile phone viruses being written, they remain insignificant<sup>23</sup> compared to the much larger number of viruses which target Windows desktop computers. Virus authors, hell bent on stealing money and resources from internet users, find attacking Windows computers easy and profitable.

In a Sophos web poll, 70% of enterprises said they believed some anti-virus vendors were overhyping the mobile phone virus threat.

## *Microsoft*

Microsoft's venture into producing anti-virus software for consumers is likely to be a thorn in the side of those security vendors who protect home users. Microsoft will, however, face considerable challenges in presenting itself as a credible security vendor for enterprises. A Sophos poll conducted after the high profile Zotob worm outbreak found that 35% of respondents felt Microsoft was to blame as the worm exploited a critical security vulnerability in the Windows code<sup>24</sup>.

Furthermore, it is likely that a large number of future viruses will be designed to specifically subvert Microsoft's anti-virus product, just as their anti-spyware and firewall products have been targeted<sup>25</sup>.

## *Malware authors*

Virus writers will continue to use more methods to make money from their malware – whether it be stealing confidential information, using exploited computers as spam factories<sup>26</sup> or for DDoS attacks<sup>27</sup>, or planting adware on infected PCs. Increasingly, we expect to see fewer traditional email worms making an impact, and an increase in the use of Trojan horses in targeted attacks against specific victims<sup>28</sup>.

## *Vulnerability exploitation*

Although Microsoft will continue to have its vulnerabilities exploited by malware authors, we will see an increase in attacks taking advantage of security holes in other products (for instance, desktop tools, alternative web browsers, email gateway software, etc) which are widely used.

## *Zombies*

As more and more home users switch to Windows XP SP2 and benefit from its improved security (basic firewall, automatic downloading of security patches), hackers will no longer be able to rely solely on internet worms blasting their way onto computers to compromise them. Instead, they will use social engineering to enter the computer and turn off the protection from within, allowing a zombie component to be downloaded.

Efforts, such as ISPs sharing knowledge on how to crack down on spammers and authorities enforcing the CAN-SPAM legislation, have helped North America tackle the spammers based on their doorsteps. Some of the most prolific spammers have been forced to either quit the business or relocate overseas as a result.

The introduction of Windows XP SP2 a year ago, with its improved security, has also helped to defend home users from computer hijacking.

It is becoming apparent that Boca Raton, Florida, can no longer be considered the spam capital of the world, and that Russia is now the natural home for many of the spammers. Unfortunately, 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.

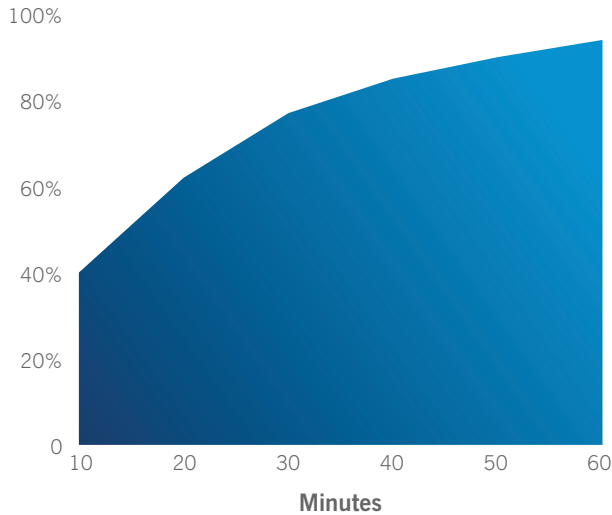
## **Need for protection**

Insufficiently protected computers are coming under attack in shorter timescales than ever before. Exploits, taking advantage of software flaws, can spread without human intervention. Internet worms like Zotob make use of vulnerabilities in the Windows operating system, infecting potentially hundreds of thousands of computers worldwide. 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.

Microsoft issued 29 critical patches between January and November 2005 – an average of 2.4 critical patches each month – as well as numerous other important patches that are vital to security.

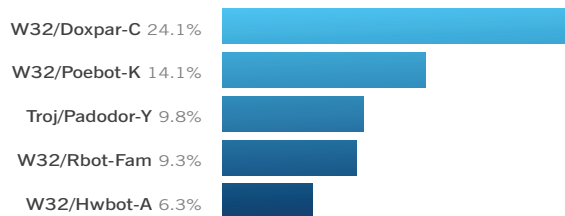
Sophos research shows that connecting an unprotected, unpatched computer running Windows XP (without SP2) to the internet leads to a 40% risk of infection from an internet worm within about 10 minutes, rising to a 94% chance after 60 minutes (see figure 11). There may not even be enough time to download and install security patches or firewalls, so computers must be protected before going online.

The good news is that a properly patched and protected Windows XP SP2 installation provides a much stronger defense against internet worms, dramatically reducing the opportunity for an internet worm to blast through onto a PC. However, more and more malware is being written which, if it reaches the user's desktop via a web download or email attachment, will instantly disable the security of Windows XP SP2 to allow in external threats.



*Figure 11: Risk of infection from an internet worm if computer is unprotected*

The top five internet-borne threats which are causing these infections are shown in figure 12.



*Figure 12: Top internet-borne threats*

The danger posed by internet worms is that they require no user interaction. Computer users do not have to visit any websites or open any emails to be infected. Simply plugging an unprotected computer into the internet is enough to put the PC at risk.

Infection is invariably silent and invisible, the user having no idea that their computer has been compromised and that they may be passing infections onto other net users, being spied upon, or sending out spam on the hacker's behalf.

## 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 in 2006. The combination of spreading methods and the multi-level nature of many threats means that organizations will look increasingly to single vendors with cross-threat expertise and consolidated product solutions to protect their systems, their data and their business continuity.

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.

SOPHOS INC North America Toll free 1 866 866 2802 Email [nasales@sophos.com](mailto:nasales@sophos.com)

**SOPHOS**  
WWW.SOPHOS.COM

## References

- 1 IDC - Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc, Nov 2005
  - 2 Sober-Z worm poses as bogus email 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)
  - 3 Genotype technology defends against Mytob mass attack, Sophos reports on multitude of worms  
[www.sophos.com/pressoffice/news/articles/2005/04/va\\_mytobmultitude.html](http://www.sophos.com/pressoffice/news/articles/2005/04/va_mytobmultitude.html)
  - 4 Latest Zafi worm spreading in the wild as email Christmas greeting  
[www.sophos.com/pressoffice/news/articles/2004/12/va\\_zafid.html](http://www.sophos.com/pressoffice/news/articles/2004/12/va_zafid.html)
  - 5 War of the worms: Netsky-P tops list of year's worst virus outbreaks  
[www.sophos.com/pressoffice/news/articles/2004/12/pr\\_uk\\_20041208yeartopten.html](http://www.sophos.com/pressoffice/news/articles/2004/12/pr_uk_20041208yeartopten.html)
  - 6 Sasser worm writer walks free from court, Sophos comments on conviction of Sven Jaschan  
[www.sophos.com/pressoffice/news/articles/2005/07/va\\_sasserfree.html](http://www.sophos.com/pressoffice/news/articles/2005/07/va_sasserfree.html)
  - 7 Sober-N worm seen in over 40 countries, shows no sign of disappearing  
[www.sophos.com/pressoffice/news/articles/2005/05/va\\_sobern2.html](http://www.sophos.com/pressoffice/news/articles/2005/05/va_sobern2.html)
  - 8 Breaking news: worm attacks CNN, ABC, The Financial Times, and The New York Times  
[www.sophos.com/pressoffice/news/articles/2005/08/va\\_breakingnews.html](http://www.sophos.com/pressoffice/news/articles/2005/08/va_breakingnews.html)
  - 9 Sophos ZombieAlert Service identifies spammer-controlled computers on business networks  
[www.sophos.com/pressoffice/news/articles/2005/07/pr\\_uk\\_20050713zombiealert.html](http://www.sophos.com/pressoffice/news/articles/2005/07/pr_uk_20050713zombiealert.html)
  - 10 95% say anti-virus software should also stop spyware  
[www.sophos.com/pressoffice/news/articles/2005/07/va\\_pollspyav.html](http://www.sophos.com/pressoffice/news/articles/2005/07/va_pollspyav.html)
  - 11 Trojan horse exploits Sony DRM copy protection vulnerability  
[www.sophos.com/pressoffice/news/articles/2005/11/stinx.html](http://www.sophos.com/pressoffice/news/articles/2005/11/stinx.html)
  - 12 Suspected gang who stole from online game players arrested in Korea  
[www.sophos.com/pressoffice/news/articles/2005/07/va\\_krarrests.html](http://www.sophos.com/pressoffice/news/articles/2005/07/va_krarrests.html)  
Trojan steals usernames and passwords for fantasy role-playing game  
[www.sophos.com/pressoffice/news/articles/2005/01/va\\_legmiry.html](http://www.sophos.com/pressoffice/news/articles/2005/01/va_legmiry.html)
  - 13 Man spends \$100,000 on virtual space station in online game  
[www.informationweek.com/story/showArticle.jhtml?articleID=173601281](http://www.informationweek.com/story/showArticle.jhtml?articleID=173601281)
  - 14 Sophos issues health warning after spammers peddle drugs to combat bird flu  
[www.sophos.com/pressoffice/news/articles/2005/10/sa\\_tamifluspam.html](http://www.sophos.com/pressoffice/news/articles/2005/10/sa_tamifluspam.html)
  - 15 Spammers sell drugs and pump stocks on back of bird flu fears  
[www.sophos.com/pressoffice/news/articles/2005/10/sa\\_tamifluspam.html](http://www.sophos.com/pressoffice/news/articles/2005/10/sa_tamifluspam.html)
  - 16 Phishers use wheelchair-bound old lady to target eBay Good Samaritans  
[www.sophos.com/pressoffice/news/articles/2005/08/sa\\_samaritan.html](http://www.sophos.com/pressoffice/news/articles/2005/08/sa_samaritan.html)
  - 17 Sophos hoax description: Letter from tsunami victim  
[www.sophos.com/virusinfo/hoaxes/tsunami.html](http://www.sophos.com/virusinfo/hoaxes/tsunami.html)
  - 18 Sick 419 scammers use name of London bombing victim in attempt to steal money  
[www.sophos.com/pressoffice/news/articles/2005/08/sa\\_419bombscam.html](http://www.sophos.com/pressoffice/news/articles/2005/08/sa_419bombscam.html)
  - 19 Bogus Liverpool Football Club emails aim to steal money from the unwary  
[www.sophos.com/pressoffice/news/articles/2005/11/liverpoolfc.html](http://www.sophos.com/pressoffice/news/articles/2005/11/liverpoolfc.html)
  - 20 The "Dirty Dozen" 2004: Sophos reveals the top spamming countries  
[www.sophos.com/pressoffice/news/articles/2004/12/sa\\_dirtydozenyear.html](http://www.sophos.com/pressoffice/news/articles/2004/12/sa_dirtydozenyear.html)
-

- 
- 21 FBI arrests 20-year-old suspected zombie king  
[www.sophos.com/pressoffice/news/articles/2005/11/ancheta.html](http://www.sophos.com/pressoffice/news/articles/2005/11/ancheta.html)
  - 22 Gates forecasts victory over spam  
[news.bbc.co.uk/1/hi/business/3426367.stm](http://news.bbc.co.uk/1/hi/business/3426367.stm)
  - 23 Customers unlikely to encounter Mibir mobile phone worm  
[www.sophos.com/pressoffice/news/articles/2005/04/va\\_mibir.html](http://www.sophos.com/pressoffice/news/articles/2005/04/va_mibir.html)
  - 24 PC users point the finger at Microsoft over latest virus outbreak  
[www.sophos.com/pressoffice/news/articles/2005/08/va\\_zotobpoll.html](http://www.sophos.com/pressoffice/news/articles/2005/08/va_zotobpoll.html)
  - 25 First Trojan to attack Microsoft anti-spyware product discovered  
[www.sophos.com/pressoffice/news/articles/2005/02/va\\_bankash.html](http://www.sophos.com/pressoffice/news/articles/2005/02/va_bankash.html)
  - 26 Spammer Sober-Q Trojan horse stopped proactively by Sophos Genotype technology  
[www.sophos.com/pressoffice/news/articles/2005/05/va\\_soberq.html](http://www.sophos.com/pressoffice/news/articles/2005/05/va_soberq.html)
  - 27 Suspected zombie kings who ran botnet of 100,000 PCs arrested  
[www.sophos.com/pressoffice/news/articles/2005/10/va\\_dutchbotarrests.html](http://www.sophos.com/pressoffice/news/articles/2005/10/va_dutchbotarrests.html)
  - 28 Critical infrastructure organisations targeted by hackers  
[www.sophos.com/pressoffice/news/articles/2005/06/va\\_niscc.html](http://www.sophos.com/pressoffice/news/articles/2005/06/va_niscc.html)
-