Security threat report

2008

SOPHOS

secured.

© Copyright 2008. Sophos Plc.

All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

SOPHOS

Security threat report: **2008**

Overview

The world of malware fundamentally changed in 2007, as hackers fully embraced the web as their primary route for infecting computers. As more computer users have defended their email gateways with security solutions, cybercriminals are planting malicious code on innocent websites, lying in wait for victims to come to them and be silently infected.

Whereas virus writers of ten years ago were typically creating code for mischief, today's attacks are organized, commercial endeavors designed to steal information and resources from the computers of victims for one reason above any other: to make money. The scale of their global criminal operations have reached such a height that Sophos discovers a new infected webpage every 14 seconds – 24 hours a day, 365 days a year.

It has also become clear that malware is more than a Microsoft problem. Although the number of Windows threats overshadows attacks against any other platform, financially-motivated cybercriminals are turning their attention to alternative platforms such as Apple Macintosh and web servers running Apache. This trend seems likely to continue in 2008, and we may see the emergence of new threats against portable Wi-Fi enabled devices such as the iPhone, iPod Touch and ultra-mobile PCs.

It remains paramount for businesses to defend themselves at all levels of their organization - not only do they need to secure their email and web gateways, but also to ensure that networks and endpoints are comprehensively protected in 2008 against the myriad of threats posed by the criminal underground.

2007 at a glance

Hackers use the web to infect users – malicious code increasingly embedded on high-traffic websites or adverts

Web threats – one new infected webpage discovered by Sophos every 14 seconds, or 6,000 a day

Cybercrime reaches Apple – Mac users being targeted by financially motivated hackers for the first time, proving malware is not just a Windows problem

Threats to mobile and Wi-Fi users – iPhones, iPod Touches, ultra-mobile PCs and others at greater risk of attack and may encourage exploitation of browser vulnerabilities

Information theft soars – scammers using stolen data to craft targeted emails

State-sponsored cyberwarfare cited – but no evidence of the danger made public

Pessimism reigns – public not confident that IT security will improve in 2008 following headline-making incidents

International authorities stepping up to the mark – law-enforcement around the world at last seeing punishment fit the crime

Web threats

Web threats in 2007

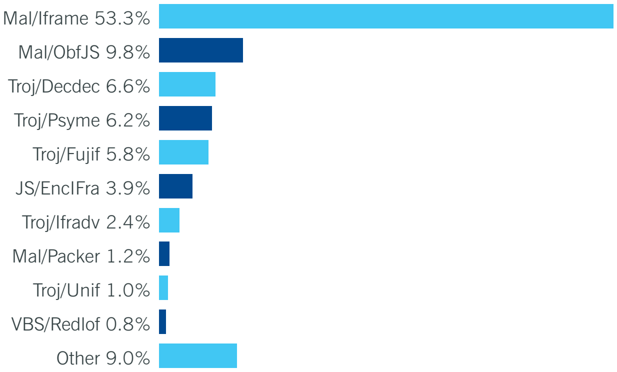
Web threats continue to be cybercriminals' preferred approach for delivering malware. Sophos currently sees 6,000 new infected webpages each day – one infected page every 14 seconds. Only about 1 in 5 of these sites is a hacker site, i.e. malicious in intent; 83 percent are hacked sites, or legitimate websites that have been compromised by an unauthorized third-party.

Surfers are often lured to these compromised webpages via emails which use social engineering tactics to attract unsuspecting users[1]. In other examples, hackers place their malicious code on sites which they know have a high number of visitors. Once the site is infected, unwary visitors without web security, firewall or patches on their PCs, can themselves be infected.

The content of these sites varies dramatically. Just some examples of the wide variety of sites that SophosLabs has seen hacked to host malware in a typical month are:

- Art galleries
- Christian ministry
- Computer network cabling
- Escort agencies
- Holiday property rental
- Ice-cream making
- Landscape gardening
- Museums
- Organic produce
- Oven cleaning
- Pilates
- Poker event organization
- Political activism
- Printing and graphics
- Tyre supply
- Web design.

Because of the range of subjects that hacked sites cover, blocking sites by content is not sufficient to protect users against these threats. A security solution to protect innocent computer users can help block web access to sites hosting malware.

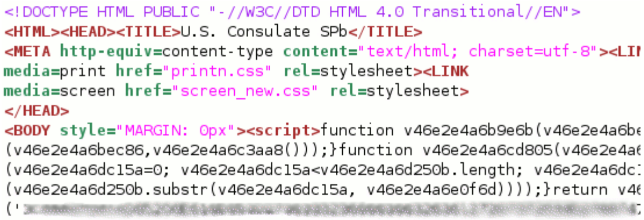


Top ten malware found on the web in 2007

Accounting for over half of all web-based threats in January to December 2007, was Mal/Iframe, which has dominated the charts from April. Particularly rampant in China, although also seen affecting websites hosted elsewhere, a growing number of web-based attacks look for vulnerabilities on legitimate hosted websites and injecting malicious code onto the site.

In June 2007, Mal/Iframe was found to have infected more than 10,000 legitimate Italian websites, including sites belonging to high-profile organizations like city councils, employment services and tourism sites. Most of the affected pages appeared to be hosted by one of the largest ISPs in Italy[2].

Mal/ObfJS, an obfuscated malicious script, has also affected many legitimate websites, for example the US Consulate General's in St Petersburg, Russia in October[3] (despite the fact that protection had been available in anti-virus products since May 2007).

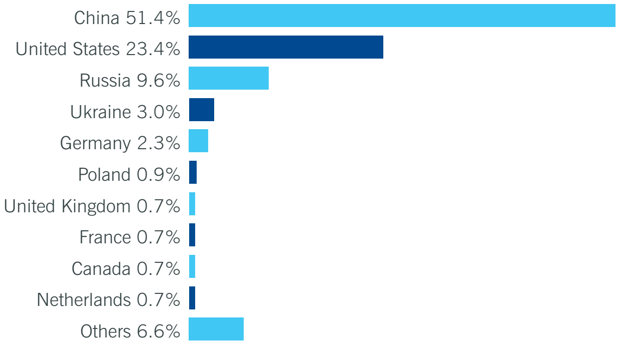


```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD><TITLE>U.S. Consulate SPb</TITLE>
<META http-equiv=content-type content="text/html; charset=utf-8"><LI
media=print href="printn.css" rel=stylesheet><LINK
media=screen href="screen_new.css" rel=stylesheet>
</HEAD>
<BODY style="MARGIN: 0px"><script>function v46e2e4a6b9e6b(v46e2e4a6be
(v46e2e4a6bec86,v46e2e4a6c3aa8()));}function v46e2e4a6cd805(v46e2e4a
(v46e2e4a6dc15a=0; v46e2e4a6dc15a<v46e2e4a6d250b.length; v46e2e4a6dc
(v46e2e4a6d250b.substr(v46e2e4a6dc15a, v46e2e4a6e0f6d))));}return v4
('
```

The US Consulate General removed the malicious code quickly and efficiently, but the fact that such a knowledgeable and security-conscious organization could become infected highlights the seriousness of the web threat.

Where is malware hosted?

The results of research into which countries contain the most malware-hosting websites reveal some significant changes over last year's top ten list.



Top ten malware hosting countries in 2007

China has moved from second place in 2006, when it accounted for just over 30 percent of infected websites, and now dominates the chart, with more than 50 percent of infected websites. Unfortunately whether a website is based in China is not necessarily obvious from its domain name, and so just avoiding websites ending in .cn will not significantly reduce your chances of being attacked by a China-hosted website.

The US has dropped from the top position, where it accounted for 34 percent of malware-infected websites in 2006, and accounts for less than a quarter this past year.

Poland is a new addition to this list, with 1 in 100 malicious webpages being hosted there. The Netherlands, which held fourth position in 2006, has managed to drop to tenth place, but still accounts for unusually large number of malicious sites, given its population and infrastructure. Sophos worked with computer crime authorities in The Netherlands last year to help them identify websites hosting malware so that they could be dealt with.

Making your web server more secure

- Don't install any unnecessary components on the server – more code means more vulnerabilities for hackers to exploit
- Sign up to your operating system security notifications
- Patch all operating systems and any applications with official security fixes
- Run up-to-date anti-virus software on the web server, regardless of what operating system you are using.

IIS users

- Do not enable directory browsing unless you really need it –why show visitors (malicious or legitimate) all the files on your system?
- Disable any FrontPage server extensions that are not being used.

Apache users

- Deny "all resources" by default and only allow the necessary functionality to each specific resource
- Log all web requests to allow you to spot suspicious activity.

Writing safer code

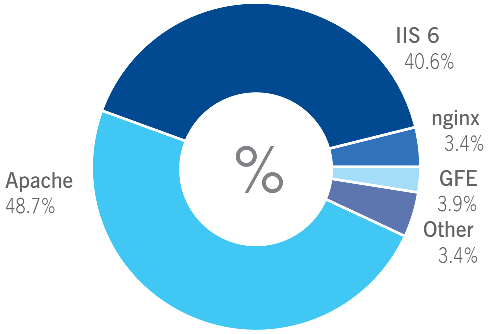
- Always initialize global variables (avoiding the danger of them being initialized by a fake GET or POST request)
- Turn off error reporting and log to file instead (making it more difficult for hackers to get the information they need)
- Never trust any user input or output, so use filter functions to strip out special SQL characters and escape sequences.

For further advice on securing your web server read the SophosLabs technical paper *Securing Websites*[4].

What web servers are being infected?

At the end of 2007, SophosLabs looked at a snapshot of the millions of web servers infected worldwide, closely examining over 50,000 to see what operating system they were running. The findings are in line with research done by Sophos in the first half of 2007, with almost 50 percent of the malware found on servers running Apache, and about 40 percent running Microsoft IIS.

As evidenced in other areas, malware affecting web servers is not just a Windows problem. A large number of Apache servers are hosted on Linux or some flavor of UNIX, and many administrators consider these systems to be much less vulnerable to attacks. While it is true that there is less malware written to target Linux and UNIX, the websites are not necessarily safe from attack. This is because the attacks target the website – not just the server – and often attempt to embed secret scripts or redirection malicious code.



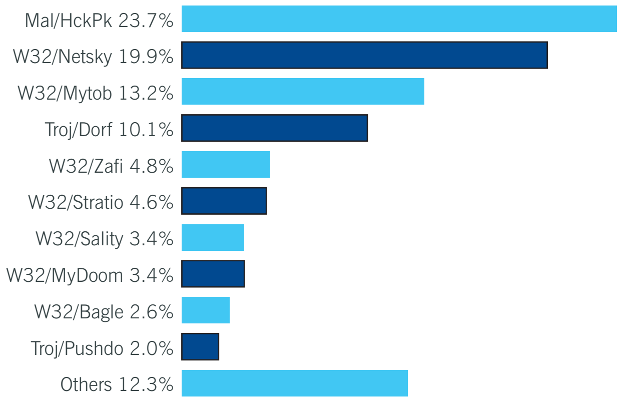
Websites hosting malware, split by web server type

Email threats

Threats spreading via email file attachment continued their decline, as hackers and malicious code writers turn to the web to host their attacks:

Year	No of emails with infected attachments
2005	1 in 44
2006	1 in 337
2007	1 in 909

However, although malicious email attachments have reduced in percentage terms, emails containing links to malicious websites continue to pose a growing problem to computer users.



Top ten threats spread by email attachments in 2007

Top of the chart of malware threats spreading via email file attachments, and responsible for about a quarter of all such threats seen in the last year, is HckPk. It gets its name from the use that it makes of encryption and packing technology to try to bypass security filters. Like Mytob and Dorf (also known as Storm) there are thousands of variants that make up this family.

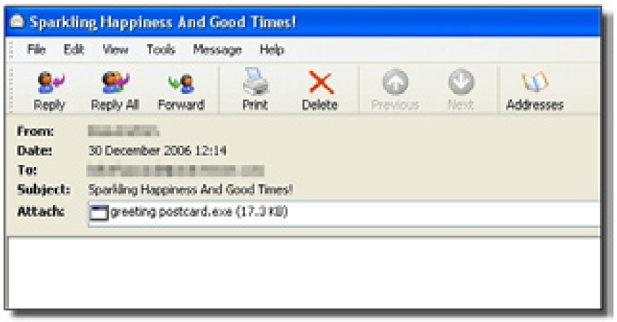
Netsky, Mytob, Zafi, MyDoom and Bagle are well-established malware families that have been around for several years and continue to spread on unprotected computers.

Although mass-mailing worms have dropped from malware writers' favor, Dorf blended this older technique with other newer techniques to infect computers.

Storm of Malware – a chronology

The Storm worm, also known as Dref or Dorf, was 2007's most disruptive threat, with around 50,000 variants seen over the course of 2007.

The criminals behind the Storm attack used topical news stories, electronic greeting cards, videos and fear tactics to lure people into opening their widely spammed-out emails and click on their malicious links.



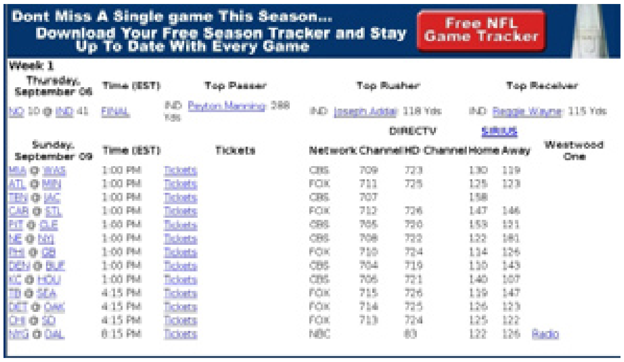
From: [redacted]
Date: 30 December 2006 12:14
To: [redacted]
Subject: Sparkling Happiness And Good Times!
Attach: greeting postcard.exe (17.3 KB)

Early January 2007: Starting as Happy New Year malware[5] which spread malicious greetings via email attachments, the hackers changed their tack in January using news-related events to encourage recipients to click on what claimed to be video content. One of these disguises, which had subject lines such as "230 dead as storm batters Europe"[6], gave the worm its popular name of Storm.

Late January 2007: The Storm worm turned to love in a major new attack as St Valentine's Day approached[7], and in the run-up to US Independence Day on 4th of July[8] the malware gang aggressively took advantage of the celebrations with another malicious ecard campaign. On this occasion, the email contained a web link to compromised zombie computers hosting a Trojan horse.

August 2007: Storm used a wave of malicious emails which posed as links to YouTube videos[9], and then posed as links to music videos of popstars like Beyoncé, Rihanna and The Eagles. If infected, hackers could use victims' computers to steal personal information, spam out malware and junk email, or launch distributed denial-of-service attacks against innocent parties.

September 2007: The Storm worm took advantage of the NFL Kickoff weekend[10] and spammed out an email campaign with links to a hacked website, which would drop malicious code onto insufficiently protected computers.

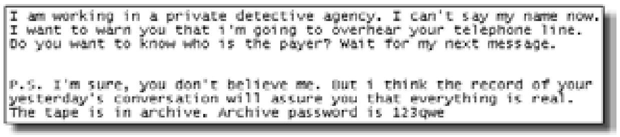

Dont Miss A Single game This Season...
Download Your Free Season Tracker and Stay Up To Date With Every Game
Free NFL Game Tracker

Week 1

Thursday, September 06	Time (EST)	Top Passer	Top Rusher	Top Receiver
NO 10 @ IND 41	FINAL	IND Peyton Manning: 288 Yds	IND Joseph Addai: 118 Yds	IND Reggie Wayne: 115 Yds

				DIRECTV		SIRIUS		
Sunday, September 09	Time (EST)	Tickets	Network	Channel	HD Channel	Home	Away	Westwood One
MIA @ WAS	1:00 PM	Tickets	CBS	709	723	130	119	
ATL @ MIN	1:00 PM	Tickets	FOX	711	725	125	123	
TEN @ JAC	1:00 PM	Tickets	CBS	707		158		
CAR @ STL	1:00 PM	Tickets	FOX	712	726	147	146	
PIT @ CLE	1:00 PM	Tickets	CBS	705	720	153	121	
NE @ NYJ	1:00 PM	Tickets	CBS	708	722	122	181	
PHI @ GB	1:00 PM	Tickets	FOX	710	724	114	126	
DEN @ BUF	1:00 PM	Tickets	CBS	704	719	110	143	
KC @ HOU	1:00 PM	Tickets	CBS	706	721	140	107	
TB @ SEA	4:15 PM	Tickets	FOX	715	726	119	147	
DET @ OAK	4:15 PM	Tickets	FOX	714	725	126	123	
CHI @ SD	4:15 PM	Tickets	FOX	713	724	125	122	
NYG @ DAL	8:15 PM	Tickets	NBC		83	122	126	Radio

November 2007: The hackers tried to scare email users into believing their telephone conversations were being recorded[11], but the ruse was designed to get people to buy bogus security software. In reality, however, the attached MP3 file was a malicious executable program that installed further malware onto the victim's computer which it downloaded from a dangerous website. Amongst these was a piece of scareware which displayed a fake Windows Security Center alert and tried to convince the victim to purchase bogus security software.



```
I am working in a private detective agency. I can't say my name now.
I want to warn you that i'm going to overhear your telephone line.
Do you want to know who is the payer? Wait for my next message.


P.S. I'm sure, you don't believe me. But i think the record of your
yesterday's conversation will assure you that everything is real.
The tape is in archive. Archive password is 123qwe
```

December 2007: The criminal hackers behind the Storm malware showed no signs of letting up and continued their offensive attacks, sending emails claiming to point to websites offering pictures of a stripping "Mrs Clause"[12] and Happy New Year messages[13].

Where is malware 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, 21 percent of all malware is written in China. This is a smaller proportion than in 2006 when the republic's hackers accounted for 30 percent of the malicious code seen.[14]

Country	% of malware written
China	21.0%
Brazil	12.5%
Russia	9.2%

Most of the Chinese malware takes the form of backdoors, but there is also a proportion of Chinese malicious software whose motive is to steal passwords from online gamers.

Brazil accounts for 12.5 percent of the malware that has been analyzed by SophosLabs. The majority of the code written in the South American country is Trojan horses, designed to steal information from online banks. Russian hackers, meanwhile, are responsible for 9.2 percent of the malware seen, mostly creating backdoors that allow cybercriminals to gain access to compromised computers.

Rootkits

SophosLabs estimates that threats from rootkit technology account for about 7 percent of all malware, including high-profile malware, such as Pushdo and Dorf.

There is a renewed interest in rootkits, thanks to hardware-assisted virtualization technologies available in both Intel and AMD processors. Proof-of-concept source code of a hardware virtualization rootkit known as Blue Pill was made publicly available at the Black Hat conference in Las Vegas in August 2006. Virtualization rootkits are supposed to sit deviously between the host hardware and the virtualized subsystem (the guest) to make malware hard or impossible to detect.

In spite of this, SophosLabs does not anticipate that hardware-assisted virtualization-based rootkits will become a significant threat in the near future as they are very complex and rely heavily on hardware extensions that vary from processor to processor. Standard detection techniques, such as on-access scanning, are well suited for detection of malicious hypervisors before install (as the malware arrives on the system).

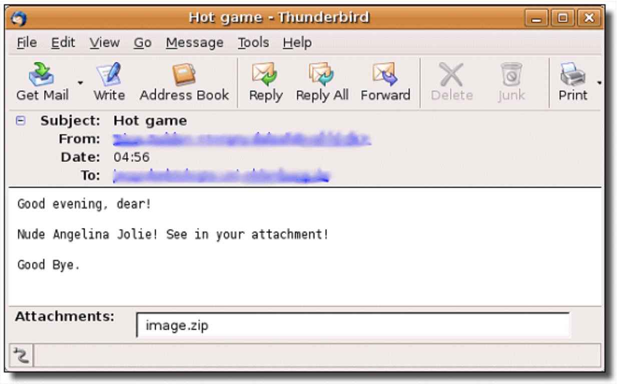
Detection evasion

There is an arsenal of techniques that can be used to try to evade detection by anti-malware products. One of the most common techniques is server-side polymorphism.

Viruses have used polymorphic technology since the early 1990s to mutate their appearance on each infection, in effect making each sample of the malware unique. Server-side polymorphism, however, uses code on the webserver to generate mutated malware. In the past, anti-malware vendors could detect polymorphic viruses by identifying the mutation engine's code. However, with server-side polymorphism, the code which mutates the malware is left on the web server, making it impossible to identify the mutation engine as it is not present in the brand new one-off variant of the malware.

Other techniques often used by malware include encryption, obfuscation and rapidly changing code with potentially automated builds. Obfuscation is particularly frequently used in script-based malware.

These techniques are often used to prevent generic detection techniques. For example, the author of Pushdo – a hacker who spent much of 2007 attempting to infect unwary computer users with the promise of naked pictures of Angelina Jolie[15] – often adds junk (do nothing) instructions, changes the first few bytes of the code, uses encryption of strings commonly present in malicious software and reorders the sequence and the way of calling Windows system functions.



Subject: Hot game
From: [redacted]
Date: 04:56
To: [redacted]

Good evening, dear!

Nude Angelina Jolie! See in your attachment!

Good Bye.

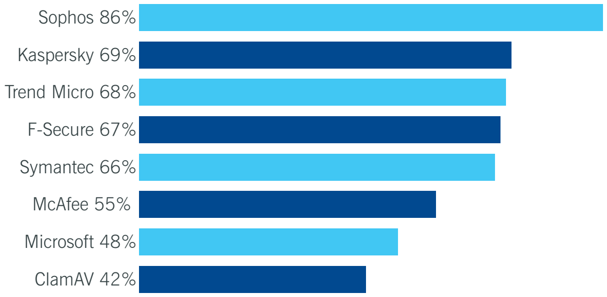
Attachments: image.zip

Detection techniques

Alongside the growing amount of new malware which tries to bypass security measures, there have also been significant technological advances in detection techniques.

To combat the threat of zero-day attacks, and new malware and spyware attacks, security leaders have been looking at behavioral or proactive protection as a method to stop unknown malware from running on a victim machine. This type of protection looks at what a piece of code wants to do, decides whether the action is legitimate or malicious, and acts accordingly.

Unfortunately the implementation of this technology is not trivial and the different approaches taken by some of the industry leaders had varying degrees of success, as can be seen in the results of tests performed by independent testing laboratories, such as AV-Test.org.[16]



Proactive detection rates of new in-the-wild malware

Source: AV-Test.org test, July–September 2007

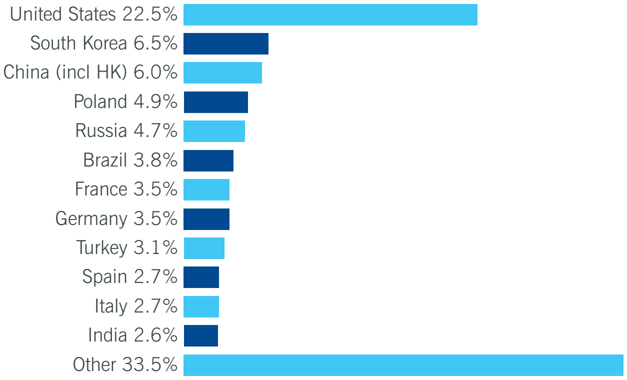
Spam

Spam remains a significant problem for business, with Sophos research revealing that 95 percent of all email is spam. Sophos conducts analysis of all the spam messages received in the company's global network of spam traps. Millions of new messages from these honeypots are analyzed automatically every day, and are used to refine and update existing spam rules.

Occasionally, new techniques are used to try to bypass even the most successful spam filters. When a message is sufficiently different from any previously analyzed by the Sophos spam engines, analysis by researchers establishes whether the message is legitimate or not. Illegitimate emails using new techniques are immediately fed into the spam rules, ensuring that customers are protected against any campaigns using these new techniques.

Dirty dozen

2007 brings some interesting changes to the chart of the 12 countries relaying the most spam.



Dirty Dozen: the top spam-relaying countries in 2007

The top three this year have led the chart since the inception of the threat report in 2005.

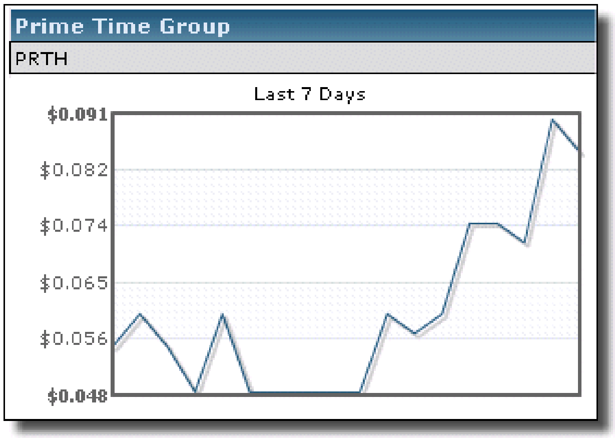
The United States, responsible for sending about a fifth of all the spam in the world for the last few years, needs to tackle this problem urgently. Not only is the problem polluting our inboxes with unwanted emails – some of which will go to malicious or infected websites – it also means that a large number of US computers, most likely those run by home users, are infected. Educating users on how to protect their system against a compromise is paramount to the US's success in its war against spam.

Despite holding onto the same chart positions, the proportion of spam-relaying reported from China has significantly diminished. In 2006, Chinese compromised machines sent more than 15 percent of the world's spam, whereas in 2007, they more than halved this number. In contrast, the US and South Korea have made no significant impact on the problem of spam being relayed via their countries.

Pump-and-dump spam

Pump-and-dump stock campaigns remain a significant problem. They work by spammers purchasing stock at a cheap price and then artificially inflating it by encouraging others to purchase more (often by spamming "good news" about the company to others). The spammers then sell off their stock at a profit.

August 2007 saw a colossal spike in spam volume for 24 hours due to a single pump-and-dump campaign that urged potential investors worldwide to purchase stock in a company called Prime Time Group.[17]



Prior to 2007, pump-and-dump spam campaigns typically attempted to influence the stock price of small North American companies. During 2007, however, Sophos experts noticed a shift in tactics as cybercriminals increasingly tried to manipulate European stocks.[18]

This increased targeting of non-American companies might well be because US authorities have taken stronger action to defuse the criminal activity. For instance, in March 2007, in "Operation Spamalot", the Securities and Exchange Commission (SEC) suspended trading on 35 companies mentioned in stock manipulation campaigns.[19]

As security vendors have become more proficient in intercepting stock spam at email gateways, stock-manipulating hackers have turned to more elaborate methods to get their messages in front of internet users. For example, PDF files, JPGs and other image attachments are used to carry the message in the hope that this type of file will be harder to identify as spam.

One of the more bizarre schemes was seen in October 2007 when a pump-and-dump spam campaign used MP3 music files in an attempt to manipulate share prices[20]. Files posing as music from stars such as Elvis Presley, Fergie and Carrie Underwood actually contained a monotone voice encouraging people to buy shares in a little-known company.

User response to spam

One of the main reasons spammers invest their resources into devising new techniques is that spam works – and looks increasingly successful. In a Sophos web poll conducted in February 2007, 5 percent of respondents admitted to buying goods sold via spam. In a second poll conducted in November 2007, the figure had risen to a concerning 11 percent.[21]

Are you a spammer?

Virtually all spam comes from compromised computers (called “bots” or “zombies”) that have been successfully attacked and now, unbeknown to their owners, are sending out large volumes of spam, launching distributed denial-of-service attacks, or stealing confidential information.

Having up-to-date anti-virus protection, installing and running a firewall, and ensuring that all security patches are in place for both the operating system and any installed applications, will significantly lower the likelihood of being compromised.

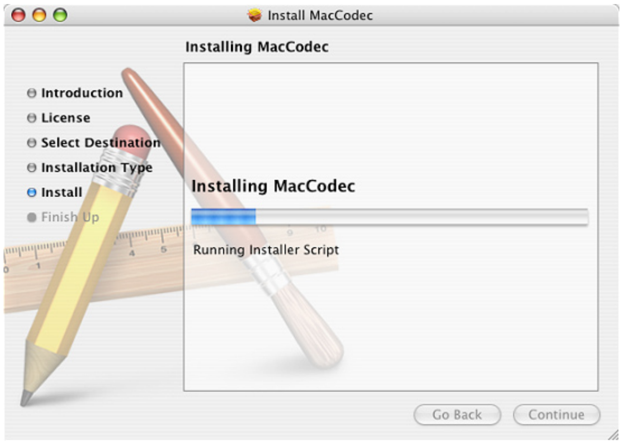
Sophos ZombieAlert Service[22] identifies business computers that have been hijacked and which are sending out emails on behalf of the spammers.

Apple and threats and the future

One of the most significant developments of 2007 was the rise of malware for Apple Mac computers. Although malware for Apple Macs, and even the Mac OS X operating system, has been seen before[23] it has not encountered anything like the number of viruses, Trojans and worms that run on Microsoft Windows. This is largely because malware writers have not felt it necessary to infect the computers of Apple Mac owners when there have been so many poorly protected Windows users available.

Now, however, financially motivated gangs have begun to think that there is a viable reason to infect Macs alongside Windows PCs.

In November 2007, Mac OS X malware made the headlines. The functionality of the malicious program, known as OSX/RSPlug[24], was fairly simple. It modified settings to redirect DNS requests to a server under the hacker control, allowing hackers to serve up fake websites requiring usernames and passwords, display adverts and so on.



Installing MacCodec

Running Installer Script

OSX/RSPlug is connected to a widespread family of Windows malware called Zlob[25], which promises to display pornographic material when the user loads a new codec (a program that allows internet users to watch video content).

Clicking on malicious email or web links takes the unwitting computer user to a site hosting malware. The malicious website examines the request made by the user's web browser and responds appropriately, depending on whether the computer visiting the site is a Mac or Windows PC. Apple Mac computers receive the OSX/RSPlug-Gen file, which is not able to infect the Windows platform. A Windows PC, however, receives the Zlobar-Fam Trojan.

This approach means that the malware authors can target a much wider range of users with a single set of links – while the Trojans themselves are not cross-platform, the delivery mechanism is. Sophos has seen Mac malware planted on a large number of websites, with many variants of the Trojan being distributed.[26]

Although Macintoshes have a long way to go before they overtake PCs in popularity, particularly in the office environment, analysts are reporting that an increasing number of consumers are open to considering purchasing a Mac computer rather than a PC in future. This may drive the emergence of more financially motivated malware for this platform.[27]

It is concerning that the Mac has become the focus of at least one malware gang. Ultimately, future Mac malware attacks will be driven by how effective the attackers are at infecting Apple Mac users. The criminal hacking gangs are in business to make money, so if they do not see a return on their investment, they will not invest more effort.

For this reason, it is essential that Apple Mac users ensure they are properly defended - and stay clued-up about the various attack mechanisms that cybercriminals can use to break into their computers.

Mobile phones and Wi-Fi devices

Mobile security threats

There are approximately 200 malware threats for mobile phones, compared to over 300,000 for Windows. The risk of being infected on a mobile phone is tiny in comparison.

Nevertheless, the mobile malware threat has been growing steadily over the last few years and more businesses are now looking to secure confidential data against potential attacks at all endpoints. In a Sophos web poll, in November 2006, 81 percent of business IT administrators expressed concern that malware and spyware targeting mobile devices will become a significant threat in the future. However, 64 percent also said they currently have no solution in place to secure company smartphones and PDAs.[28]

Last update: Oct 17 2006
Version: 1.0.0.905m
On-access scanning: Active

Ultimately the main vulnerability on any system is the user and Sophos expects to see messages sent to mobile users luring them to fake webpages on which they will be instructed to enter confidential data, in just the same way that desktop email users are trapped.

IT managers should not only be looking to protect their PDAs and mobile phones from malware, but also be investigating data encryption and access control. It is also wise to invest in user education on how to safely browse online. Those with mobile devices need to understand that many of the web threats affect them as well, regardless of the device or operating system they are using.

Ultra-mobile PCs, iPhones and Wi-Fi devices

The wider availability of wireless internet services has increased the attractiveness of Wi-Fi-enabled devices.

Although simple Trojans have been seen, the Apple iPhone has not yet been the target of commercially motivated hackers. The fact that most versions of the phone/music player/browser are locked to particular service providers and lengthy contracts has, however, limited its appeal to the mass-market and may mean iPhone adopters have some breathing space before attacks begin in earnest.

Flaws have been found in Apple's mobile email application and Safari browser and it is more likely that attacks would be focused on these areas than the underlying operating system. But cybercriminals seeking a larger return are likely to stick mostly to Windows desktops for the foreseeable future.

The iPod Touch is more affordable than the iPhone, and shares its Safari web browser. As both the iPhone and iPod Touch are designed to connect to the internet, and can retrieve email and visit websites, it is theoretically possible that hackers will target them more in the future. At the moment, Safari appears to be the most likely place where vulnerabilities would be exploited.

Meanwhile, 2008 looks set to be the year of increased take-up of ultra-mobile PCs (UMPCs). UMPCs, like the Asus EEE subnotebook, have shaken up the laptop market with their low price, usability and portability.

Interestingly, this new range of UMPCs does not necessarily come with a version of Windows pre-installed (in the case of the Asus EEE, it comes with the Xandros flavor of UNIX). For this reason, UMPCs are automatically immune to the vast majority of spyware, adware and malware attacks – but if such devices continue to increase in popularity the situation might change.

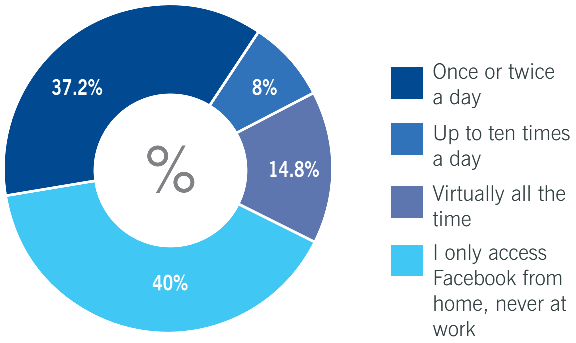
Of course, as has been pointed out earlier, a lot of hacking attacks actually have very little to do with technology, but with vulnerabilities in the human operating the computer. So it is perfectly possible right now for users of any of these mobile devices to receive spammed phishing messages, follow the link and enter their confidential data.

A procrastinator's paradise or an identity thief's dream?

Social networking websites like Facebook, Bebo, Orkut, and MySpace have become phenomenally popular – not just with teenagers trying to keep in touch and internet-savvy pop groups, but also with hackers interested in stealing information from individuals and companies. So organizations are facing the dual concerns of social networking websites causing productivity issues by distracting employees from their work, and the risk of malware being introduced to the workplace.

Productivity threat

Users openly brag about logging in to their Facebook accounts rather than work. The "I have dossed around on Facebook all day and consequently have done no work" group for instance has more than 220 members. Sophos research into how addictive social networking can become, showed that one in seven users were logged into their Facebook profile virtually all the time during office hours.[29]

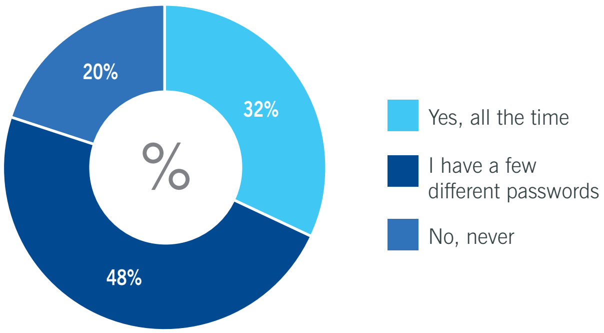


How often employees access Facebook from work
Source: Sophos online survey, September–October 2007

Identity theft threat

Sophos also conducted research into the dangers of irresponsible behavior on Facebook. Using a fake profile[30] Sophos was able to discover information about other Facebook users, such as their date of birth, current email address or phone number. Sophos also gained access to further personal facts including employer details, complete resumés and one user even divulged his mother's maiden name – information often requested by websites in order to retrieve account details.

Giving up so much information about their interests and personal life, along with detailed information about their companies online, is playing into the cybercriminals' hands. 32 percent of people use the same password for every website they access – if criminals guess it in one place, they may well be guessing it for the company network too. In order to protect their data and their reputations, organizations need to act quickly to set up guidelines for employees who are posting on these sites.

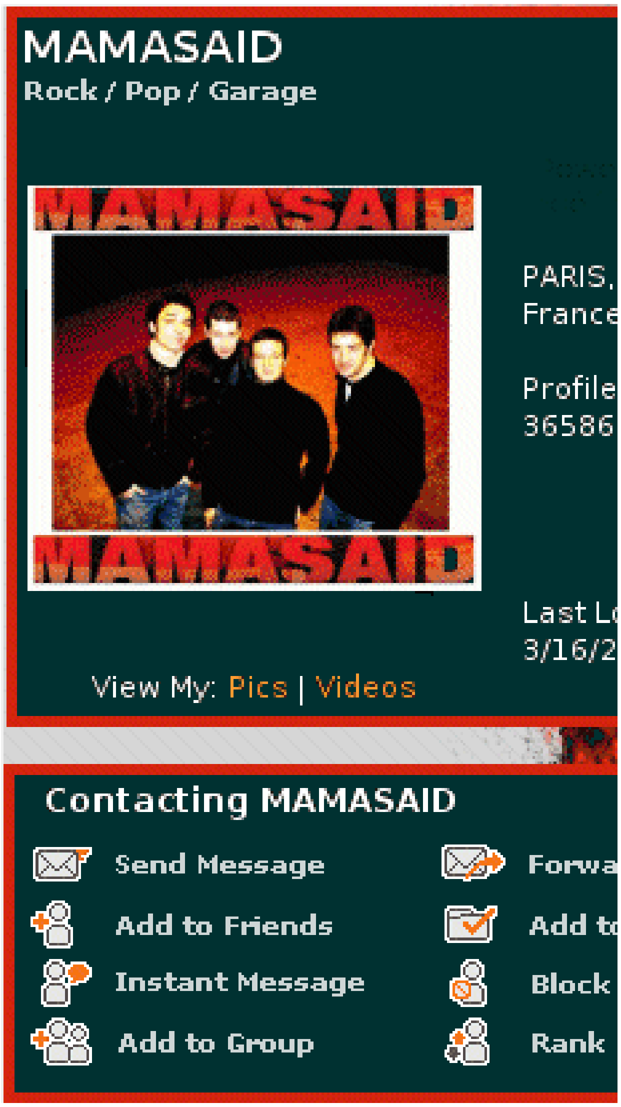


Do you use the same password for every website you access?
Source: Sophos online survey, November 2007 - December 2007

The social networking sites themselves also need to address the problem. While Facebook has been commended for the strict security options available[31], it needs to do more to educate its users on securing profiles, and consider changing its own default settings.

Malware threat

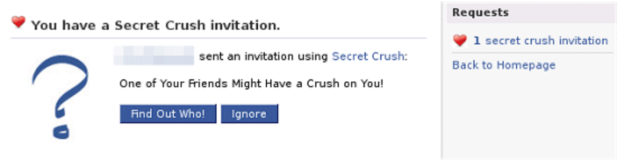
Social networking websites have also been abused by criminals trying to spread code to unsuspecting users. For instance, in March 2007, the SpaceStalk spyware Trojan horse was discovered embedded in a QuickTime movie on the MySpace page of MAMASAID, a French rock band. The Javascript code downloaded further malicious code from the net designed to steal information[32].



In September, in a separate incident, MySpace and Bebo were amongst the websites which fell foul of poisoned banner advertisements designed to install Trojan horses onto the computers of Windows users. The infected adverts were served by Right Media, an advertisement network owned by Yahoo. Hackers circumvented security checks by programming the offending files not to infect PCs on Right Media's network.

Google's social networking website, Orkut, which is particularly popular in Brazil, was struck by the JS/Adrecl-A worm in December 2007, and infected over 670,000 users[33].

Meanwhile the Secret Crush application, which had over 50,000 daily users on Facebook, invited people to find out who amongst their friends has a secret crush on them. Users tempted to discover more have to invite at least five other Facebook users to install the application before their mystery admirer is revealed.



You have a Secret Crush invitation.

[redacted] sent an invitation using Secret Crush:

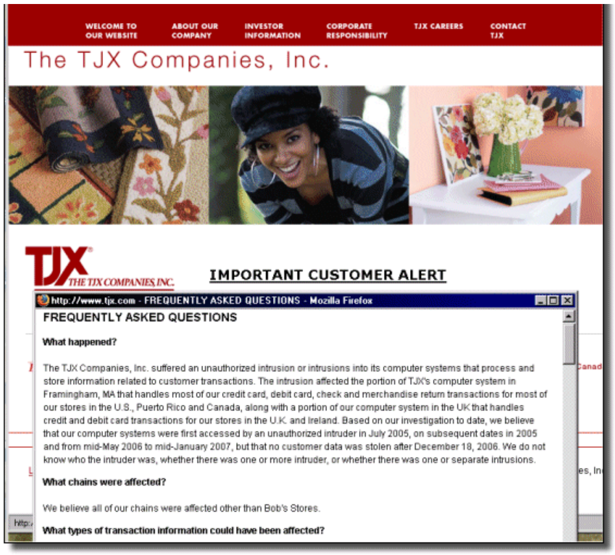
One of Your Friends Might Have a Crush on You!

However, no secret crush is ever revealed. Instead users are directed to an external website which invites Facebook users to download adware that will display pop-up advertising.[34] Whoever wrote the Secret Crush application earned money by encouraging people to download and install the advertising program.

Identity theft – a corporate problem

Countless news stories, from TJ Maxx losing details of around 90 million customers over a two-year period[35], and the November 2007 debacle of the UK's HMRC (Her Majesty's Revenue and Customs) losing sensitive data about 25 million families in Britain[36], indicate that even large organizations are at risk.

In August 2007 it was revealed that employment search website Monster.com had lost personal information about more than 1 million people[37]. Attackers used the usernames and passwords of professional recruiters to access Monster.com's resumé database, and then spammed out phishing emails and malware to innocent job searchers.



IMPORTANT CUSTOMER ALERT

FREQUENTLY ASKED QUESTIONS

What happened?

The TJX Companies, Inc. suffered an unauthorized intrusion or intrusions into its computer systems that process and store information related to customer transactions. The intrusion affected the portion of TJX's computer system in Framingham, MA that handles most of our credit card, debit card, check and merchandise return transactions for most of our stores in the U.S., Puerto Rico and Canada, along with a portion of our computer system in the UK that handles credit and debit card transactions for our stores in the U.K. and Ireland. Based on our investigation to date, we believe that our computer systems were first accessed by an unauthorized intruder in July 2005, on subsequent dates in 2005 and from mid-May 2006 to mid-January 2007, but that no customer data was stolen after December 18, 2006. We do not know who the intruder was, whether there was one or more intruder, or whether there was one or separate intrusions.

What chains were affected?

We believe all of our chains were affected other than Bob's Stores.

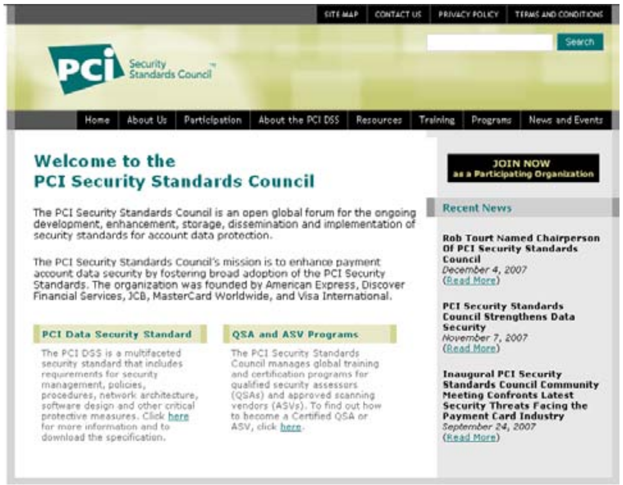
What types of transaction information could have been affected?

Payment card industry compliance

In response to serious data breaches, the payment card industry security standards council (PCI DSS) was formed and has since put in place 12 requirements with which organizations that deal with credit and debit card transactions must be compliant.

It has been reported that only one third of retailers are PCI compliant[38].

The cost of a data breach, both in resource and software terms, can be huge, and many companies without a detailed security strategy and the right information may be paying a premium to secure their networks. By properly securing and controlling their computers and the access to its network, an organization can significantly reduce the chances of a security breach happening. In addition, regulations that deal with the human aspect of mishandling data – accidental or otherwise – must be put in place to combat lax security.



Welcome to the PCI Security Standards Council

The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The PCI Security Standards Council's mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

PCI Data Security Standard

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. Click here for more information and to download the specification.

QSA and ASV Programs

The PCI Security Standards Council manages global training and certification programs for qualified security assessors (QSAs) and approved scanning vendors (ASVs). To find out how to become a Certified QSA or ASV, click here.

Recent News

Rob Tourt Named Chairperson Of PCI Security Standards Council
December 4, 2007
(Read More)

PCI Security Standards Council Strengthens Data Security
November 7, 2007
(Read More)

Inaugural PCI Security Standards Council Community Meeting Confronts Latest Security Threats Facing the Payment Card Industry
September 24, 2007
(Read More)

NAC – helping enforce compliance

Leading security analysts such as Gartner and IDC agree that companies need to start their investigations now into network access control solutions and how they can integrate into the security framework. Integration of security point-solutions at the heart of the organization - the desktop and file server - is the recommended route forward, simplifying the management for administrators while using less resource on the network.

What does NAC do?

NAC (network access control) helps reduce the risk of compromising your network security.

- Works alongside anti-malware and firewall products and meet the following criteria:
- Stops unauthorized, guest or non-compliant systems accessing your network
- Ensures all computers conform to a defined security policy
- Is simple to deploy and easy to use
- Allows easy identification and isolation of unmanaged computers.

State-sponsored cybercrime

During 2007 it became more common for countries to openly accuse each other of engaging in spying via the internet – even though it can be extraordinarily difficult to prove an attack is being sponsored by a government.

In April, a large-scale distributed denial-of-service attack against websites belonging to the Estonian prime minister, banks and schools, were claimed to be masterminded by the Kremlin[39] after Estonia decided to remove a statue of a Soviet-era soldier that comprised part of a World War II memorial. Estonian Minister of Defence, Jaak Aaviksoo, accused the Russian government of launching the attack and called on NATO to amend its protocols to recognize the attack as a form of military action. However, no proof was presented that the attacks could be traced back to the Kremlin.

In another example in December 2007, it was revealed that MI5, the British secret service, had written a secret letter to 300 chief executives warning them that they were under attack from "Chinese state organizations"[40]. According to reports, the Chinese government was behind electronic espionage against British firms designed to give China a commercial advantage.

Three months earlier, newspapers reported that the Chinese military were being blamed for a cyberattack which targeted a Pentagon computer system serving the office of US defense secretary, Robert Gates. Unnamed sources claimed that the People's Liberation Army (PLA) were blamed in an internal investigation for perpetrating the attempted hack. The British and German governments were also said to have been subject to similar probes by hackers working for the PLA.

When Sophos asked in a poll[41] in September 2007 who people believed were likely to have been responsible for the attack the results were:

Believed responsible	**% of respondents**
Chinese	45%
Impossible to say	36%
Someone pretending to be Chinese	19%

The Chinese foreign ministry vigorously denied the claims, and said it works hard to fight cybercrime.

2008 is likely to bring more claims of countries attacking and spying on each other via the internet, but so far there has been no convincing evidence released to the public proving that attacks are backed by foreign governments. It must be remembered that internet hackers can hide their tracks, hopping from computer to computer, and leapfrogging around the world, making it very hard sometimes to determine precisely who is behind an attack. There is no doubt, however, of the importance of securing critical computers inside government from hackers whether motivated by politics, espionage or money.

Arrests and the law

The repercussions for cybercriminals are finally coming in line with the severity of their crimes. With international computer crime authorities joining efforts in a bid to bring down hackers, malware authors and spammers, the past 12 months have seen more arrests and harsher sentencing for criminals involved in high-profile crimes.

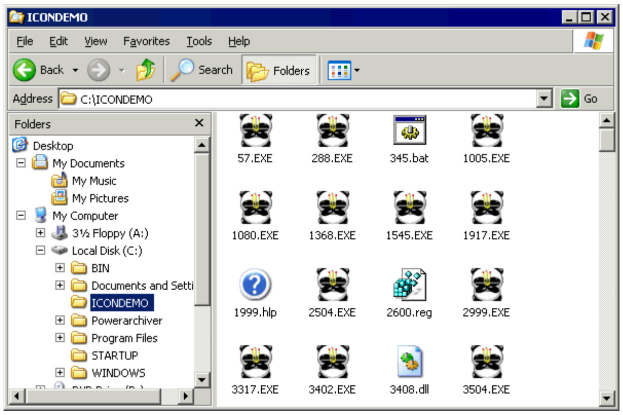
Below are some of the cases that made the news in just in the second half of 2007.

August 2007: 27-year-old Christopher Smith was sentenced to 30 years in prison in the US for selling millions of dollars worth of medications online to customers without prescriptions or a license[42].

August 2007: Jacob Vincent Green-Bressler was sentenced to seven years in prison for buying stolen data from hackers[43]. Armed with account numbers, identification numbers (PINs), passwords and social security numbers, 21-year-old Green-Bressler was able to create counterfeit credit cards and withdraw money from cash machines.

September 2007: A Chinese court found four men guilty of writing and selling the Fujacks worm[44], which converted icons of infected files into joss-stick-burning pandas. The malware was designed to steal usernames and passwords from online gamers, details which would fetch a high price on the black market. The men were sentenced to between two and half and four years in jail, but not before they wrote and gave the authorities a fix for the infection.*

October 2007: James R Schaffer and Jeffrey A Kilbride were each sentenced to five years in jail and fined $100,000 for their part in sending innocent internet users sexually explicit images, a crime that netted them over $2 million[45].



November 2007: A 17-year-old was arrested in The Netherlands following claims that almost $6,000 worth of virtual furniture was stolen from users of a popular teenage gaming website[46]. Virtual furniture at Habbo Hotel is purchased with credits that cost real currency. The teenager created fake Habbo Hotel websites, captured the players' login details and used the information to break into the real website and steal virtual furniture.

With hacking, phishing and web threats on the increase, Sophos looks expectantly to 2008 for further improvements in solving computer crime cases, but warns that authorities should not become complacent if they are to keep users safe.

Shockingly, one was offered a job by one of the victim companies

The future

Predicting the future in such a rapidly evolving scene is near impossible. One only needs to look at the virus scene five years ago to see how quickly the threat has become more serious in a short period of time. Indeed, a Sophos poll revealed that 70 percent of those surveyed believed that 2008 would actually be just as bad or worse for IT security than 2007.

It does seem inevitable that the variety and number of attacks will continue to escalate, driven by organized crime's desire to break into computers to steal information, identities and resources. Sophos expects computer users will continue to face challenges in securing and controlling their computers as criminals attempt to capitalize on new technology to make money and cause disruption. In addition, threats like identity theft and fraud will still be occurring far into the future because of human mistakes.

However, if managed properly, the problem should not be insurmountable as sound security practices, up-to-date protection and an active commitment to keep informed can all help defend business networks in the year ahead.

The good news is that security software is getting better all the time. Proactive detection of new, unknown malware threats is at an all-time high, and computer users who are sensible and properly defended can dramatically reduce the risks.

Sources

1. www.sophos.com/security/technical-papers/modern_web_attacks.html
2. www.sophos.com/news/2007/07/toptenjun07.html
3. www.sophos.com/news/2007/09/consulate.html
4. www.sophos.com/security/technical-papers/sophos-securing-websites.html
5. www.sophos.com//news/2007/01/drefv.html
6. www.sophos.com/news/2007/01/malwarestorm.html
7. www.sophos.com/news/2007/01/dorflove.html
8. www.sophos.com/news/2007/07/july4.html
9. www.sophos.com/news/2007/08/youtube.html
10. www.sophos.com/security/blog/2007/09/577.html
11. www.sophos.com/news/2007/11/detective-dorf.html
12. www.sophos.com/news/2007/12/santa-storm.html
13. www.sophos.com/news/2008/01/holiday-hackers.html
14. www.sophos.com//news/2007/01/secrep2007.html
15. www.sophos.com/news/2007/10/toptensep07.html
16. www.sophos.com/security/blog/2008/01/974.html
17. www.sophos.com/news/2007/08/spam-pump.html
18. www.sophos.com/news/2007/03/german-pump.html
19. www.sophos.com/news/2007/03/sec.html
20. www.sophos.com/news/2007/10/stock-mp3.html
21. www.sophos.com/news/2007/12/spam-buyers.html
22. www.sophos.com/products/enterprise/alert-services/zombiealert.html
23. www.sophos.com/news/2006/02/macosxleap.html
24. www.sophos.com/security/blog/2007/11/729.html
25. www.sophos.com/security/blog/2007/05/117.html
26. www.sophos.com/security/blog/2007/11/797.html
27. money.cnn.com/news/newsfeeds/articles/newstex/IBD-0001-21528092.htm
28. www.sophos.com/news/2007/02/mobile-security.html
29. www.sophos.com/pressoffice/news/articles/2007/10/facebook-addiction.html
30. www.sophos.com/news/2007/08/facebook.html
31. www.sophos.com/security/best-practice/facebook.htm
32. www.sophos.com/news/2007/03/myspace-malware.html
33. www.sophos.com/security/blog/2007/12/900.html
34. www.sophos.com/news/2008/01/facebook-adware.html
35. www.sophos.com/news/2007/03/tjx.html
36. www.sophos.com/news/2007/11/hmrc-id-theft.html
37. www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032518
38. www.computerweekly.com/Articles/2007/09/06/226599/vendor-report-pci-is-your-business-up-to-the-standard.htm
39. www.guardian.co.uk/russia/article/0,,2081438,00.html
40. www.sophos.com/news/2007/12/mi5-china-internet-spy.html
41. www.sophos.com/news/2007/09/chinese-hack.html
42. www.sophos.com/news/2007/08/rizler.html
43. www.sophos.com/news/2007/08/stolen-identity.html
44. www.sophos.com/news/2007/09/fujacks-jail.html
45. www.sophos.com/news/2007/10/porn-spam-jail.html
46. www.sophos.com/news/2007/11/habbo-hotel.html

About Sophos

Sophos enables enterprises worldwide to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. With over 20 years of experience, we protect over 100 million users in nearly 150 countries with our reliably engineered security solutions and services. Recognized for our high level of customer satisfaction, we have an enviable history of industry awards, reviews and certifications. Sophos is headquartered in Boston, MA and Oxford, UK.

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

SOPHOS

secured.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan