SOPHOS

Security threat report: 2009

Prepare for this year's new threats

SOPHOS

Security threat report: **2009**

Overview

On 2 November 1988 a 22-year old Cornell University student called Robert Morris released an internet worm capable of exploiting vulnerabilities in the UNIX operating system. It is estimated that it infected 10 percent of the internet. Twenty years on, the scale of the malware problem has grown astronomically. Today's internet attacks are organized and designed to steal information and resources from consumers and corporations. Although there have been instances of attacks driven by politics and religion, the main motivation is financial.

The web is now the primary route by which cybercriminals infect computers, mainly due to the fact that increasing numbers of organizations have secured their email gateways. As a consequence, cybercriminals are planting malicious code on innocent websites. This code then simply lies in wait and silently infects visiting computers.

The scale of this global criminal operation has reached such proportions that Sophos discovers one new infected webpage every 4.5 seconds – 24 hours a day, 365 days a year. In addition, SophosLabs, our global network of threat analysis centers, is sent some 20,000 new samples of suspect code every single day.

2008 proved that malware is more than just a Microsoft problem. Although the sheer number of Windows threats far outweighs attacks against any other platform, cybercriminals are turning their attention to other operating systems such as Apple Macintosh, and vulnerable cross-platform software. This seems likely to continue in 2009, with the increasing popularity of portable devices such as the iPhone, iPod Touch, Google Android phone and ultra-mobile netbooks.

2008 at a glance

Biggest malware threats – SQL injection attacks against websites and the rise of scareware

New web infections – one new infected webpage discovered by Sophos every 4.5 seconds

Malicious email attachments – five times more at the end of 2008 than at the beginning

Spam-related webpages – one new webpage discovered by Sophos every 15 seconds

New scareware websites – five identified every day

Top malware-hosting country – US with 37 percent

Top spam-relaying continent – Asia with 36.6 percent

Amount of business email that is spam – 97 percent

It remains paramount that organizations defend themselves at all levels of their business, not just at the email and web gateways. Networks, desktops, laptops and mobile devices must be comprehensively secured to defend against the myriad threats posed by the criminal underground.

Web threats

Exploiting legitimate websites

In the last couple of years the web has become a major vector of attack for cybercriminals, replacing their previous reliance on email systems. By exploiting poorly secured legitimate websites hackers have been able to implant malicious code onto them, which then attempts to infect every visitor. One of the reasons the web is so popular is that legitimate websites can attract large numbers of visitors, all of whom are a potential victim.

Many well known organizations and brands have fallen victim to this kind of attack during 2008. Both large and small organizations have been targeted, emphasizing the importance of proper web security across the board.

- **January 2008**: Thousands of websites belonging to Fortune 500 companies, government agencies and schools were infected with malicious code.
- **February 2008:** UK broadcaster ITV was the victim of a poisoned web advert campaign, designed to deliver scareware to Windows and Mac users[1].
- **March 2008:** A site selling tickets for the Euro 2008 football championship was hacked[2], while anti-virus firm Trend Micro found some of its webpages had been compromised[3].
- **April 2008:** Cambridge University Press's website was compromised so that visitors to its online dictionary were subject to unauthorized hacker scripts[4].
- **June 2008:** As the Wimbledon tennis tournament opened in the UK, the Association of Tennis Professionals site was infected[5].
- **July 2008:** Sony's US PlayStation website suffered an SQL injection assault which put visiting consumers at risk from a scareware attack[6].
- **September 2008:** *BusinessWeek* magazine was infected with an SQL injection attack that attempted to download malware from a Russian-based server[7].
- **October 2008:** An area of the Adobe website designed to offer support to video bloggers was compromised by an SQL injection attack[8].

SQL injection attacks

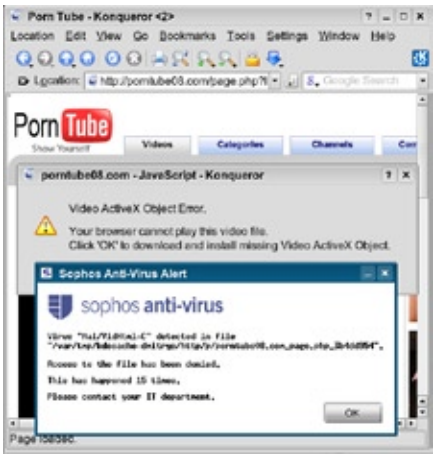
One of the major headline grabbers of 2008 was the SQL injection attack. Such attacks exploit security vulnerabilities and insert malicious code (in this case script tags) into the database running a site. When user input, for instance via a web form, is not correctly filtered or checked, the code peppers the database with malicious instructions. Recovery can be difficult, and there are numerous cases of website owners cleaning up their database only to be hit again a few hours later.

Automated systems

Hackers have developed automated tools that use search engines such as Google to identify potentially vulnerable websites, and then inject code into the servers. Websites are rarely specifically targeted, and are often just unfortunate enough to have been discovered by the cybercriminals' malware distribution tool.

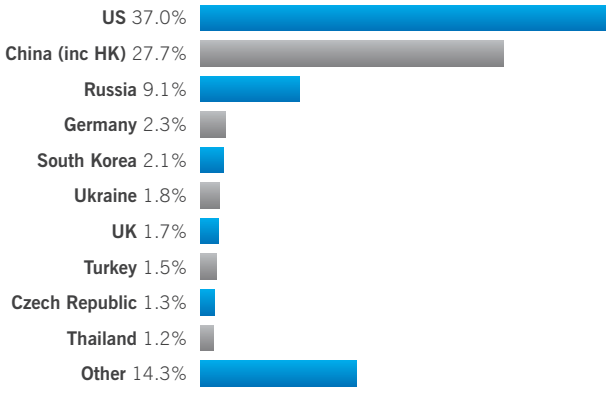
Cybercriminals are also building their own malware-infected websites, often using free web-hosting services which do not require users to go through a rigorous identification process. They then use automated systems to plant malicious links on legitimate blogs and web forums, pointing at these infected sites.

For instance, during 2008 Sophos encountered many examples of legitimate blogs and message boards carrying comments which linked to websites pretending to offer adult videos, but which actually demanded a browser plug-in upgrade before anything could be seen. The updated fake codec or bogus Flash Player software that the user downloaded was in reality scareware that attempts to frighten the user into purchasing fake security software.



Top 10 countries hosting malware on the web

2008 showed the US, China and Russia accounting for almost three quarters of all the world's websites that spread malware. However, it would be misleading to believe that other countries are not also contributing to the problem.



The top 10 malware hosting countries

Sophos research reveals that there is a "long tail" effect with more than 150 countries identified as hosting malware on webpages based within their borders. Of these affected webpages, 85 percent are on legitimate websites that have been hacked by criminals.

Malware chart rundown

- The US tops the chart with just under three in every eight infected webpages based there. This shows an increase over 2007, when it accounted for less than one in four (23.4 percent) .
- China, which was responsible for hosting more than half (51.4 percent) of all the world's malware in 2007, has now almost halved its proportional contribution to the problem.
- The Czech Republic is a new entrant on the list and hosts over one percent of all the world's malware on the web.
- Poland, France, Canada, Netherlands were present in positions six, eight, nine and ten respectively in 2007, but now have too few malicious websites to appear on the chart.

User resistance

Although web security is designed to protect against malware and other threats, some users have responded negatively and taken steps to subvert the protection. This is particularly true where companies and organizations filter URLs to particular websites for policy reasons, such as blocking social networking or video websites.

Anonymizing proxies

Some users have responded to web filtering by using anonymizing proxies[9], which disguise the true nature of a website in order to trick an organization's web filter into allowing access.

Information about public anonymizing proxies is shared freely on thousands of blogs, forums and websites, and there are an unknown number of private anonymizing proxies built for the use of an individuals or small groups. This makes it extremely easy for users to access an anonymizing proxy, but difficult and time-consuming for administrators to track and block them. If users are browsing via anonymizing proxies, then in addition to bypassing URL filtering, they are also circumnavigating content scanning at the perimeter, which dramatically increases the chance of infection.

Sophos has even identified anonymizing proxies that are themselves infected with malware. It's not possible to tell whether the anonymizing proxies are the innocent victims of infection, or have been set up with malware embedded inside them. But regardless of whether the infection is deliberate or not, anyone using them runs the real chance of infecting their computer and the network it is connected to.

Anonymizing proxy use appears to be particularly prevalent among educational establishments, where technology-savvy students attempt to subvert acceptable use policies. Sophos actively tracks internet forums to discover new anonymizing proxy services, and incorporates real-time detection of private anonymizing proxies through traffic inspection in its web appliance.

Email threats

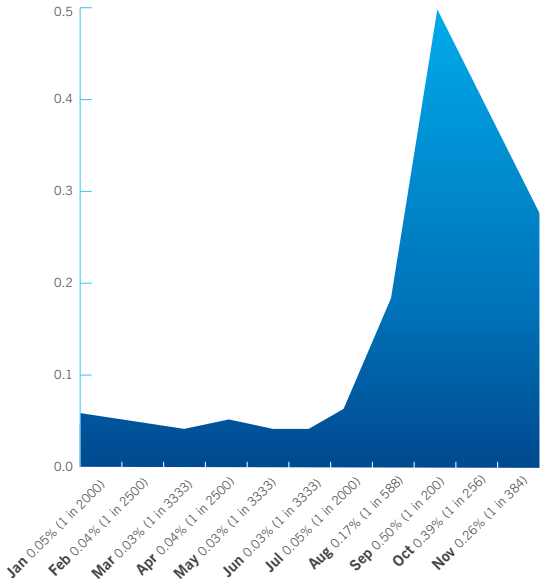
Attachment-based threats on increase

In recent years, the number of threats spread via email attachment has declined.

Year	Emails with infected attachments (average)
2005	1 in 44
2006	1 in 337
2007	1 in 909
2008	1 in 714

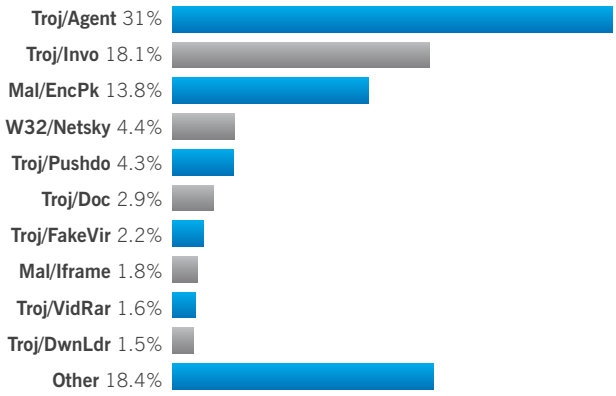
However, while web-based threats have tended to dominate the malware agenda in the last 12 months, there were five times as many malicious email attachments at the end of 2008 than at the beginning.

The increase is most apparent when shown by month – from a low of 1 in 3333 in the first quarter of the year to a high of 1 in 200 by September.



Percentage of infected email attachments in 2008, month by month

Sophos identified that much of this increase can be attributed to several large-scale malware attacks made by spammers from August 2008 onwards. High profile attacks during this period included the Invo-Zip Trojan horse which masqueraded as a notice of a failed parcel delivery from firms such as FedEx and UPS[10], the Agent-HNY Trojan that was spammed out disguised as the Penguin Panic Apple iPhone arcade game[11], and the EncPk-CZ Trojan, which pretended to be a Microsoft security patch[12].



Top 10 email attachment-based malware for 2008

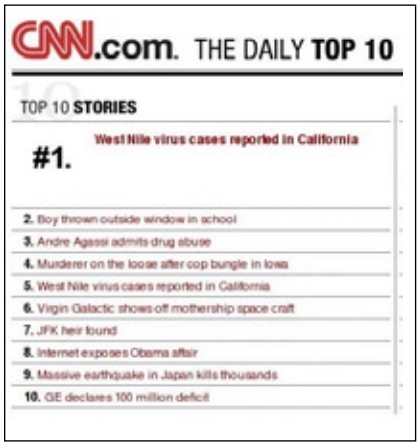
The scale of the email attacks in the second half of 2008 can be seen in the Pushdo Trojan[13] (which posed as naked pictures of Angelina Jolie and Nicole Kidman) that accounted for 31 percent of all reports in the first half of the year.

Troj/Agent's and Troj/Invo's rapid dominance of the email attachment-based malware chart – accounting for almost 50 percent – is notable for outstripping the Netsky worm, which has consistently plagued the higher positions of the chart since it was released in early 2004[14]. Whereas Netsky contains self-replicating code to duplicate itself and spread across the internet, the Agent and Invo Trojans can not travel under their own steam but rely on spam – usually from a compromised computer.

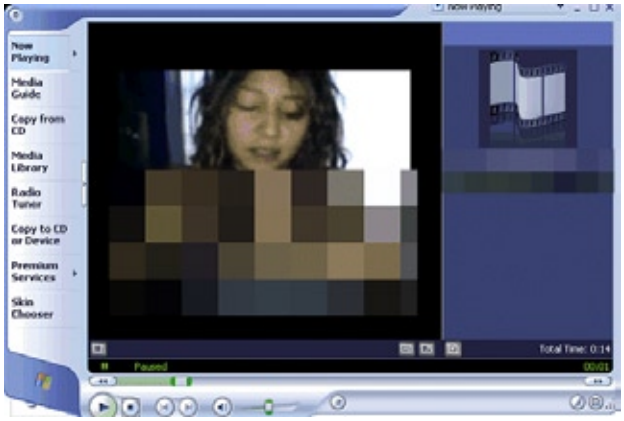
Malicious links

As well as using malicious email attachments, cybercriminals continue to embed malicious links in emails and spam out creative and timely attacks designed to prey on users' curiosity.

For example, in August 2008 Sophos warned of a widespread wave of spam messages claiming to be breaking news alerts from MSNBC and CNN[15]. Each email encouraged users to click on a link to read the news story, but instead took them to a malicious webpage that infected Windows computer with the Mal/EncPk-DA Trojan.



In September 2008, an email was widely spammed containing a link to what was said to be a pornographic video of US presidential candidate Barack Obama[16]. However, the webpage really installed the Mal/Hupig-D malware.



On the day after Obama's presidential victory, another spammed-out malware campaign invited recipients to click on a web link to watch a video of the successful Democratic candidate[17]. In reality, visiting the website could lead to information being stolen from the victim's computer and sent to a server in Kiev in the Ukraine.

Fear of infection

One significant method used by cybercriminals to make money during 2008 was the use of fake anti-virus software, also known as scareware or rogueware. Such attacks prey on IT security fears and fool users into believing their computer has a problem when it has nothing of the kind.

Typically, scareware is planted on websites in the form of pop-up adverts, or disguised downloads. However, there have also been occasions when hackers have spammed out scareware, or links to it, using traditional social engineering tricks to fool users into clicking on the attachment or link. In just one of its spam traps, Sophos detected approximately 5000 such emails every day.

Scareware-linked websites often carry security software that pretends to be bona fide, complete with bogus reviews concerning its fake effectiveness at killing off viruses. Sometimes the websites steal users' credit card details.

Hacking gangs have become proficient at rapidly producing professional-looking bogus websites posing as legitimate security vendors. On average Sophos identifies five new scareware websites every day, with the figure rising to over 20 a day on occasions. Even established security brands such as Norton AntiVirus[18] and AVG have been targeted.

Some legitimate software companies may even be embroiled in the scams, with rogue advertising affiliates using scareware to increase sales of the legitimate product.

The motivation for the gangs responsible for the scareware problem is apparent in the case of Lee Shin-ja, the former CEO of a Korean anti-virus company. Lee is said to have earned over US $9.8 million since 2005 with a free anti-spyware program that displayed fake security warnings and directed users to purchase her company's Doctor Virus clean-up solution[19].

It is worth noting that the scareware problem is not limited to Windows computers. In February 2008, Sophos encountered scareware campaigns that targeted both Windows and Apple Mac users[20].

Malware on the move

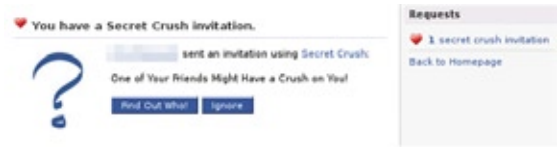
Malware transferred via USB memory sticks is also on the rise. Perhaps the most bizarre USB malware-related story which emerged during 2008 was that of astronauts infecting computers on the international space station because of lax security measures[21].

Malware attacks via social networking

2008 saw much more interest in using social networking websites to spread malware. In August, Facebook admitted that up to 1800 users had had their profiles defaced by an attack that secretly installed a Trojan while displaying an animated graphic of a court jester blowing a raspberry[22 and 23].

Facebook members are also receiving messages from friends' hacked accounts via the social network, linking to third-party websites designed to infect the recipient's computer[24]. Hackers have found value in compromising Facebook accounts, stealing usernames and passwords, and then using the profiles as a launching pad for mass-distributing malware attacks and spam[25].

There are also third-party Facebook applications designed to present irritating pop-up adverts[26]. However, these appear to have become less of a threat since Facebook changed its user interface, making third-party applications less prominent.



Exploiting wider programs

Instead of simply looking for operating system and browser vulnerabilities to exploit, hackers are also exploring security holes in other widely used programs and tools such as Adobe Flash and PDFs.

The rise in malicious Flash and PDF files can be partly explained by the use of malware construction kits that build web attack pages incorporating booby-trapped code. The inclusion of the Flash and PDF content targets vulnerabilities that have been found in the widely used Adobe browser plug-ins, underlining the importance of keeping these up to date.

In addition, there was a 46 percent increase in the amount of kernel mode rootkits during 2008. These rootkits attempt to evade detection by traditional security products by cloaking themselves using sophisticated low-level operating system techniques.

Malware by location

Research by SophosLabs identified malware written in a total of 44 different languages, although it was not possible to extract location information on 47.9 percent of the malware samples examined.

China accounts for 11.6 percent of all malware. This is a smaller proportion than 2007 when the republic's hackers accounted for 21 percent of malicious code identified as coming from a particular region. The exact language breakdown is:

- English-speaking world – 24.5 percent
- Chinese – 11.6 percent
- German – 3.7 percent
- French – 3.1 percent
- Russian – 3.0 percent
- Brazilian Portuguese – 1.6 percent
- Other – 4.6 percent

The analysis also revealed some interesting differences in the motives and tactics used by different hacking groups around the globe.

Much of the Chinese malware takes the form of backdoor Trojans, but there is also a proportion of Chinese malware whose motive is to steal passwords from online gamers.

The majority of malicious code written in Brazil is Trojans designed to steal information from online banks. Russian hackers, meanwhile, appear to be concentrating largely on creating botnets and opening backdoors to give cybercriminals remote access to compromised computers.

A tale of three internet companies

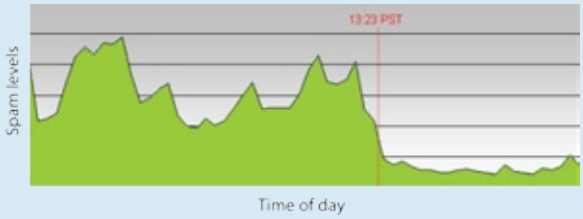
Atrivo
This Californian-based ISP (also known as Intercage) was disconnected from the internet in September after evidence was published showing that large parts of its network were being used to peddle fake anti-virus software (or scareware) and malware[27].

ESTDomains
Shortly afterwards, questions were raised about Vladimir Tsastsin, an ethnic Russian living in Estonia[28]. Tsastsin was the founder of EstDomains, a domain registrar service and, coincidentally, a customer of Atrivo. His company was accused of providing a safe harbor to criminals registering domains for malicious activity, ensuring that their activities were not shut down when EstDomains received abuse reports.

After the Estonian government pressed charges against Tsastsin for credit card fraud, money laundering and other offences, ICANN withdrew his firm's license as a domain registrar.

McColo
Another Russian-owned network, McColo was widely believed to be hosting command and control centres for five major botnets: Srizbi (Zlob), Mega-D, Rustock, Dedler and Storm.

When McColo was disconnected from the internet at 13.23 on 11 November 2008[29], the botnets went offline resulting in a huge drop in spam levels. Spam volumes plunged 75 percent[30] immediately after McColo was taken offline. Since then hackers have tried to regain control of these botnets, with some success[31].



It has been shown by these examples that the security community working together can severely disrupt cybercriminal activities on a global scale. Indeed, the takedown of McColo has had more of an impact on global spam levels (even if temporarily) than any hacker arrest by the authorities has ever achieved.

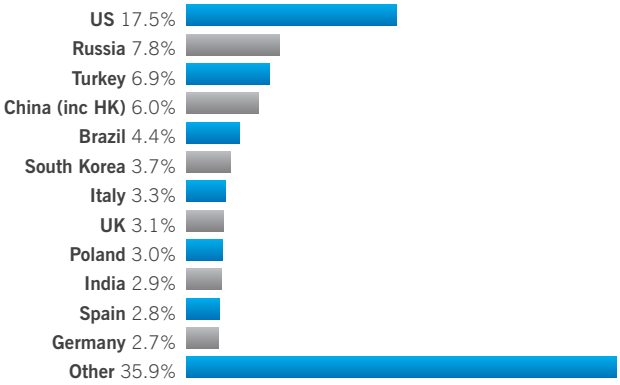
Spam

Spam still popular

Spam remains a significant problem for business, with Sophos research revealing that an incredible 97 percent of all business email is spam. Sophos receives millions of new messages every day from its global network of spam traps.

Spam by country

Spam was sent from 240 countries in 2008. The US has decreased its contribution to the spam problem, relaying 17.5 percent of all spam compared to 22.5 percent in 2007. However, it still has much work to do to tackle the problem.



Top 12 spam relaying countries for 2008

The US then is still responsible for most of the world's unwanted emails – some of which will have malware attached, or link to malicious or infected websites. Most of this spam will come from unwitting home users, whose computers are part of a botnet.

However, the botnet problem is truly global. It is clear that more computers require up-to-date anti-virus protection and the latest security patches, and that the general public needs to be better educated about how to avoid putting their personal data and computers at risk.

Are you a spammer?

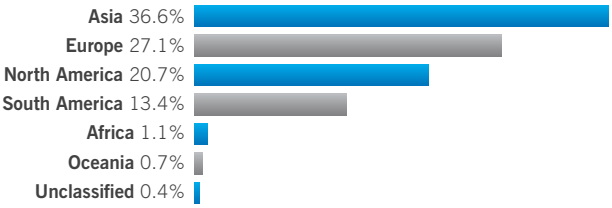
Virtually all spam comes from compromised computers (called "bots" or "zombies") that have been successfully attacked and now, unbeknown to their owners, are sending out large volumes of spam, launching distributed denial-of-service attacks, or stealing confidential information.

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

Spam by continent

Asia delivers more than one-third of all spam, and when combined with Europe accounts for almost two-thirds of the world's unwanted emails.



Spam relayed by continent in 2008

Blog spam

Spam is not just sent via email. Increasingly, internet blogs, which invite visitors to leave comments are also used, typically by automated bots that hunt for vulnerable pages.

It is estimated that over 85 percent of all submitted blog comments are in fact spam[33], although many blogs use free tools to try to filter it out before publication.

Spam and social networks

Spammers proved themselves to be unafraid of trying new methods of distributing their marketing messages and malware during 2008. Social networking websites, such as Facebook and Twitter, have increasingly popular with them.

Typically, hackers steal members' usernames and passwords and then bombard the victims' friends and family with thinly disguised marketing messages, directing them to third-party webpages.

An interesting trend has also emerged in exploiting social networks. Conmen are breaking into innocent Facebook accounts to pose as an individual. They then spam out messages to that person's friends claiming that while holidaying in a foreign city, they have been mugged and lost their wallet and return airline ticket. They then ask for funds to be wired to them via Western Union[34].

Computer users who would normally be suspicious of similar emails arriving in their regular inbox, may be more susceptible when they are communicated via Facebook from a contact they believe to be a friend. Scammers can exploit the network further by having an ongoing conversation with their intended victim, using information from the compromised account. For instance, if the owner of the hacked account has told his Facebook friends via a status message that he is traveling to a particular country, it makes the story of the mugging all the more believable.

Internet users need to become more sceptical and cynical about such messages if they are going to avoid such confidence tricks in the future.

In November 2008, Facebook was awarded US $873 million in a court judgement against a Montreal-based spammer who was said to have sent more than four million messages to its users via compromised accounts[35]. Sophos has seen an escalation in the amount of spam being sent via social networking websites and expects to see this continue to rise.

Other trends in spam

"Newsletter" spam is proving a popular method of delivery, with spammers copying the templates and design of legitimate email newsletters. Hackers also use webmail accounts like Gmail, Hotmail and Yahoo to spew spam to the world, having broken the CAPTCHA (completely automated procedure for telling computer and humans apart) system.

Apple

Mac users a soft target

The Apple malware problem is tiny compared to the situation for Windows users. However, since the emergence of the first financially motivated malware for Mac OS X in late 2007 there have been more attempts by hackers to infect Mac computers.

In February 2008, a new Flash-based Trojan, Troj/Gida-B[36], was designed to scare users into purchasing bogus security software. This scareware attack used poisoned web adverts that worked equally well on Mac and Windows computers.

The OSX/Hovdy-A Trojan[37], discovered in June 2008, is also capable of infecting Mac OS X computers and attempts to steal passwords, open firewalls and disable security settings. It takes advantage of the ARDAgent vulnerability in Mac OS X to gain root access. Once a computer has been infected the hacker can gain complete control and cover their tracks by disabling system logging.

In August 2008, Troj/RKOSX-A[38], a Mac OS X tool to assist hackers create backdoor Trojans, was discovered. Three months later, Sophos announced the discovery of a new piece of Mac malware being planted on websites – OSX/Jahlav-A[39]. This Trojan poses as a legitimate application, but after installation downloads additional components from a server in the Netherlands.

Although there is less Mac malware around, there are several reasons why Mac users should be wary.

- A high level of complacency in the Mac community means many users incorrectly believe they are immune from internet security threats. This makes them a soft target for future attacks.
- The use of Intel-based chips in Apple Mac hardware has made use of Windows on Macs more common. This makes Macs more likely than before to be harboring and spreading Windows malware.
- 2008 saw record sales of Apple Mac computers[40], with some users undoubtedly switching from PCs due to disgruntlement with Windows Vista. As the marketshare for Apple Macs increases, Mac users are likely to see more attacks launched against them.

With so many Windows home users seemingly incapable of properly defending themselves against malware and spyware, it seems sensible to suggest that some of them should consider switching to the Apple Mac platform. This is not because Mac OS X is superior, but simply because there is significantly less malware currently being written for it. Cybercriminals looking to maximize their return are likely to stick mostly to attacking Windows computers for the foreseeable future.

However, malware aimed at Macs will continue to be written, and users should continue to follow safe computing best practices such as running an anti-virus product and keeping up-to-date with security patches.

Mobile phones and Wi-Fi devices

Security flaws in smartphones

To great fanfare, 2008 saw the launch of the 3G version of the Apple iPhone, and the first phone to use the Google Android mobile operating system.

Apple iPhone

There is no disputing that the 3G version of the iPhone is more attractive to business and internet users than its predecessor owing to its superior connectivity and cheaper price point. In its most recent set of financial results, Apple reported that its iPhone was outselling RIM's popular Blackberry device[41].

Apple's increased market share, however, may in turn herald more concerted attempts by criminals to take advantage of their devices in future.

Although simple malware has already been seen, the iPhone has not yet been the target of a significant attack. However, security flaws have been found in Apple's mobile email application and its Safari web browser, and the company has been criticized for not patching these flaws at the same time as its other computers running Mac OS X.

iPhone users should also be aware that they may be more vulnerable to phishing attacks than their desktop counterparts because:

- They have to enter URLs via the touch-sensitive screen, and may be more willing to just click on email links.
- The iPhone version of Safari does not display URLs that are embedded in emails before they are clicked on. It is therefore harder for users to tell if the link leads, for example, to a bogus banking website.
- The iPhone's browser only displays partial URLs in its address bar, making it far easier for cybercriminals to fool users into believing they are on a legitimate website.

Google Android

At the time of writing the only mobile phone on the market that uses the Google Android operating system is the T-Mobile G1, giving hackers their first real look at its operating system. Although early reviews have typically concentrated on its cosmetic differences to the Apple iPhone (such as a slide-out keyboard and less flexible touch screen), a security vulnerability in the G1's web browser was rapidly discovered[42].

Concerns have also been raised that Google's "open" attitude to applications may mean malicious programs can be distributed amongst its phone's users far more easily.

Sophos believes that early examples of malware for these operating systems are likely to be written by enthusiasts with a desire to make headlines, rather than financially-motivated criminals. However, as millions more people purchase them, creating mobile phone threats will become increasingly attractive for the criminally minded. One example could be the creation of a generic Mac OS X attack, which could threaten the common features and technology of the Mac computer and iPhone[43].

Similarly, it would not be a surprise to see experimental attacks against Google Android users.

Such attacks are likely to rely upon social engineering – rather than software vulnerabilities – to fool users into running dangerous code. As such, mobile phone owners who are in the habit of adding third-party applications without caution will be increasing their chances of infecting their device.

Data leakage

Unsafe data

Data leakage filled the headlines in 2008 as corporations and government proved themselves to be lax in protecting their confidential data[44].

Organizations of all sizes are finding that today's mobile and collaborative workforce needs access to information inside and outside the office, along with the ability to share data with co-workers and partners.

Users are routinely using and sharing data without giving thought to confidentiality and regulatory requirements. Almost 30 percent store contract and financial data, customer information, sales targets, contact details and personal account data on removable media[45]. This has led to numerous incidents of data loss that are often accidental rather than malicious.

Used hardware

A number of incidents were reported of confidential data ending up in the public domain after old computer hardware, which had not been securely erased, was sold on auction sites like eBay[46].

This has led some observers to suggest that there is a higher demand (and thus higher price offered) for used hard drives on eBay than for brand new ones. This is unsurprising, considering the amount of confidential information that is potentially recoverable[47].

Encryption

The most important step in stopping data leakage is to encrypt sensitive information, laptops, removable storage devices and email. If data is encrypted with a password it cannot be deciphered or used unless the password is known. This means that even if all other security measures fail to prevent a hacker from accessing your most sensitive data, they will not be able to read it and so compromise the integrity of your information.

Data loss is big money

In August 2008 US authorities charged 11 men with being involved in a hack that stole more than 40 million credit and debit card numbers. The retailers affected included OfficeMax, Barnes & Noble, Boston Market, and TJX, which operates retail stores TJ Maxx (known as TK Maxx in the UK) and Marshall's.

According to the Secret Service and Department of Justice, the "wardriving" gang (driving through an area in search of insecure wireless corporate networks to hack) installed malicious programs and then sold the stolen information to other criminals in the US and Eastern Europe. Tens of thousands of dollars were then illegally withdrawn from ATMs using forged credit cards.

In another incident, the British Home Office confirmed that a USB memory stick containing the unencrypted personal details of some 130,000 convicted criminals had gone missing. Information included names, addresses, dates of birth and, in some instances, prisoners' release dates. The USB stick was being used by external contractor PA Consulting, which as a result, lost a £1.5 million contract with the British government.

The second step is controlling how users treat information. You want to stop any risky behavior, such as transferring unencrypted information onto USB sticks. Organizations should extend their anti-malware infrastructure in order to:

- Control the use of information.
- Guarantee efficient operations.
- Ensure that they meet regulatory requirements.

With the possibility of mounting job losses in 2009, organizations should also be careful to ensure that devices used by departing workers are properly encrypted or securely wiped. Furthermore, the potential risk of disgruntled employees leaving with data or undertaking competitive espionage must also be considered.

State-sponsored cybercrime

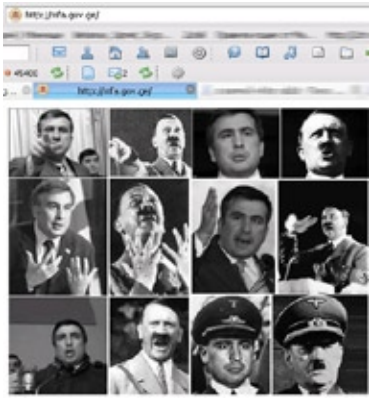
Digital espionage increasing

Countries spy on each other for political, commercial and military advantage and it would be naive to think they do not take advantage of computers and the internet to help them do so.

During 2007 it became common for countries to openly accuse each other of engaging in spying via the internet, such as the Chinese military being blamed for a cyberattack on a Pentagon computer system in September of that year[48], for example. Concern about state-sponsored cybercrime climaxed at the end of 2007 with the discovery that MI5, the British Security Service, had written to 300 chief executives and security chiefs at UK companies warning them of the "electronic espionage attack".

2008 saw even more reports of alleged government-sponsored cybercrime. Even though it can be extraordinarily difficult to prove an attack has been endorsed by a state, 2009 is likely to bring more claims of countries attacking and spying on each other via the internet.

- **April 2008.** *Der Spiegel* reported that the BND – Germany's foreign intelligence service – used spyware to monitor the Ministry of Commerce and Industry in Afghanistan[49]. Confidential documents, passwords and email communications were reportedly compromised by German spies, and sent to the BND's headquarters. This news followed revelations that the BND had intercepted emails between *Spiegel* journalist Susanne Koelbl and Afghanistan's Commerce Minister Amin Farhang, resulting in a diplomatic row between the countries.
- **May 2008.** Senior Indian government officials in New Delhi were said to have confirmed that Chinese hackers targeted the Ministry of External Affairs and the National Informatics Centre[50], which provides the network backbone for central and state government, as well as other administrative bodies in India. The unnamed officials were quoted as saying that this was China's way of gaining "an asymmetrical advantage" over a potential adversary.
- **May 2008.** Belgium also accused the Chinese government of cyber-espionage, claiming that hacking attacks against the Belgian Federal Government had originated in China, and were likely to have been at the behest of the Beijing government[51]. Separately, the Belgian Minister of Foreign Affairs told parliament that his ministry had been the subject of cyber-espionage by Chinese agents several weeks before.
- **August 2008.** As tensions rose over South Ossetia, Russian and Georgian hackers launched attacks against each other[52]. Examples include a distributed denial of service attack against the website of the South Ossetian government and the defacement of the Georgian Ministry of Foreign Affairs website with a collage of pictures of Georgian president Mikheil Saakashvili and Adolf Hitler[53].



- **September 2008.** Seoul accused its adversaries in North Korea of stealing documents from military officers through the use of spyware and a female agent[54]. The spyware attack took the form of a malicious email attachment designed to steal documents from infected computers. The email addresses were supplied by 35-year-old Won Jeong Hwa.

Arrests and the law

Behind bars

With international computer crime authorities uniting to tackle cybercriminals, the past twelve months have seen more arrests and harsher sentences for criminals involved in high-profile and financially rewarding computer crimes.

Below are just some of the cases that made the news in 2008.

- **January 2008**. Three men who constructed an elaborate email scam pleaded guilty in a New York court to stealing more than $1.2 million[55]. The men sent emails that claimed to come from a victim of terminal throat cancer who wanted to distribute $55 million to charity. One of the gang, Nnamdi Chizuba Ainsiobi, is then said to have telephoned recipients, disguising his voice to pretend he was that suffering from the disease.
- **February 2008**. An American teenager pleaded guilty to seizing control of hundreds of thousands of zombie computers and using them to display cash-generating adverts[56]. Some of the compromised computers were based at the Weapons Division of the US Naval Air Warfare Center and the US Department of Defense.

- **March 2008**. A Chinese court handed out jail sentences of between six and a half to eight years to four men who used a Trojan to steal internet bank account information[57].
- **April 2008**. An Israeli court jailed three members of the Modi'in Ezrahi private investigation firm after they were found guilty of using a Trojan to steal commercial information[58].
- **May 2008**. Authorities in the US and Romania charged a total of 38 people suspected of running an international crime ring that targeted hundreds of financial institutions through phishing emails and SMS text messages[59].
- **June 2008**. 19-year-old Jason Michael Milmont admitted to being the programmer of the Nugache malware that infected Windows computers[60]. The malware turned the computers into a sophisticated peer-to-peer (P2P)-controlled botnet that contained 5,000 to 15,000 compromised computers at any one time. Milmont used stolen bank information to access accounts and buy goods.
- **July 2008.** A federal court in Manhattan sentenced 17-year-old Adam Vitale to 30 months in prison for sending out more than 1.2 million spam messages in less than a week[61]. Vitale was looking for a share of the profits made from selling goods via the messages.
- **August 2008.** Dutch authorities apprehended Leni de Abreu Neto, following assistance from the FBI and the Brazilian Federal Police[62]. The 35-year-old Brazilian allegedly ran and leased access to a botnet that comprised 100,000 computers.
- **September 2008**. A gang of alleged credit card data thieves, said to have stolen CDN $1.8 million (approximately US $1.69 million) from a company in Calgary, were arrested by police in Canada[63]. One of the arrested men was Ehud "The Analyzer" Tenenbaum who had been caught illegally accessing Pentagon computers 10 years earlier.
- **October 2008**. The Federal Trade Commission (FTC) convinced a court to shut down a group suspected of being a major international spam operation[64]. The FTC claimed to have received over three million complaints from computer users who had received emails connected with the spam campaign, many of them offering what was described as a "100 percent safe and natural herbal" male enhancement pill.
- **November 2008**. A US court ordered CyberSpy Software LLC to stop selling its RemoteSpy keylogging software while the FTC investigates whether it is being used to break the law[65]. In December the ban was overturned[66].

The future

Growth in complexity of attacks

Predicting the future in such a rapidly evolving environment is near impossible. One only needs to count the rate at which new malware appears today compared to five years ago to see how quickly the threat has become more serious.

Some things do seem certain however:

- **The variety of attacks** and their number will continue to escalate, driven by organized crime's desire to break into computers to steal information, identities and resources.
- **Data leakage** will become an ever-larger concern, especially with the increasing use of mobile technologies. Many countries have introduced strict disclosure laws, or will soon do so. These laws are aimed at stopping companies from sweeping security breaches under the carpet. Even a very restricted data breach, once disclosed, may affect overall trust in an organization's products and services.

- **Compromised PCs**, both at home and at work, will continue to remain the primary source of spam. With many botnets adopting a decentralized, P2P-style of operation, quick wins such as the success of taking down the botnet command-and-control centers hosted by provider McColo will become harder to achieve.
- **Web insecurity**, notably weakness against automated remote attacks such as SQL injections, will continue to be the primary way of distributing web-borne malware. Cybercriminals can then send innocent-looking spam which link to legitimate, but hacked, webpages. These hacked sites link invisibly to malicious content.
- **Malicious emails** will include an increasing proportion of attachments or web links to non-program (non-EXE) files. These will be legitimate-looking data files, such as Word DOCs and PDFs, that are booby-trapped with exploits against software vulnerabilities. Viewing these files, which would be harmless on a patched computer, could lead to an invisible disaster on an unpatched one.
- **Identity theft** will continue to adversely affect customer loyalty. In the year ahead, companies must assure their customers that proper and thorough security measures have been taken so that the risk of a breach is minimal.

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 occur far into the future because of human mistakes.

However, if managed properly, the problem should not be insurmountable. 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/pressoffice/news/articles/2008/02/poisoned-adverts.html
2. www.sophos.com/pressoffice/news/articles/2008/03/euro2008.html
3. www.sophos.com/security/blog/2008/03/1186.html
4. www.sophos.com/security/blog/2008/04/1292.html
5. www.sophos.com/pressoffice/news/articles/2008/06/infected-tennis-sites.html
6. www.sophos.com/pressoffice/news/articles/2008/07/playstation.html
7. www.sophos.com/blogs/gc/g/2008/09/15/hackers-infect-businessweek-website-via-sql-injection-attack/
8. www.sophos.com/pressoffice/news/articles/2008/10/adobe-infection.html
9. www.sophos.com/security/sophoslabs/anonymizing-proxies.html
10. www.sophos.com/security/blog/2008/08/1685.html
11. www.sophos.com/blogs/gc/g/2008/09/17/hackers-distribute-trojan-as-iphone-game/
12. www.sophos.com/blogs/gc/g/2008/10/13/malicious-microsoft-security-patch-spammed-out-before-patch-tuesday/
13. www.sophos.com/pressoffice/news/articles/2008/07/security-report.html
14. www.sophos.com/pressoffice/news/articles/2004/03/va_bagelnetsky.html
15. www.sophos.com/blogs/gc/g/2008/08/07/exposed-cnn-top-ten-video-malware/
16. www.sophos.com/blogs/gc/g/2008/11/05/the-president-elects-first-malware-campaign/
17. www.sophos.com/blogs/gc/g/2008/09/10/barack-obama-sex-video-malware-campaign/
18. www.sophos.com/blogs/gc/g/2008/09/23/free-norton-antivirus-hackers-disguise-fake-product-to-spread-trojan/
19. www.sophos.com/pressoffice/news/articles/2008/03/lee-shin-ja.html
20. www.sophos.com/pressoffice/news/articles/2008/02/poisoned-adverts.html
21. www.sophos.com/blogs/gc/g/2008/08/27/computer-worm-strikes-international-space-station/
22. www.sophos.com/blogs/gc/g/2008/08/08/up-to-1800-profiles-hit-by-malware-attack-says-facebook/
23. www.sophos.com/blogs/gc/g/2008/08/07/more-malicious-links-seen-on-facebook/
24. www.sophos.com/blogs/gc/g/2008/08/04/facebook-and-myspace-malware/
25. www.sophos.com/blogs/gc/g/2008/09/17/facebook-malware-is-a-real-threat/
26. www.sophos.com/pressoffice/news/articles/2008/01/facebook-adware.html
27. voices.washingtonpost.com/securityfix/2008/09/internet_shuns_us_based_isp_am.html
28. voices.washingtonpost.com/securityfix/2008/10/icann_de-accredits_estdomains.html
29. www.sophos.com/security/blog/2008/11/1970.html
30. voices.washingtonpost.com/securityfix/2008/11/the_badness_that_was_mccolo.html
31. www.sophos.com/security/blog/2008/11/2028.html
32. www.sophos.com/products/enterprise/alert-services/zombiealert.html
33. akismet.com/stats
34. www.sophos.com/blogs/gc/g/2008/11/10/facebook-friend-stranded-in-nigeria-would-you-rescue-them/
35. www.sophos.com/blogs/gc/g/2008/11/25/facebook-takes-on-spammer-and-wins-873-million/
36. www.sophos.com/pressoffice/news/articles/2008/02/poisoned-adverts.html
37. www.sophos.com/pressoffice/news/articles/2008/06/machovdyA.html
38. www.sophos.com/security/blog/2008/11/1999.html
39. www.sophos.com/security/blog/2008/11/2024.html
40. www.apple.com/pr/library/2008/10/21results.html
41. www.apple.com/pr/library/2008/10/21results.html
42. www.nytimes.com/2008/10/25/technology/internet/25phone.html
43. www.sophos.com/blogs/gc/g/2008/11/03/guest-blog-will-hackers-make-the-iphone-an-iph0wn/
44. www.sophos.com/blogs/gc/g/category/data-leakage/
45. Utimaco Removable Media survey, 2007.

46. www.sophos.com/blogs/gc/g/2008/09/30/who-needs-to-steal-data-when-you-can-buy-it-on-ebay/
47. www.sophos.com/blogs/gc/g/2008/08/26/are-your-bank-details-being-sold-on-ebay/
48. www.sophos.com/pressoffice/news/articles/2007/09/chinese-hack.html
49. www.sophos.com/blogs/gc/g/2008/04/28/german-spooks-deploy-spyware-against-afghan-ministry/
50. www.sophos.com/blogs/gc/g/2008/05/09/china-crisis-now-india-claims-hackers-are-attacking-it-from-behind-the-bamboo-curtain/
51. www.sophos.com/pressoffice/news/articles/2008/05/belgium.html
52. www.sophos.com/blogs/gc/g/2008/08/12/update-on-website-attacks-in-georgia-and-russia/
53. www.sophos.com/blogs/gc/g/2008/08/12/conflict-between-russia-and-georgia-turns-to-cyber-warfare/
54. www.sophos.com/blogs/gc/g/2008/09/02/sex-spyware-and-north-and-south-korea/
55. www.sophos.com/news/2008/01/nigerian-scam.html
56. www.sophos.com/news/2008/02/sobe.html
57. www.sophos.com/news/2008/03/zhang.html
58. www.sophos.com/blogs/gc/g/2008/04/29/i-spy-with-my-private-eye
59. www.sophos.com/news/2008/05/phishing-gang.html
60. www.sophos.com/news/2008/06/milmont.html
61. www.sophos.com/blogs/gc/g/2008/07/16/30-months-of-bread-and-water-for-spammer/
62. www.sophos.com/blogs/gc/g/2008/08/22/brazilian-charged-with-selling-access-to-100000-pc-botnet/
63. www.sophos.com/blogs/gc/g/2008/09/05/gang-arrested-in-canada-for-alleged-credit-card-data-heist/
64. www.sophos.com/blogs/gc/g/2008/10/14/ftc-shuts-down-major-international-spam-operation/
65. www.sophos.com/blogs/gc/g/2008/11/18/court-orders-company-to-stop-selling-spyware/
66. www.prweb.com/releases/spy/software/prweb1706254.htm

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

Boston, USA | Oxford, UK

tr/081208

SOPHOS
WWW.SOPHOS.COM