SOPHOS

Security threat report: July 2009 update

Overview

When a Word document was posted to the alt.sex usenet news group on March 26, 1999, many people probably assumed the file was harmless, and were all too eager to open the file and access the passwords for pornographic websites.

This trigger led to the Melissa virus spreading like wildfire via email, exploiting the macro language built into Microsoft Word.

Melissa was certainly a big deal at the time, but ten years on, malware has become more insidious, turning unpatched PCs into vectors for malicious and financially-motivated activity.

Today, most companies have guarded their email gateways and broadened their defenses against email-borne malware and malicious spam. Consequently, cybercriminals are developing techniques to infect machines behind-the-scenes by embedding malicious code on innocent websites and luring victims to them.

2009 has proven attacks are continuing to broaden. While the number of web-based attacks outweighs the attacks through email, financially motivated cybercriminals are turning their attention to Web 2.0 platforms such as Facebook and Twitter and alternative programs and tools such as Adobe Flash and PDFs.

Businesses adopting new technologies, and workers bringing software and devices into the workplace to facilitate communication and information-gathering, are giving hackers new opportunities for exploitation.

Sophos receives 39,726 unique suspicious files every day – accounting for 28 unique files every minute, 24 hours a day. Independent testing agency, AV-Test.org, currently counts over 22.5 million unique samples of malware in its collection – compared to 12.3 million in June 2008, demonstrating that the scale of the problem has almost doubled.

Six Months at a Glance

23,500 new infected webpages are discovered every day. That's one every 3.6 seconds, 4 times worse than what it was in the same period in 2008.

The US hosts more malware, relays more spam than any other country.

40,000 new suspicious files are examined by SophosLabs every day.

22.5 million different samples of malware in the collection of independent testing agency, AV-Test.org

15 new bogus anti-virus vendor websites are discovered every day. This number has tripled, up from an average of five detected per day, during 2008.

89.7 percent of all business email is spam.

Approximately 6,500 new spam-related websites are discovered every day - accounting for one new website every 13 seconds, 24 hours a day. This figure is almost double what it was in the same period in 2008.

source: SophosLabs

It's clear that the global criminal operation has reached such a level that it's a true "conveyor belt of crime". Businesses are continuing to face a challenging threat landscape.
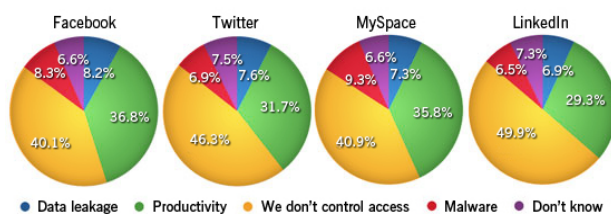
Web 2.0 and social networking

A battleground for malware

Increasing worker productivity has always been a top priority for most organizations. It was also the initial driver to control access to social networks. Sites like Facebook were quickly identified as a procrastinator's paradise, with some firms determining that their workers were not only spending more time using the site than any other but also using excessive bandwidth.

Organizations have become increasingly concerned about malicious attacks originating from social networking sites, as well as the risks of users revealing sensitive personal or corporate data online.

**What is your primary reason for controlling access?**

source: Sophos research

Sophos research reveals two thirds of businesses fear that social networking endangers corporate security[1].

Research findings also revealed that 63 percent of system administrators worry that employees share too much personal information via their social networking sites, putting their corporate infrastructure - and the sensitive data stored on it — at risk[2].

Evidence shows that their worry is justified. In June 2009, the personal information belonging to the incoming head of MI6 was exposed to the entire Facebook network, when his spouse allowed members of the "London" network to view her profile[3].

Have you, or any of your colleagues, ever been...
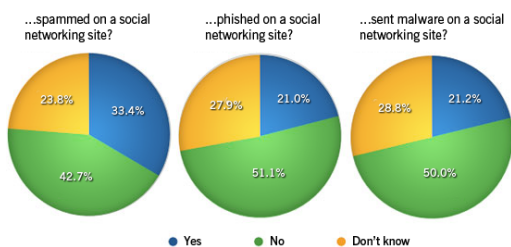
source: Sophos research

The same research findings also indicate that a quarter of businesses have been the victim of spam, phishing or malware attacks via sites like Twitter, Facebook, LinkedIn and MySpace.

Here is a sample of some of the social networking attacks Sophos has discovered in the past six months:

- **January** Twitter users received direct messages from their online followers enticing them to visit a phishing website [4]which attempted to steal their username and password.

Direct messaging enticed Twitter members to phishing website

- **January** Sophos learned of a Facebook scam[5] which usurped user accounts and attempted to derive sensitive information from Facebook users' friends and family.

- **January** MySpace user Shane Symington, lost over US$210,000 in an email scam[6]. The postman was weaseled out of money when his Nigerian cyber-pal started asking for money to help her ailing mother. In actuality, the woman, and the FBI investigation that followed, was an elaborate hoax designed to take advantage of a Good Samaritan.

- **April** Two cross-site scripting attacks crafted by 17 year-old Mikeyy Mooney, were inflicted on Twitter users[7]. These XSS attacks attempted to load a remote highly-obfuscated script from a third-party website and take over the profiles of unsuspecting users.
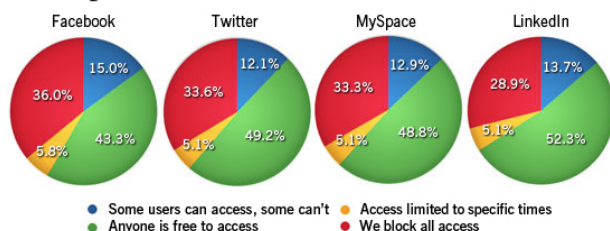
- **May** A French hacker broke into Twitter's internal administration systems[8], gaining access to Twitter users' accounts. Users known to have been affected by the hacker's subsequent actions include Barack Obama, Britney Spears, Ashton Kutcher and Lily Allen.
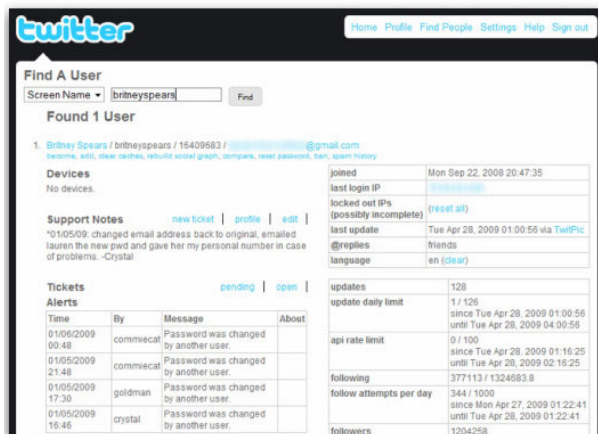
- **May** Hundreds of accounts on the Twitter micro-blogging service were hacked by Acai Berry weight loss spammers[9], emphasizing the need for better password security.

- **June** Hackers gained access to British politician Michael Fabricant's [10] Facebook username and password, sending messages to 1500 of his friends which pointed them to a malicious webpage.

To combat the growing problem of Web 2.0 threats, Sophos has discovered that approximately 50% of companies are blocking all or some access to social networks[11].

But by completely denying access to their favorite social networking site, organizations will drive their employees to find a way round the ban, creating even greater holes in corporate defenses. This will inevitably lead to IT teams having less visibility on their users' activities.

Social networks are here to stay, and as they can bring business benefits as well as risks, it is better to ensure that users can participate in social networks sensibly and safely rather than banning them from taking part at all.

To protect users, corporations should run web security solutions that check every link and webpage as it is clicked on, to see if it contains malware or suspicious activity. Companies should also:

- Educate their workforce about online risks — make sure all employees are aware of the impact that their actions could have on the corporate network

- Consider allowing access to popular social networking sites only at specific times, e.g. to Facebook over lunch

- Check the information that the organization and staff share online — if sensitive business data is being shared, evaluate the situation and act as appropriate

- Apply multi-layered security at both the gateway and at the endpoint

How does your company control access to the following sites?

source: Sophos research

Data leakage

Unprotected data

Data leakage remains a top concern in 2009, with scandals continuing to dominate the headlines. Many corporations and government institutions have failed to protect their confidential information — including the identities of their workforce, customers and general public.

It is not only the threat of negative publicity which is driving interest in data protection, but also concern that the organization is failing to meet compliance with regulatory security standards.

A variety of techniques are being used by corporations around the world to prevent data loss in a mobile connected world. These include anti-virus software, encryption and firewalls, access control, written policies and improved employee training.

Nevertheless, users are routinely using and sharing data without giving enough thought to confidentiality and regulatory requirements. This has led to numerous incidents of data loss in the first six months of 2009 - some accidental, some malicious:

- **May** Hackers broke into a Virginia government website, stealing the details of almost 8.3 million patients, and threatening to auction them to the highest bidder.[12]

- **May** The theft of a single laptop in the UK put the personal identities of 109,000 pension holders at risk. The laptop contained names, addresses, dates of birth, National Insurance numbers, employer names, salary details and bank account information[13].

- **June** 530,000 Viriginia patients were individually notified that their SSNs had potentially been exposed after a hacker gained access to the Virginia Prescription Monitoring Program [14].

- **June** Authorities arrested a former Goldman Sachs employee who uploaded the company's secret source code to an FTP server based in Germany[15].

Encryption

The most important step in stopping data leakage is to encrypt sensitive information, laptops, and removable storage devices. 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 confidentiality of your information.

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

- Protect data in motion and data in use

- Guarantee efficient operations.

- Ensure that they meet regulatory requirements.

In this current economic climate, firms should be careful to ensure that the devices of departing workers are properly encrypted or securely wiped.

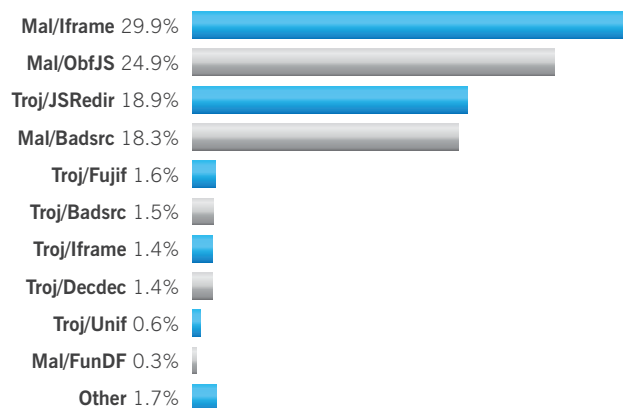A stolen laptop put 109,000 pension holders at risk

Web threats

Exploiting legitimate websites

The web remains a major vehicle for cybercriminals looking to infect computers around the world.

The vast majority of infected websites are in fact legitimate sites that have been hacked to carry malicious code, or more commonly, scripts that then download further malicious scripts from third-party websites. Users visiting the websites may be infected by simply visiting affected webpages, or be fooled into downloading malicious code onto their computer.

The scope of these attacks cannot be underestimated, since all types of sites — from government departments and educational establishments to embassies and political parties to websites devoted to high-tech gadgets and online programming communities have been targeted.

Top 10 web-based malware threats

Mal/Iframe 29.9%
Mal/ObfJS 24.9%
Troj/JSRedir 18.9%
Mal/Badsrc 18.3%
Troj/Fujif 1.6%
Troj/Badsrc 1.5%
Troj/Iframe 1.4%
Troj/Decdec 1.4%
Troj/Unif 0.6%
Mal/FunDF 0.3%
Other 1.7%

source: SophosLabs

The most significant entry in this chart is Troj/JSRedir. Despite its arrival only in late April, it was discovered on many thousands of websites. For instance, in just one week in May it was reported to have infected six times more webpages than any other malware." [16]

However many well-known and reputable sites have fallen victim to these kinds of attacks, emphasizing the need for all organizations, both large and small, to properly defend their websites.

The following is just a tiny sample of the affected websites around the world which have fallen victim to a malicious attack during the first six months of 2009:

- **January** Multiple sites, including a social networking site for ex-service men in the UK, suffered an SQL attack and were infected with malicious code[17].

- **January** The Indian embassy in Spain fell victim to a Mal/IFrame-F attack[18].

- **January** Sophos discovered that Pravda.ru, the website of the famous Russian news service, was compromised and served up malicious content, Mal/Iframe-F[19].

- **March** The Embassy of Ethopia in Washington D.C. fell victim to an Iframe attack[20].

- **April** Paul McCartney's website was hacked[21], falling foul of an obfuscated JavaScript designed to spy on computer users when they went banking online.

- **May** Sophos discovered that obfuscated JavaScript was being injected into sites that host the unsavory "2 Girls 1 Cup" viral video[22]. The malware attempted to redirect the user to another domain hosting a malicious payload.

- **June** The Communist Party of Britain website was infected with Mal/Iframe-F[23]. The obfuscated code pointed to a malicious website in China that spoofs Google.

SQL injection attacks

One of the reasons the web is so popular with attackers is that innocent sites that users would naturally trust can be compromised and used to infect large numbers of victims. However, it is not just the unsuspecting visitor who suffers — the website owner does as well.

This is particularly apparent with SQL injection attacks which exploit security vulnerabilities and insert malicious code (in this case script tags) into the database running a website. The attack works when user input, for instance on a web form, is not correctly filtered or checked and unexpectedly executes as code, peppering the database with malicious instructions. Recovery can be painful, and there are numerous cases of website owners cleaning up their database only to be hit again a few hours later.
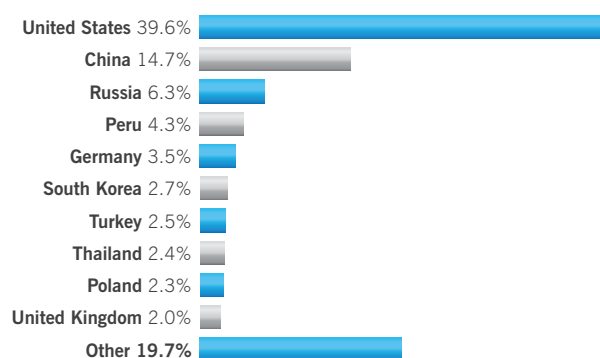
The best solution is prevention[24]. Developing and abiding by best practices can minimize the chance of future attacks[25].

Malicious links

Aside from SQL injection, hackers continue to use automated systems to post malicious links into the comment sections of blogs and web forums, and use free web-hosting services to create their own sites carrying malware because new pages are trivial to set up without requiring identification.

Hackers also keep on developing automated tools that use search engines such as Google to identify potentially vulnerable websites, and then inject code into their servers. As a result, websites are rarely specifically targeted to carry malware, and are often simply unfortunate enough to have been discovered by the cybercriminals' malware distribution tool.

Top 10 countries hosting malware on the web

Country	%
United States	39.6%
China	14.7%
Russia	6.3%
Peru	4.3%
Germany	3.5%
South Korea	2.7%
Turkey	2.5%
Thailand	2.4%
Poland	2.3%
United Kingdom	2.0%
Other	19.7%

source: SophosLabs

User resistance to web security

Although web security is designed to protect users from 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, blocking access to particular sites for policy reasons. For instance, companies may choose to block access to social networking or video websites for productivity or privacy reasons.

Some users have responded to web filtering by using technology such as anonymizing proxies[26].

Anonymizing proxies disguise the true nature of a website in order to trick an organization's web filter into allowing inappropriate or blocked content.

Perhaps the most high profile use of anonymizing proxies recently was seen in Iran in June 2009, where citizens attempting to avoid their government's censorship of the internet made use of the technology[27].

Supporters outside Iran even posted details of anonymizing proxies on social networks like Twitter and Facebook to assist Iranians trying to find out what the outside world was reporting.

However, anonymous proxies are not just used for political reasons — office workers can also use them in order to bypass company policies and perimeter defences.

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 individual or small group. This makes it easy for users to access an anonymizing proxy, but difficult and time consuming for administrators to track and block them.

Malware chart rundown

The chart showing which countries contain the most malware-hosting webpages reveals some interesting changes:

- The proportion of the world's malware hosted in China has halved from 31.3% in the first period of 2008, to 14.7% today. However, it's worth remembering that during the same period the volume of infected webpages detected by Sophos quadrupled around the globe.

- Peru's significant contribution to the problem was due in a large part to a massive number of webpages that were determinined to have been compromised by Mal/iFrame-F.

It is worth noting that although websites may be carrying malware, it does not necessarily mean that the hackers are based in the same country as the affected site. Hackers abuse websites worldwide in their attempt to spread malware.

If employees are using anonymizing proxies, then in addition to bypassing URL filtering, they are also circumventing content scanning at the perimeter. This can obviously have an impact on security.

Sophos has even identified anonymizing proxies that are themselves infected with multiple pieces of malware. It's not possible to tell whether the anonymizing proxies are the innocent victims of infection, or have been set up knowingly with malware embedded inside them to compromise any computers making use of them.

Further research by SophosLabs reveals the use of anonymizing proxies appears to be particularly prevalent in some educational establishments, where tech-savvy students attempt to subvert acceptable use policies.

Sophos actively tracks internet forums to discover new anonymizing proxy services to block, and incorporates real-time detection of private anonymizing proxies through traffic inspection in its web security appliance.
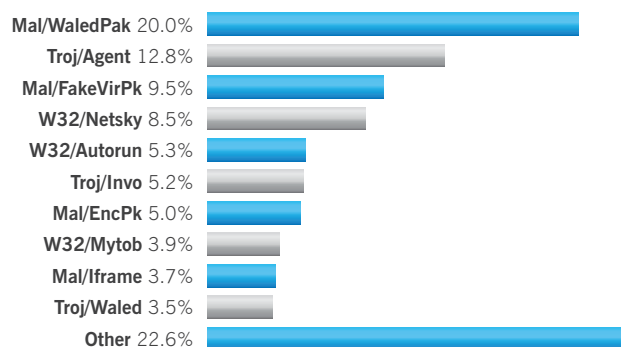
Email threats

A cause for concern

Although web-based threats have tended to dominate the malware agenda in the first six months of 2009, the number of threats distributed via email remains a cause for concern.

Aside from using malicious email attachments, cybercriminals regularly embed malicious links in emails to dangerous websites and find spam out creative attacks designed to lure curious users.

Top 10 email attachment malware Jan. –June 2009

Mal/WaledPak 20.0%
Troj/Agent 12.8%
Mal/FakeVirPk 9.5%
W32/Netsky 8.5%
W32/Autorun 5.3%
Troj/Invo 5.2%
Mal/EncPk 5.0%
W32/Mytob 3.9%
Mal/Iframe 3.7%
Troj/Waled 3.5%
Other 22.6%

source: SophosLabs

WaledPak's control of the email attachment malware chart — accounting for 20% of all reports in the first six months of 2009 — is significant as it first surfaced in late December 2008. It has since used several disguises to propagate.

- **January** On the eve of Obama's inauguration, Sophos discovered a malicious spam campaign that posed as news that Barack Obama was refusing to be the President of the United States[28]. Each email led unsuspecting users to a malicious webpage that
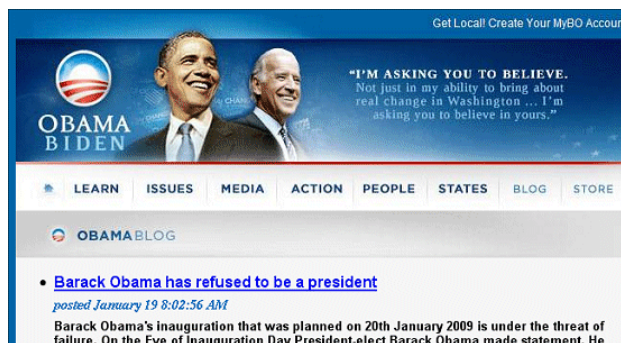

WaledPak disguised as bogus news about President Obama

infected Windows PCs with WaledPak.

- **March** Hackers distributed emails posing as breaking news from a Reuters-related site of a bomb blast in your city[29]. Each email contained a link to a webpage that installed malicious code, and video footage, which actually downloaded WaledPak.

However, while not topping the chart, many of the other viruses listed have spread during the first half of the year.

- **March** Sophos warned of a new malware campaign that affected members of Classmates and FriendsReunited[30]. Each email enticed users to click on links to view a video an imminent school reunion, but instead took them to a malicious webpage that infected their Windows PC with a malicious Trojan horse.
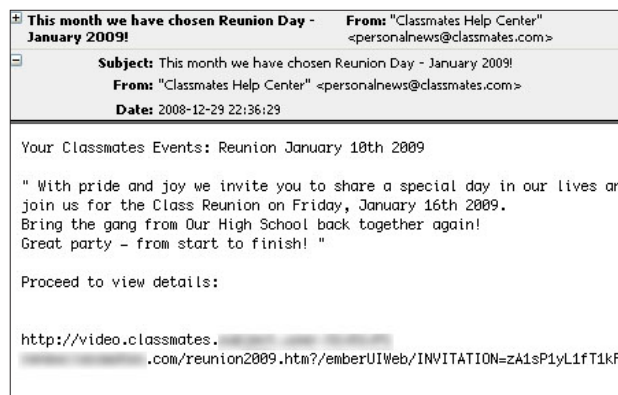
Web-based malware affected members of Classmates

- **May** One variant from the second most prevalent family of malware, Troj/Agent-JUC, posed as communications from WorldPay[31] claiming that your credit card has been charged on behalf of Amazon. When the user clicked on the attached file, Troj/Agent-JUC infected your machine.

- **June** Sophos intercepted a widespread attack by hackers who distributed Mal/FakeVirPk by posing as an electronic greeting card from a family member[32]. When the email recipient opened the greeting card, the malicious executable file would run.

- **June** An email was widely circulated containing a link to what was said to be a pornographic movie the recipient had recently featured in[33]. However, when the user clicked out of curiosity on the link, they would be directed to site that infected their PC with malicious spyware.

Spam

Spam still significant threat

Spam remains a considerable problem for business, with Sophos research revealing that 89.7 percent of all business email is spam. Sophos also identifies approximately 6,500 new spam-related webpages every day — that's one new website every 13 seconds, 24 hours a day. This figure has almost doubled from what it was in the same period of 2008 (1 every 20 seconds).

While the first ever spam message was sent over 30 years ago[34], spammers are constantly creating new web domains in an attempt to avoid detection by rudimentary security solutions that rely solely on a blacklist of known bad websites.

It is important that more be done to raise awareness amongst computer users about the importance of keeping their PCs secure. It is estimated that over 99% of all spam is sent from home users' botnet computers that are not properly protected with up-to-date anti-virus software, firewalls and security patches.

Sophos saw spam being sent from countries around the world, emphasizing the need for all nations to properly ensure that their personal computers are being properly defended from malware attack.
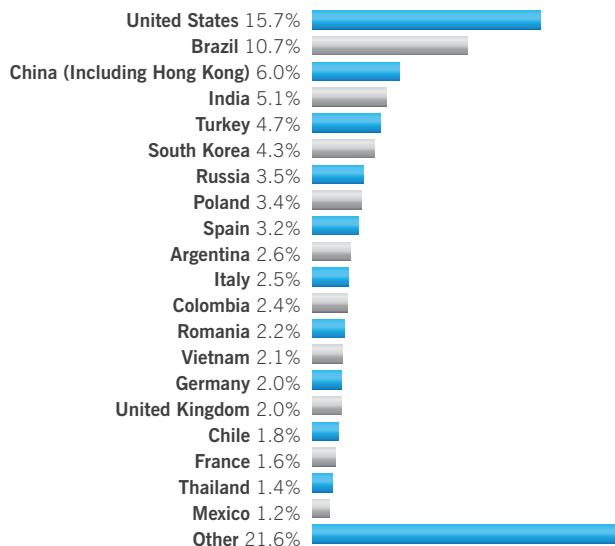
Are you a spammer?

Virtually all spam comes from compromised computers (called "bots" or "zombies") that have been successfully attacked and now, without their owners knowledge, 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 identifies business computers that have been hijacked and which are sending out emails on behalf of the spammers[36].

Spam-relaying by country

Country	%
United States	15.7%
Brazil	10.7%
China (Including Hong Kong)	6.0%
India	5.1%
Turkey	4.7%
South Korea	4.3%
Russia	3.5%
Poland	3.4%
Spain	3.2%
Argentina	2.6%
Italy	2.5%
Colombia	2.4%
Romania	2.2%
Vietnam	2.1%
Germany	2.0%
United Kingdom	2.0%
Chile	1.8%
France	1.6%
Thailand	1.4%
Mexico	1.2%
Other	21.6%

source: SophosLabs

The United States has increased its proportion of the total amount of spam relayed around the world slightly, sending 15.7% as compared to 14.9% in the same period in 2008.

Russia has dropped from its earlier second position in the chart, down to 3.5% from 7.5%. This is possibly attributed to ISPs being more aggressive in preventing spam-like behavior from their customers' computers.
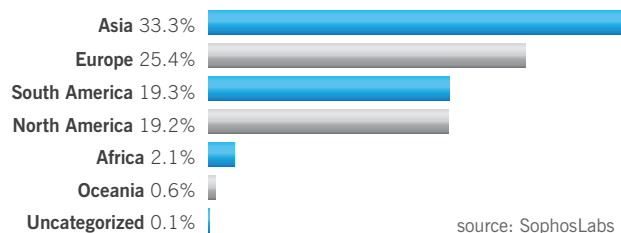
The presence of countries such as Turkey, Poland and India may be linked to those countries' growing high speed internet user base. However, their populations may not be as well versed in computer security (or less prepared to pay for anti-virus software).

Bill Gates's prediction that spam would be eradicated by 2006[35] has been proven wrong, and the botnet problem remains truly global. It is clear that the fight against spam needs to be a coordinated one.

Computers must be defended with up-to-date anti-virus software to prevent them from being used as relays by spammers. Email perimeters must be protected with sophisticated solutions to block incoming threats. The authorities must have the resources to pursue spammers and bring them to justice. And, the general public needs to be better educated about computer security and the importance of never purchasing goods advertised via spam.

Although USA rules the roost of individual countries responsible for relaying spam, when viewed by continent, the breakdown of spam-relaying countries shows Asia delivers one-third of all spam.

Spam by continent, Jan. 2009 – June 2009

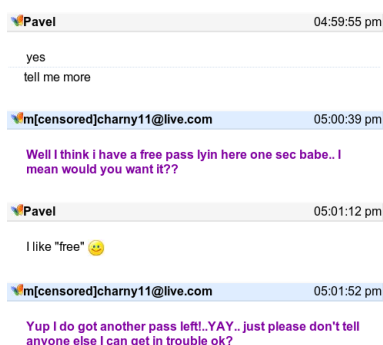|	
Asia 33.3%	
Europe 25.4%	
South America 19.3%	
North America 19.2%	
Africa 2.1%	
Oceania 0.6%	
Uncategorized 0.1%	source: SophosLabs

These statistics should not be overly surprising. What they demonstrate is a very simple equation — the higher the number of connected and insufficiently protected computers, the greater the percentage of spam that they are relaying to the rest of the world

Other new trends in spam

IM spam is proving a popular method of delivery, with spammers using instant message applications, such as MSN Chat, to avoid spam filters and trick unsuspecting users into revealing sensitive and financial information. Hackers spew spam from a botnet, containing a variety of email addresses and minor randomization of content.

In June, SophosLabs trapped IM spam by which a botnet, disguised as a woman, engaged users in a flirtatious chat, then lure them to a malicious website[37].

Pavel	04:59:55 pm
yes tell me more	
m[censored]charny11@live.com	05:00:39 pm
Well I think i have a free pass lyin here one sec babe.. I mean would you want it??	
Pavel	05:01:12 pm
I like "free" 🙂	
m[censored]charny11@live.com	05:01:52 pm
Yup I do got another pass left!..YAY.. just please don't tell anyone else I can get in trouble ok?	

IM spam using MSN Chat to lure users to phishing site

Social networking spam

Spammers are also exploiting the growing popularity of social networks like Twitter and Facebook to spread their advertisements and dangerous links. Whereas web-based email services like Gmail, Yahoo and Hotmail have matured over some years and developed solutions to protect their users, social networks have become popular in a short period of time — often meaning that they have are lagging behind in defending users from unwanted messages.

Malware

Using fear

The fake anti-virus software business continues to be a big earner for cybercriminals. Because of this, cybercriminals are putting serious resources behind it. Such attacks, commonly known as scareware or rogueware, prey on IT security fears and fool users into believing their computer has a problem when it does not.

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.

On average, Sophos identifies fifteen new scareware websites every day. This number has tripled, up from an average of five detected per day, during 2008.

Hacking gangs have become proficient at rapidly producing professional-looking bogus websites posing as legitimate security vendors. Fake anti-virus has also been distributed via poisoning the results of popular search engines through search engine optimization (SEO) techniques and affiliate schemes.

- **January** SophosLabs discovered hackers were using SEO in combination with photographs of celebrities like Warren Beatty and Shania Twain in their attempts to steal money[38].

- **March** Hackers used Natasha Richardson's untimely death in advantageously[39] stuffing webpages with keywords about the late-actress in order to lure unwary surfers into visiting their dangerous sites and infecting their computers.
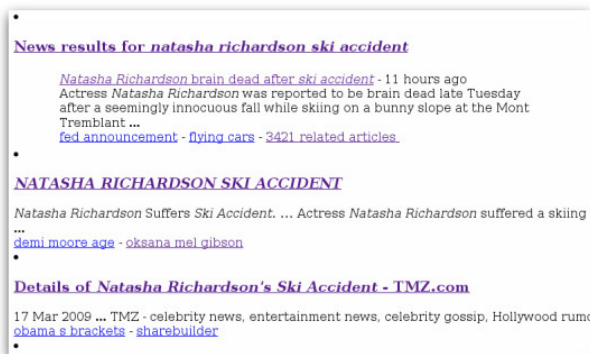
Hackers exploited death of an actress using SEO techniques

- **March** Hackers capitalized on a widespread issue with Symantec's Norton Anti-Virus product[40], poisoning search engines in an attempt to cash in on unsuspecting computer users searching for advice.

- **June** Opportunistic cybercriminals took advantage of the deaths of Farrah Fawcett[41] and Michael Jackson[42] to spread malware and spam.

Other trends in malware

Not all malware spreads via email or the web. The Conficker worm[43], for instance, uses internet and network protocols to spread, alongside infecting USB sticks — but does not infect email or web systems.

While Conficker, which exploited a Microsoft security vulnerability and first appeared in late 2008, truly made its presence known during the first few months of 2009, media hysteria leading up to April 1, 2009 when it was scheduled to change the way it looked for new instructions, helped push Conficker into notoriety.

Although it is clear that many firms and organizations struggled to protect themselves adequately from attack[49], it is debatable whether the hyperbole regarding the worm, helped improve the general state of computer security or was mistakenly seen as the computer security industry "crying wolfs".

Conficker – A worm gains notoriety

"Will your PC be jacked on April first [44]" "The Conficker Worm: April Fool's Joke or Unthinkable Disaster?[45]", "PC security forces face April 1 showdown with Conficker worm[46]" are just some of the headlines that helped Confickermania gain momentum before the alleged significant date of April Fool's Day.

Ironically, by and large, the computer security industry was not responsible for the hysteria regarding Conficker and April 1st. Instead, it appears that the story was largely brewed up by elements of the media, despite many security vendors announcing that users were unlikely to notice anything different on April Fool's Day.

Sure enough, April 1st 2009 saw no unusual activity by Conficker and many were left wondering who had started the buzz [47], and perhaps more importantly, how to protect themselves from future iterations[48].

One of the ways in which Conficker could spread itself was via USB memory sticks, a technique that Sophos has identified as a growing trend for malware during 2009[50]. Such malware typically exploits the Windows AutoRun feature to automatically execute when plugged in to a computer. As these portable drives have reduced significantly in price and increased in popularity over the years, so hackers have seen them as the modern equivalent of the floppy disk — and used their travel to spread infections.

2009 has seen a rise in using USB sticks to spread malware

The plague of USB malware spurred Microsoft into announcing that they were changing the way Windows 7 will handle AutoRun functionality[51].

Organizations are increasingly looking for security solutions that can control the use of USB drives — not only to prevent malware distribution but also to prevent data leaking out of their offices

Other trends in malware seen in early 2009, included discovery by SophosLabs of the first malicious code seemingly designed to help criminals steal money from ATM machines[52].

Diebold issued an update to its ATM software[53], and recommended that it be installed on all of its Windows-based ATMs globally. According to the company, the update should prevent the Skimer-A Trojan horse[54] from successfully stealing information from cash machine users.

In addition, they confirmed that hackers from Russia had attempted to plant the malicious software on ATMs in an audacious attempt to steal money. What isn't publicly known is how the managed to gain physical access to a number of ATMs in Russia.

Was it a breach in security along the supply-chain that delivers ATM hardware to banks, or an inside job? All Diebold has said so far is that there was not a network-level security compromise.

Clearly, following best practices can help minimise the chances of ATM security breaches, and users should be aware that some hackers might now be targeting the ATMs directly, rather than just the bank customers using the internet to manage their online finances.

Viruses that use polymorphism to mutate their appearance first rose to prominence in the early 1990s. However, the latest evolution of this technology is being deployed by malware today, in an attempt to avoid detection. The Scribble[55], Sality[56] and Vetor virus families are all examples of malware which is both polymorphic and widespread in the wild.

Scribble, for instance, stood out for not only mutating its appearance on each infection, but also its ability to target HTM, HTML, PHP and ASP web files, alongside Windows executables, as it spread via network shares and auto-running USB drives.

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.

Concerns about hackers taking advantage of security vulnerabilities in Adobe's PDF-reading software, spurred the company to announce that it would be making security updates available on a regular schedule. Adopting a similar initiative to Microsoft (which releases security patches on the second Tuesday of each month); Adobe announced that it would issue vulnerability fixes on the second Tuesday of every *third* month[57].

Apple Macs

A soft target

While small compared to the situation for Windows users the Mac malware problem does exist.

A high level of complacency in the Mac community means that many users incorrectly believe they are immune from internet security threats. This makes them a soft target for future attacks, and runs contrary to the advice that Apple itself provides for its users.[58] Mac users must understand malware authors use the same techniques to infect both Windows and Macs.

In June 2009, Sophos surveyed Mac users about their anti-virus use. It found 69% of the 108 respondents did not use anti-virus. These findings suggest that some Mac users still do not understand malware authors use the same techniques to infect both Windows and Macs, and therefore make themselves more vulnerable to attack.

Mac users: Do you use anti-virus?
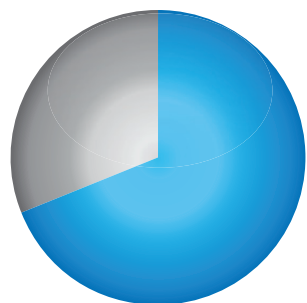
Don't use anti-virus software 69%

Use anti-virus software 31%

source: Sophos survey

Much of the malware seen for Mac OS X does not rely on flaws in the operating system, but instead use social engineering tricks to fool unsuspecting users into installing dangerous code. This is similar to how much Windows-based malware works, and emphasizes that the weak link is in the user making bad decisions rather than the software.

A typical trick would see a Mac computer user lured to a website with the promise of seeing a sexy video. When the user arrives at the page they are told that they need to install a plugin or codec to watch the movie. Downloading and installing the plugin, however, gives the hacker's malicious code control over the computer leading to the Mac having data stolen from it or being turned into part of a botnet. In other cases the malware may not be a plugin to view an X-rated movie, but may present the Trojan horse as an attractive piece of downloadable software.

An example of this kind of social engineering was a new version of the OSX/RSPlug Trojan horse, discovered in March 2009, being distributed via a seemingly legitimate website offering HDTV software[80]. The website was capable of infecting both Mac OS X and Windows computers and opened the door for hackers to steal personal information, display revenue-generating adverts, and install further malware.

More evidence of the increasing exposure to malware Mac users are facing came in June 2009, when a message about a sex videotape starring "Gossip Girl" star Leighton Meester was posted to the Twitter stream celebrity blogger Guy Kawasaki[81]. Anyone who followed Kawasaki's link, who has approximately 140,000 followers on the micro-blogging service, could have their Mac infected by the OSX/Jahlav-C Trojan horse (Windows-owning victims were struck by a piece of malware for their operating system).
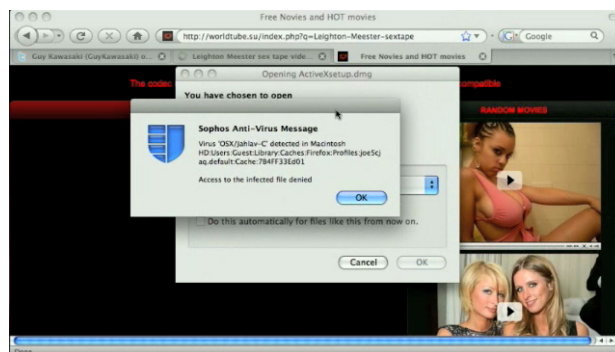
Webshot of Mac malware posed as video of TV star

In addition to websites hosting malware capable of infecting Apple Macs, 2009 saw a campaign by hackers to spread infections by distributing their malicious code disguised as pirated versions of popular software packages like Adobe PhotoShop CS4[60] and iWork '09[61] distributed via BitTorrent.

To defend against these attacks 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

BlackBerry

While there have been no reports of malware infecting BlackBerry devices, vulnerabilities have been found that can be exploited if hackers sent specially crafted files to the phone.

In January 2009, BlackBerry developers Research in Motion (RIM) issued a patch for a malicious BlackBerry PDF vulnerability that could be exploited by hackers[62]. It was revealed if a BlackBerry user tried to open a maliciously-crafted PDF file, malicious code could be executed on a computer hosting the BlackBerry Attachment Service. A similar vulnerability emerged in March 2009, with RIM issuing another patch [63].

Palm Pre and Google Android

At the time of press, there have been no reported malware attacks against Google's Android operating system or Pre, Palm's highly anticipated "iPhone killer." Nevertheless, as these devices grow in popularity, hackers will likely develop malware to exploit these devices for purposes of financial gain or simple notoriety.

Of course, cybercrime attacks that are not operating system-specific (such as phishing and 419 scams) will threaten Palm Pre and Google Android users as much as any other internet user.

iPhone

iPhones are increasingly being adopted inside enterprises by users who bring them in from home or demand that they be used for work purposes. Whereas BlackBerries (which were originally popular with more security conscious organizations including those in the field of aerospace, defence and government) have a strong history of security built into their architecture, the iPhone originally focused on usability. As such, it now finds itself attempting to adapt itself into an appropriate and secure device for the workplace.

The iPhone 3GS has made advances in data security terms, now offering hardware encryption and remote wipe capabilities. In addition, security flaws have been fixed that were present in earlier editions[64].

But the iPhone still loses to the BlackBerry when competing for the crown of enterprise-ready secure messaging, leaving some businesses to make a trade-off between usability versus risk. It's clear, however, that the total cost of ownership for managing iPhones in larger environments is still much higher.

One piece of good news is that although simple malware has already been seen, the iPhone has not yet been the target of a significant attack [65].

In the past, there has been criticism from some quarters that Apple has dragged its feet in fixing iPhone vulnerabilities, sometimes leaving the platform unpatched for months compared to the desktop Mac OS X platform. As the platform becomes grows in popularity it will become more important than ever that it is patched in a timely fashion. The potential for delayed patches has led some to speculate that hackers could take advantage of vulnerabilities in shared common code, such as the Safari Web browser (which is used on the iPhone and ships as standard on Mac OS X) as the platform for attack[66].

The very fact that a smartphone like the iPhone is a cellphone as well as a computing device can lead to potential new vectors of attack. For instance, security researcher Charlie Miller discovered a way of forcing a targeted iPhone to be disconnected from the cellphone network purely by sending it a maliciously-crafted SMS message[67].

In addition, 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 has limited space. Because of this URLs may be truncated[68], making it easier for cybercriminals to fool users into believing they are on a legitimate website.

These contributing factors may also be present on other smartphone devices of course.

Cybercrime and computer crimes

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. 2009 saw even more reports of cyberwarfare and computer crimes:

- **February** India's Ministry of External Affairs (MEA) confirmed that some of its computers had been infected with spyware[69]. Affected PCs include computers dealing with sensitive Pakistani affairs, and in the offices of senior Secretaries and Joint Secretaries.

- **June** Opponents of the incumbent government in Iran made their opinions felt when they launched distributed denial-of-service attacks against the Iranian Justice Ministry and President's websites.

Twitter users forwarded messages to each other containing links to webpages that automatically flooded Iranian government websites with traffic, overloading them and causing them to crash[70].

Arrests and the Law

With cyberwarfare and computer based crimes on the rise, governments have made several attempts, some successful, to shut down malicious operations. The first half of 2009 has seen more shutdowns, arrests and harsher sentences for criminals involved in high-profile and financially rewarding computer crimes.

Perhaps the most prominent government-forced closure during this time is the closure of Internet Service Provider Pricewert by the FTC in June 2009[71], following allegations it was knowingly involved in major spam attacks, phishing campaigns, malware distribution, and child abuse.

The FTC complaint further alleges the company consciously shielded its criminal clients by ignoring requests from the Internet security community asking for dangerous pages to be taken down[72].

While this case has yet to go court, the government's involvement proves that they are serious about stopping malicious and harmful activities.

Here are a few other success stories from the first six months of this year:

- **January** Maksym Yastremskiy, one of the men behind the infamous TJX data breach received a 30-year prison sentence for his involvement with the hack[73].

- **March** Hugh Rodley and David Nash were convicted for their part in what would have been Britain's biggest bank robbery[74] — an elaborate scheme to steal £229 million from the London branch of Sumitomi Mitsui bank by smuggling hackers[75] into the premises after-hours to install keylogging software onto terminals.

- **April** Four women and five men were arrested, suspected of targeting the financial services industry with banking Trojan horses[76]. The gangs are believed to have recruited mules to help move stolen funds into their own coffers

- **May** The US District Court in Minneapolis has sentenced a 23-year-old Romanian immigrant to 8.5 years in jail for stealing a total of approximately $700,000 from over 7,000 innocent people[77]. According to local media reports, he started his phishing campaign in June 2000, when he was 14 years old.

Cyber security departments – a new trend in government?

Educating users and raising awareness of internet threats and cybersecurity amongst the general population is paramount, especially when there can be a tendency for governments to emphasize the threat posed by other countries and terrorist groups in other countries while neglecting to understand the real threat domestic terrorists present.

President Obama recently recognized this need, and in May 2009 outlined a new government strategy designed to "deter, prevent, detect and defend" against cyber attacks, from those that originate overseas and domestically. He also promised to create a cyber security coordinator "czar" whose primary responsibility is developing and overseeing this strategy This is one of many recommendations outlined in the 60 day cyberspace policy review commissioned in February[78].

Then in June 2009, the British government published its cyber security strategy, announcing its intentions to create a central body to liaise with industry (the Office of Cyber Security or OCS) and a separate body, the Cyber Security Operations Centre (CSOC), based at the UK's surveillance headquarters GCHQ in Cheltenham[79].

Will this deter future cybercriminal activities? It's not certain. What is certain, however, is that governments increasingly want to be seen as serious in their intent to shut down cybercriminal organizations.

The future

What the future holds

Predicting the future in such rapidly evolving environments is virtually 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 becomes more serious.

But some things do seem certain however:

- **Web 2.0 websites** such as Facebook, Twitter and MySpace will become the main battleground for malware authors, identity thieves and spammers. Companies must educate users of safe ways to use social networking websites, and ensure they are properly defended.


Social media will become new battleground for malware

- **Web insecurity** (notably SQL injection attacks) will continue to be the primary driver behind malware distribution. Cybercriminals can then send innocent-looking spam which link to legitimate, but hacked, webpages. These hacked sites link invisibly to malicious content.

- **The variety of attacks** and their number will continue to escalate, as hackers and malware authors adopt new techniques and disguises to infect the unwary and unsuspecting.

Variety of attacks and malware author techniques will rise

- **Compromised PCs** will continue to be the primary source of spam. Users must take steps to avoid spreading and contributing to attacks.

- **Identity theft** will become a bigger concern and continue to adversely affect customer loyalty. In the year ahead, laws will stop companies sweeping security breaches under the carpet.
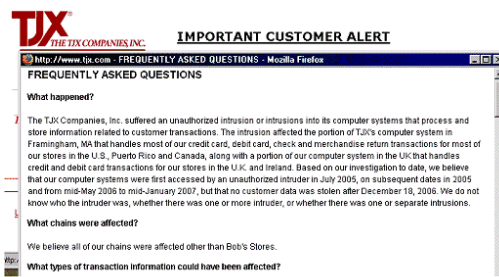
- **Prevention** will become more useful than cure as mandatory disclosure even of potential breaches leads to loss of consumer confidence

- **Email and web attacks** will increasingly use non-program (non-EXE) files, such as Word Documents and PDFs. Legitimate-looking data files can be booby-trapped with exploits against software vulnerabilities. On an unpatched PC, such files can trigger the invisible download and installation of viruses and Trojans.

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. Additionally, threats like identity theft and fraud will still occur because of human mistakes.

However, if managed properly, the problem can be solved. Sound security practices, up-to-date protection and an active commitment to keep informed can all help defend business networks.

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 properly defended can much more easily keep the bad stuff out, and the good stuff in.

Sources

1. http://www.sophos.com/pressoffice/news/articles/2009/04/social-networking.html
2. http://www.sophos.com/pressoffice/news/articles/2009/04/social-networking.html
3. http://www.sophos.com/blogs/gc/g/2009/07/05/mi6-chiefs-wife-puts-security-risk-facebook/
4. http://www.sophos.com/blogs/gc/g/2009/01/05/twitter-users-hit-phishing-spam-attacks/
5. http://www.sophos.com/blogs/gc/g/2009/01/22/facebook-scam-actio/
6. http://www.sophos.com/blogs/gc/g/2009/01/15/myspace-user-stung-130000-email-scam/
7. http://www.sophos.com/blogs/gc/g/2009/04/12/mikeyy-attack-hits-twitter-users-bad-24-hours-web-20-security/
8. http://www.sophos.com/pressoffice/news/articles/2009/05/twitter-hacker.html
9. http://www.sophos.com/blogs/gc/g/2009/05/24/acai-berry-spammers-hack-twitter-accounts-spread-adverts/
10. http://www.sophos.com/blogs/gc/g/2009/06/01/tory-mp-hacked-facebook/
11. http://www.sophos.com/pressoffice/news/articles/2009/04/social-networking.html
12. http://www.sophos.com/blogs/gc/g/2009/05/06/hackers-demand-10-million-ransom-wiping-patient-data/
13. http://www.sophos.com/blogs/gc/g/2009/05/29/109000-pension-holders-risk-laptop-stolen/
14. http://www.sophos.com/blogs/gc/g/2009/06/04/530000-virginia-patients-individually-warned-ssn-hack/
15. http://www.nytimes.com/2009/07/07/business/07goldman.html?_r=1
16. http://www.sophos.com/blogs/gc/g/2009/05/14/malicious-jsredir-javascript-biggest-malware-threat-web/
17. http://www.sophos.com/blogs/sophoslabs/v/post/2737
18. http://www.sophos.com/blogs/sophoslabs/v/post/2827
19. http://www.sophos.com/blogs/sophoslabs/v/post/2819
20. http://www.sophos.com/blogs/sophoslabs/v/post/3564
21. http://www.sophos.com/blogs/gc/g/2009/04/09/fixing-hole-paul-mccartneys-website-hacked/
22. http://www.sophos.com/blogs/sophoslabs/v/post/4325
23. http://www.sophos.com/blogs/sophoslabs/v/post/4736
24. http://www.sophos.com/pressoffice/news/articles/2008/08/sql-podcast.html
25. http://www.sophos.com/blogs/sophoslabs/v/post/1545
26. http://www.sophos.com/security/sophoslabs/anonymizing-proxies.html
27. http://www.darkreading.com/blog/archives/2009/06/the_iranian_pro.html
28. http://www.sophos.com/blogs/gc/g/2009/01/19/barack-obama-refused-president/
29. http://www.sophos.com/blogs/gc/g/2009/03/16/dirty-bomb-news-report-leads-pc-infection/
30. http://www.sophos.com/blogs/gc/g/2009/01/02/classmates-malware-campaign-poses-school-reunion-invite/
31. http://www.sophos.com/blogs/gc/g/2009/05/07/worldpay-card-transactions-carry-malware-danger/
32. http://www.sophos.com/blogs/gc/g/2009/06/03/postcards-family-member-malware/
33. http://www.sophos.com/blogs/gc/g/2009/06/15/sex-movie-sherrie-open-link/
34. http://www.sophos.com/pressoffice/news/articles/2008/05/spam-pledge.html
35. http://news.bbc.co.uk/1/hi/business/3426367.stm
36. http://www.sophos.com/products/enterprise/alert-services/zombiealert.html
37. http://www.sophos.com/blogs/sophoslabs/v/post/4927
38. http://www.sophos.com/blogs/gc/g/2009/01/06/hackers-celebrity-image-seo-spread-scareware/
39. http://www.sophos.com/blogs/gc/g/2009/03/19/natasha-richardsons-death-exploited-hackers/
40. http://www.sophos.com/blogs/gc/g/2009/03/10/malware-authors-jump-piftsexe-bandwagon/
41. http://www.sophos.com/blogs/sophoslabs/v/post/5023
42. http://www.sophos.com/blogs/sophoslabs/v/post/5070
43. www.sophos.com/conficker
44. http://www.sophos.com/blogs/gc/g/2009/03/27/hype-april-fools-day-conficker-worm/
45. http://bits.blogs.nytimes.com/2009/03/19/the-conficker-worm-april-fools-joke-or-unthinkable-disaster/?ref=technology

46. http://www.usatoday.com/money/industries/technology/2009-03-24-conficker-computer-worm_N.htm

47. http://www.sophos.com/blogs/gc/g/2009/04/10/pcs-patched-conficker-vulnerability/

48. http://www.sophos.com/products/free-tools/conficker-removal-tool.html

49. http://www.sophos.com/blogs/gc/g/2009/06/02/ten-work-pcs-fail-basic-security/

50. http://www.sophos.com/blogs/sophoslabs/v/post/279

51. http://www.sophos.com/blogs/gc/g/2009/05/01/microsoft-improves-autoplay-combat-usb-malware/

52. http://www.sophos.com/blogs/gc/g/2009/03/17/malware-lurking-atm/

53. http://www.sophos.com/blogs/gc/g/2009/03/18/details-diebold-atm-trojan-horse-case/

54. http://www.sophos.com/security/analyses/viruses-and-spyware/trojskimera.html

55. http://www.sophos.com/blogs/sophoslabs/v/post/3130

56. http://www.sophos.com/blogs/sophoslabs/v/post/4060

57. http://www.sophos.com/blogs/gc/g/2009/05/21/adobe-announces-patch-tuesday/

58. http://www.apple.com/macosx/what-is-macosx/security.html

59. http://www.sophos.com/blogs/gc/g/2009/06/24/leighton-meeter-sex-tape-lure-spread-malware-twitter-users/

60. http://www.sophos.com/blogs/gc/g/2009/01/26/reports-mac-trojan-pirated-adobe-photoshop-cs4/

61. http://www.sophos.com/blogs/gc/g/2009/01/22/reports-mac-trojan-horse-pirated-version-iwork-09/

62. http://www.sophos.com/blogs/gc/g/2009/01/14/blackberry-pdf-vulnerability/

63. http://www.sophos.com/blogs/gc/g/2009/05/27/control-blackberry-enterprise-server-pdf/

64. http://www.sophos.com/blogs/sophoslabs/v/post/975

65. http://www.sophos.com/blogs/gc/g/2009/06/18/apple-update-fixes-46-iphone-security-vulnerabilities/

66. http://blog.washingtonpost.com/securityfix/2008/07/apple_iphone_four_months_behin_1.html

67. http://www.theregister.co.uk/2009/07/02/critical_iphone_sms_bug/

68. http://www.usenix.org/events/upsec08/tech/full_papers/niu/niu_html/

69. http://www.sophos.com/blogs/gc/g/2009/02/16/indian-government-computers-hit-spyware-attack/

70. http://www.smh.com.au/technology/technology-news/cyber-activists-target-iranian-government-websites-20090617-chgy.html

71. http://www.darkreading.com/blog/archives/2009/06/suspected_malwa.html

72. http://www.ftc.gov/opa/2009/06/3fn.shtm

73. http://www.sophos.com/blogs/gc/g/2009/01/08/tj-maxx-hacker-jailed-30-years-turkey/

74. http://www.sophos.com/blogs/gc/g/2009/03/05/men-guilty-botched-229m-hightech-bank-heist/

75. http://www.sophos.com/blogs/gc/g/2009/01/22/hackers-smuggled-bank-229-million-heist-court-hears/

76. http://www.sophos.com/blogs/gc/g/2009/04/09/police-arrest-suspected-banking-trojan-gang/

77. http://www.sophos.com/blogs/gc/g/2009/05/28/guy-phishing-14-years/

78. http://www.sophos.com/blogs/sophoslabs/v/post/4568

79. http://www.sophos.com/blogs/gc/g/2009/06/26/uk-attack-countries-cyberspace/

80. http://www.sophos.com/pressoffice/news/articles/2009/03/mac-malware.html

81. http://www.sophos.com/blogs/gc/g/2009/06/24/leighton-meeter-sex-tape-lure-spread-malware-twitter-users/

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

SOPHOS
WWW.SOPHOS.COM