SOPHOS

Security Threat Report: **2010**

Contents

Social networking 2

Data loss and encryption 7

Web threats 9

Email threats 13

Spam 15

Malware trends 18

Windows 7 21

Apple Macs 23

Mobile devices 25

Cybercrime 28

Cyberwar and cyberterror 31

The future: What does 2010 hold? 33

SOPHOS

Security Threat Report: **2010**

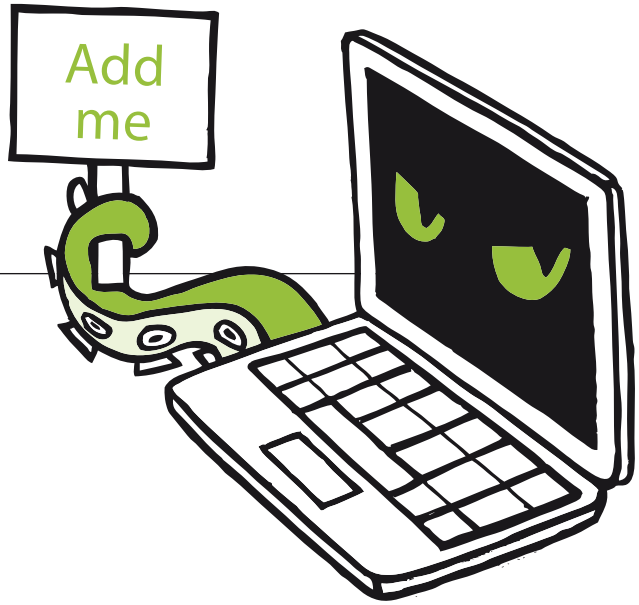
The first decade of the 21st century saw a dramatic change in the nature of cybercrime. Once the province of teenage boys spreading graffiti for kicks and notoriety, hackers today are organized, financially motivated gangs. In the past, virus writers displayed offensive images and bragged about the malware they had written; now hackers target companies to steal intellectual property, build complex networks of compromised PCs and rob individuals of their identities.

2009 saw Facebook, Twitter and other social networking sites solidify their position at the heart of many users' daily internet activities, and saw these websites become a primary target for hackers. Because of this, social networks have become one of the most significant vectors for data loss and identity theft.

New computing platforms also emerged last year, and shortly thereafter fell victim to cybercriminal activities. What was lost was once again found in 2009, as old hacking techniques re-emerged as means to penetrate data protection.

By understanding the problems that have arisen in the past, perhaps internet users can craft themselves a better, safer future.

Social networking

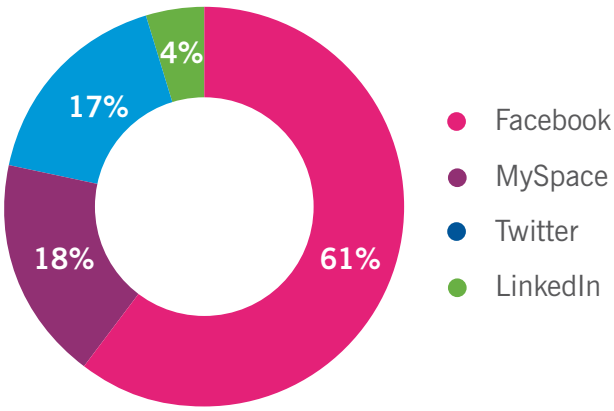


Battle lines are drawn

When the Web 2.0 phenomenon first caught on in 2004, many found it irritating and a timewaster. Likewise, organizations were concerned about wasted company time, as employees would log in to these sites during business hours and drain company bandwidth or worse—inadvertently leak confidential company information.

In 2009, however, such attitudes were relegated to the past as businesses widely adopted social networking techniques. Companies now commonly use blogs to disseminate and share information. Forums serve as a form of technical support where professionals can troubleshoot with peers and colleagues. Meanwhile, many companies embrace Facebook and MySpace because the sites present a great way to connect with customers and spread the latest company news or product offerings to the public.

According to Cisco, almost 2% of all online clicks in 2009 through 4,000 Cisco web security appliances have been on social networking sites, 1.35% on Facebook alone[1]. The business world would be foolish to ignore such a high level of activity and such a potentially lucrative resource.



Which social network do you think poses the biggest risk to security?

Why businesses are concerned

For many businesses, the idea of controlling social networking by simply imposing a blanket block on such sites is impractical. More subtle and granular controls are required, such as data loss monitoring to watch for specific types of information passing outside company boundaries via non-approved vectors, and tightly configurable usage policies that can limit illegitimate use of certain sites and technologies while granting access to those who require it.

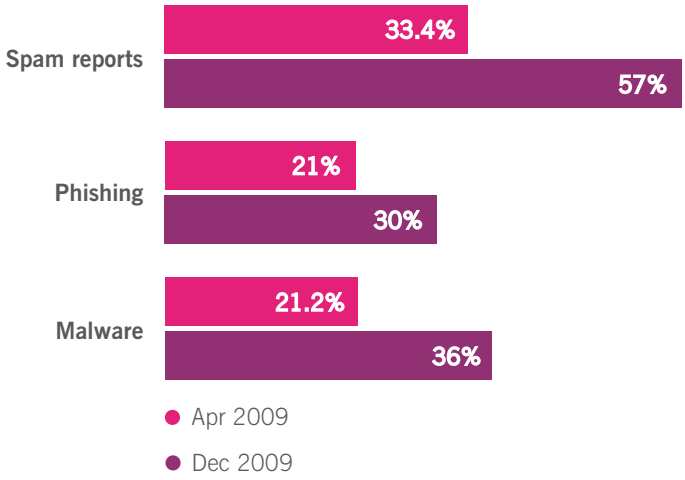
According to a Sophos survey conducted in December 2009, 60% of respondents believe that Facebook presents the biggest security risk of the social networking sites, significantly ahead of MySpace, Twitter and LinkedIn.

Although productivity continues to be the dominant reason for companies to block social networks (a third of companies say this is the reason they block Facebook e.g.), there has been a dramatic rise since April 2009 in the number of businesses who believe malware is their primary security concern with such sites.

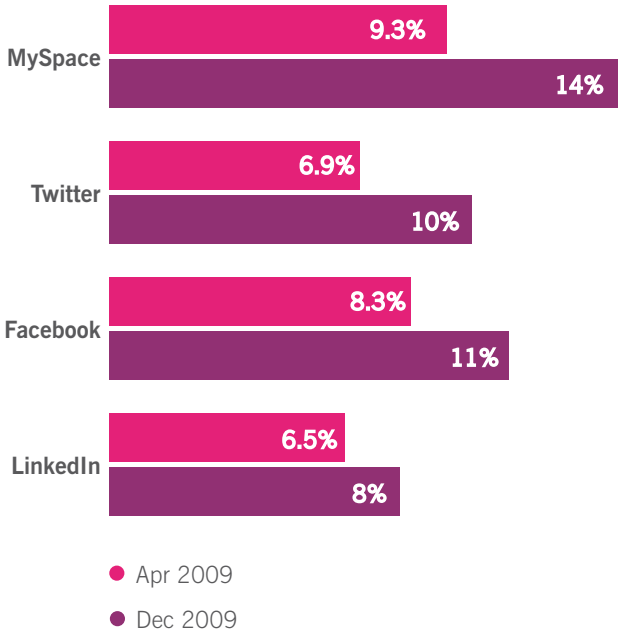
It seems these malware concerns are well-justified, with a 70% rise in the proportion of firms that report encountering spam and malware attacks via social networks during 2009. More than half of all companies surveyed said they had received spam via social networking sites, and over a third said they had received malware.

Furthermore, over 72% of firms believe that employees' behavior on social networking sites could endanger their business's security. This has increased from 66% in the previous study. The number of businesses that were targets for spam, phishing and malware via social networking sites increased dramatically, with spam showing the sharpest rise from 33.4% in April to 57% in December. This highlights a surge in exploitation of such sites by spammers[2].

Social networks Spam, Phishing and Malware reports up



Firms citing malware as their number one concern with social networks



```
var redirects = [
['facebook.com',  abc+'fb.php'],
['tagged.com',    abc+'tg.php'],
['friendster.com',abc+'fr.php'],
['myspace.com',   abc+'ms.php'],
['msplinks.com',  abc+'ms.php'],
```

Koobface

Those worried about the dangers of social networking sites have a right to be concerned, as many malicious attacks, spammers and data harvesters take advantage of under-cautious users. Most notably, the notorious Koobface worm family became more diverse and sophisticated in 2009.

The sophistication of Koobface is such that it is capable of registering a Facebook account, activating the account by confirming an email sent to a Gmail address, befriending random strangers on the site, joining random Facebook groups, and posting messages on the walls of Facebook friends (often claiming to link to sexy videos laced with malware). Furthermore, it includes code to avoid drawing attention to itself by restricting how many new Facebook friends it makes each day.

Koobface's attack vectors broadened, targeting a wide range of sites other than the one that gave it its name (i.e., Facebook). Social networking sites, including MySpace and Bebo, were added to the worm's arsenal in 2008; Tagged and Friendster joined the roster in early 2009; and most recently the code was extended to include Twitter in a growing battery of attacks.[3]

It is likely we will see more malware following in the footsteps of Koobface, creating Web 2.0 botnets with the intention of stealing data, displaying fake anti-virus alerts and generating income for hacking gangs.

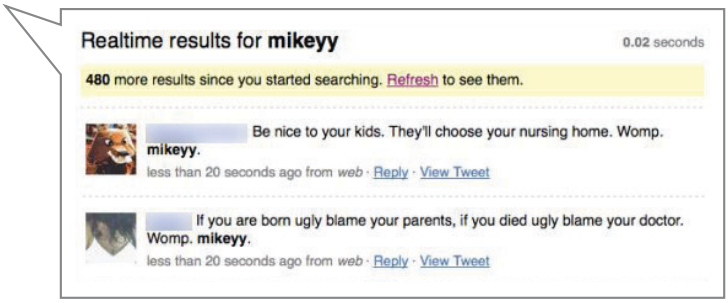
Social networks have become a viable and lucrative platform for malware distribution.

The Mikeyy Mooney worms

In April 2009, the StalkDaily worm rampaged Twitter as heavily spammed messages pushing an infected site by more subtle attacks spread from tweeter to tweeter.[4] The worm appeared to be the work of 17-year-old Mikeyy Mooney,[5] whose name was referenced in a second wave of attacks appearing just hours after the initial StalkDaily incident.[6]

Shortly afterward, yet another worm that was crafted using cross-site scripting techniques to spread referenced Mikeyy.[7] Further attacks[8] in April brought more misery to Twitter users.[9]

The speed with which these attacks have appeared, spread and become major issues should send a strong message to the big Web 2.0 companies. However, many still need to closely examine their systems and procedures to determine how to protect their members from these threats. Most of these problems can be easily corrected with improved design, programming and data usage policies, and, most important, rapid response to emerging issues.



Also a "localized" problem

Although these major global social networking sites seem to be the most significant part of the problem, they are no more than the tip of the Web 2.0 iceberg. Many countries, regions, groups and subcultures have their own social networking sites. These localized sites, like China's Renren network, are not only as vulnerable to attack, but also as likely to be both drains on corporate time and vectors for data infiltration.

Malware attacks on locale-specific sites have occurred, such as the W32/PinkRen worm, which targeted the Renren network of 40 million users in August 2009, posing as a video of Pink Floyd's classic song "Wish you were here."[10] Some of these sites are significantly smaller than the global giants and not as well maintained, so the challenges of problem solving, vulnerability patching, and provisioning adequate privacy and security controls may be even greater.

W32/PinkRen

Emerging vectors for social networking attacks

With individuals and businesses hooked on online social outlets, cybercriminals have taken notice and started using them for their gain. Beyond the common nuisances, such as wasted company time and bandwidth, malware and malicious data theft issues have presented serious problems to social networks and their users. Spam is now common on social networking sites, and social engineering—trying to trick users to reveal vital data, or persuading people to visit dangerous web links—is on the rise.

Spam is now common on social networking sites, and social engineering is on the rise

Social network logon credentials have become as valuable as email addresses, aiding the dissemination of social spam because these emails are more likely to be opened and trusted than standard messages. In many cases, spam and malware distribution are closely intertwined.[11]

Facebook privacy settings

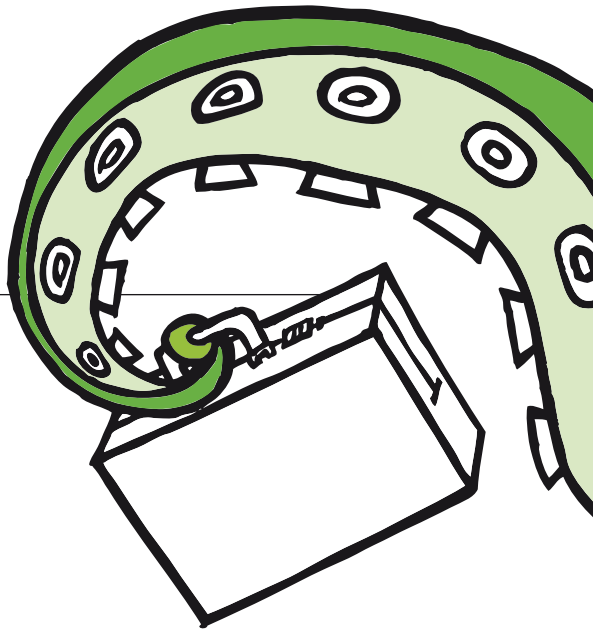
Information posted to such sites can be a valuable resource for some, as targeted phishing attacks use validated information harvested from the web and identification checks used by legitimate sites. The danger of putting too much personal information online, particularly on social networking sites, was brought to light when the wife of the chief of the British secret service MI6 posted highly revealing details about their residence and friends on her Facebook page.[12]

The wife of the chief of the British secret service MI6 posted highly revealing details about their residence and friends to her Facebook page

How to mitigate the risk

The hack that bypassed security and harvested data from Twitter in November[13] proves that social networking sites are just as vulnerable as any other software or web resource. Of course, the problem of data loss via social networks is fed by the willingness of users to share too much information with too many people. Many sites have woken up to the dangers they may present, with Facebook introducing a major new range of privacy settings in December. Sadly, in its announcement, Facebook recommended that users adopt a series of new privacy settings that would reveal their personal data to anyone on the internet forever.[14] Meanwhile, bit.ly, Twitter's favorite URL shortening service, responded to the common exploitation of such services to obfuscate malicious links, and teamed up with Sophos and other security providers to ensure its links are kept safe.[15]

The social networking boom shows no sign of stopping and businesses can no longer hide their heads in the sand. Social networking sites are now a vital part of many marketing and sales strategies. Therefore, they cannot be blocked—but they cannot be allowed to drain company resources or used as vectors for data loss or malware penetration. A unified approach providing sensible, granular access control, secure encryption and data monitoring, and comprehensive malware protection is mandatory for businesses to operate flexibly in the modern socially networked world.



Data loss and encryption

A major data leak can break a business and render an institution a laughing stock

Data leaks lead to broken businesses

Now more than ever, data is the ultimate business asset. With the sophistication of modern cybercriminal gangs, bank details are just as valuable as money itself. Business reputations are only as strong as the processes, precautions and protective solutions in place to guard company and customer data. A major data leak can break a business and render an institution a laughing stock. Large global brands such as TJX have risked losing credibility as well as the trust of their customers following the disclosure of major losses of customer data.[16]

One of the biggest data leaks of 2009 was also one of the most embarrassing. In October, a hard disk containing part of a database of 76 million US Army veterans was sent for repair with the data still intact and accessible.[17] Other leaks were recorded in 2009 from US universities, schools and colleges; banks and credit unions; hospitals and health centers; state, city and local government institutions; businesses; and even security companies.[18]

In the UK, government and national institutions, including the National Health Service, the military and the security service MI5, have suffered a number of potentially serious data leaks in recent years. Corporations around the world faced similar problems in 2009:

- **May:** Hackers break into a Virginia government website, stealing the details of almost 8.3 million patients and threaten to auction them to the highest bidder.[19]
- **May:** Information about senior officers of the Royal Air Force is exposed and fears of blackmail arise. [20]
- **November:** Rogue employees of mobile phone provider T-Mobile share data on thousands of customers with rival providers.[21]
- **November:** Hackers leak emails from the Climatic Research Unit at the University of East Anglia.[22]

To counteract this growing problem, the Information Commissioner's Office (ICO) in the UK proposed fines to punish corporations and organizations found negligent in incidents that allow unauthorized access to sensitive personal information.[23] Worldwide, compliance and disclosure regulations are becoming increasingly widely applicable and restrictive, with businesses reporting steadily growing costs involved in ensuring their data policy compliance.[24]

The biggest data losses of the decade

January 2000: 300,000 credit card numbers are stolen from online music retailer CD Universe—news is leaked to the web after ransom demands are rejected.[25]

November 2000: Travelocity exposes data on 51,000 customers on a company web server.[26]

March 2001: Bibliofind.com, an Amazon-owned service website, is breached and records of 98,000 customers are compromised.[27]

April 2001: Hackers announce the theft of personal data on 46,000 customers from US web hosting firm ADDR.com.[28]

February 2002: A former employee of US financial services firm Prudential Insurance Company is charged with stealing a database of 60,000 clients to sell online.[29]

March 2003: Five million credit card numbers and expiration dates are stolen from Data Processors International—an insider attack is suspected.

June 2004: 92 million email addresses of AOL subscribers are sold to spammers.[30]

June 2005: 40 million credit card numbers are taken from a hacked credit card processing firm.

May 2006: Details of 26.5 million US Army veterans are stolen by hackers.

June 2006: Japanese telecom firm KDDI admits data on 4 million customers was leaked.[31]

January 2007: TJX Companies Inc., the global conglomerate that includes T.J. Maxx, T.K. Maxx, Marshalls and Winners, loses at least 45 million sets of credit card details after systems are penetrated by hackers. [32]

November 2007: UK HM Revenue & Customs loses detailed records of 25 million taxpayers.[33]

March 2008: 12.5 million sets of records on backup tapes are lost by BNY Mellon shareholder services.

September 2008: Two CDs containing records on 11 million people are found on a Seoul scrapheap. The data is traced to oil refinery GS Caltex.

October 2008: T-Mobile Germany loses a hard disk containing information on 17 million customers.

January 2009: Networks at Heartland Payment Systems are hacked, exposing data on 130,000,000 credit card users.[34]

May 2009: Secret information on the Joint Strike Fighter and President Obama's personal helicopter were leaked through P2P networks.

October 2009: Hard drives sent for repair are found to contain data on 76 million US Army veterans.

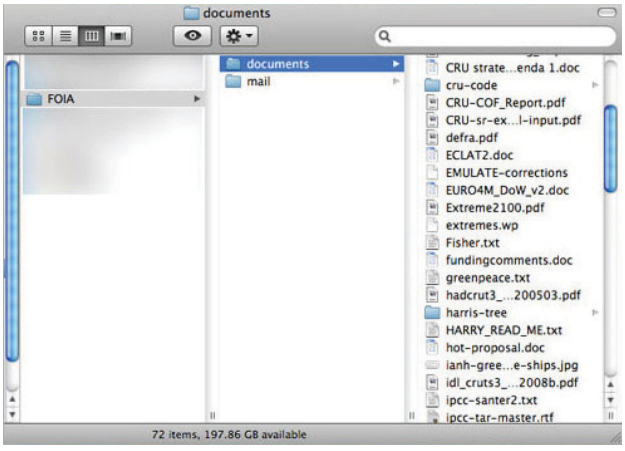
Preventing data loss

Most if not all of these incidents could have been avoided if the companies and institutions involved had implemented more stringent data management procedures. The most important step in stopping data loss 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, he or she will not be able to read it and 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

The most important step in stopping data loss is to encrypt sensitive information, laptops, and removable storage devices



A drive of lost data

Web threats

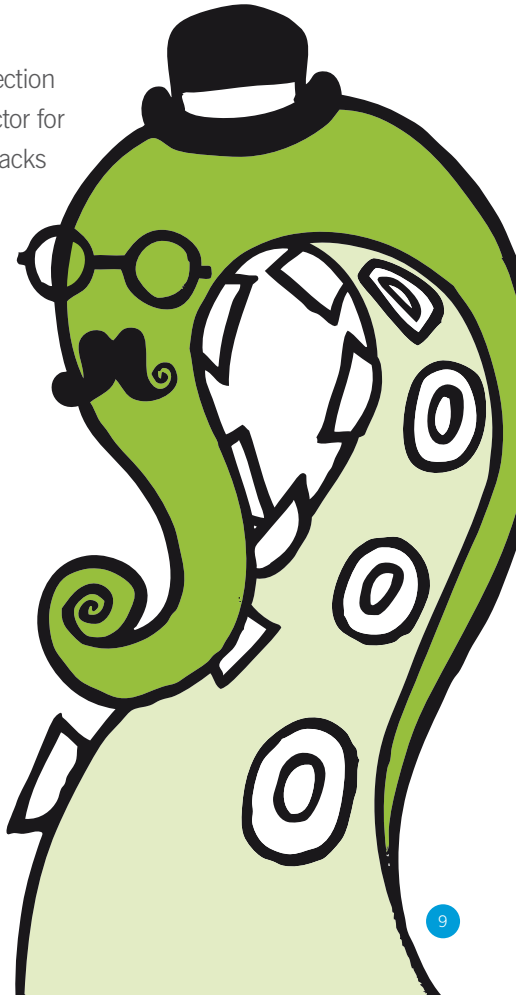
The web remains the biggest vehicle for malware.

The traditional method of maliciously crafted sites luring victims in with promises of rare and desirable content continues to flourish, but is now rivaled by legitimate sites compromised by cybercriminals to host their wares. Such sites are particularly dangerous because visitors feel secure on trustworthy web resources and therefore tend to let their guard down and believe what the popups and inserts say.

Compromised legitimate sites made big headlines in 2009, with SQL injection and malicious advertising ("malvertising") being the main penetration vector for larger, more professional sites. Websites that fell victim to malvertising attacks included The New York Times[35] and technology website Gizmodo.[36]

Meanwhile, the website of the UK's leading fish-and-chip chain, Harry Ramsden's, was compromised and made to serve up malicious iFrames.[37] Van Morrison fans were also placed at risk after hackers inserted dangerous iFrames onto pages of his website,[38] leading to sites hosted in Russia.[39]

Visitors feel secure on trustworthy web resources and therefore tend let their guard down and believe what the popups and inserts say



Fake AV and SEO malware stir up trouble

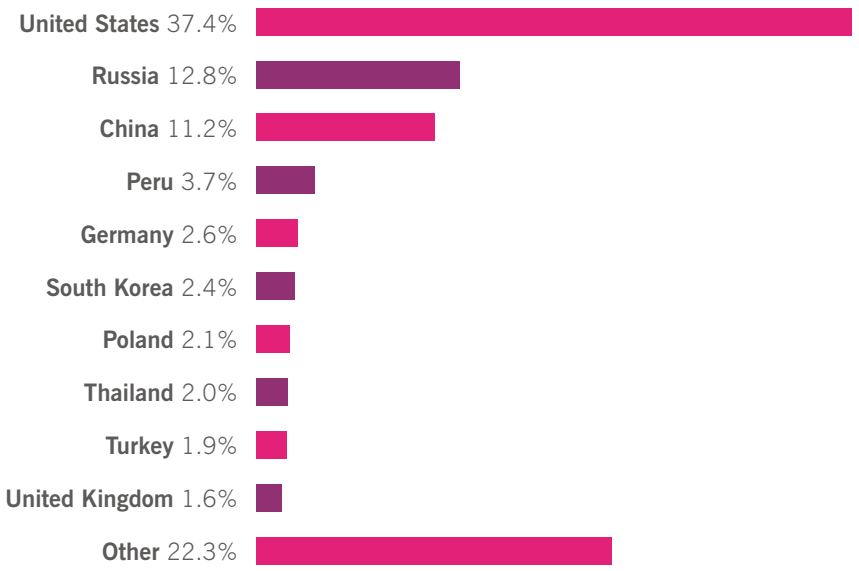
Many national embassies and consulate websites were hacked last year, often putting their visitors at risk. Among those affected were the Indian embassy in Spain,[40] Azerbaijanian sites in Pakistan and Hungary,[41] the Ethiopian embassy in Washington DC,[42] the US Consulate General in St. Petersburg, Russia,[43] and the embassy of the Republic of the Sudan in London.[44] Most of these sites were used to serve up fake anti-virus software scams.

Meanwhile, leaked or stolen FTP login credentials allowed hackers to overtake a vast number of "mom-and-pop" websites. The Gumblar web threat first reared its ugly head in May 2009, producing a massive spike in detections of malicious sites,[45] and continued to evolve and grow in waves throughout the year. The attack, like many others, mainly penetrates sites with stolen FTP information and inserts malicious iFrames and PHP scripts to lead users to download further malware.[46]

Many of these compromised sites, like those set up with explicitly malicious intentions, attract visitors thanks to aggressive search engine optimization (SEO) techniques designed to push links to the top of search results and often taking advantage of breaking news stories, popular trends and major events.

The US remains the main hosting ground for malicious webpages. Although China and Russia continue to provide some strong competition, China's share has dropped considerably from 27.7% in 2008 to 11.2% in 2009.

This continues a trend set in 2008, when China's figure had dropped from 51.4% in 2007. The remainder of malicious pages are scattered all over the world, with Peru moving strongly up the list to fourth place with 3.7%.



Top 10 countries hosting malware on the web

What is SEO, and how are the bad guys using it? ▶ Search

SEO stands for search engine optimization, a standard marketing technique used by many legitimate firms to help promote their internet presence.

SEO involves careful selection of keywords and topics to result in the display of a page when users enter search terms, and manipulation of links between resources to increase a page's popularity and rating in search results sorted based on link rankings.

Cybercriminals use SEO to target trending or popular topics, such as major news events or public holidays.

Malicious sites reference trending search terms and are optimized to pull traffic from search engines.

Custom tools are for sale on underground cybercriminal forums to generate content that seems genuine and to interlink pages across domains for the most exposure.

Page visitors are subjected to malware attacks that target browser vulnerabilities, scareware scams and more.

Reducing web risks

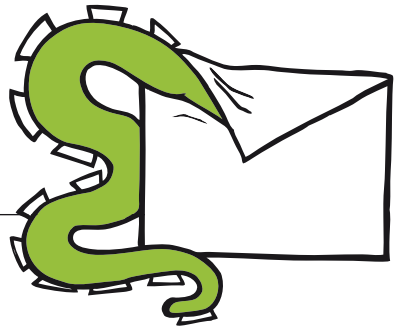
Web threats present a major problem for businesses as more employees require access to the internet to do their jobs. The "walled garden" approach, which limits browsing to a small subset of known safe sites, provides far too little flexibility for most and is really only applicable these days to the most restrictive of parental control regimes.

To reduce risk, web usage must be screened by quality web protection technology, which can detect malware on hacked websites, and respond rapidly to newly emerging malicious domains and URLs. Those who are tempted to try to circumvent the protection should be educated about its value, and prevented from accessing proxies and other security-bypassing systems.

Despite user education about safe web practices, some users will always try to find ways around filters. In this scenario, access to proxies should be as carefully monitored and controlled as access to malicious or inappropriate sites.

The web can be a dangerous place. But by exercising proper care when selecting and implementing security technologies, users can freely access all the resources they need to be productive, while being shielded from the ever-growing danger of malicious and compromised sites.

Email threats



Email malware is far from dead

Although the web has long since eclipsed email as the primary vector for distributing malware, threats spread through email attachments and embedded links have never stopped, and both saw a resurgence in 2009.

Email malware attacks traditionally draw users in with exciting or controversial subject lines, then provide either embedded links or attached files for further information. Inevitably, these links lead to sites pushing malware via exploits while the attachments are either Trojans or use vulnerabilities in Office or PDF viewing software to execute malicious code.

The WaledPak family of malware was dominant in the first half of 2009. It first surfaced in December 2008 as a spam campaign that took advantage of the excitement surrounding the start of Barack Obama's presidency in the US. A barrage of emails claiming to be news about the president led unsuspecting users to sites carrying the malware. The first attack wave commenced almost as soon as the polling booths closed, with a single Obama-related campaign responsible for 60% of all spam emails recorded in an hour-long period in late 2008.[47]

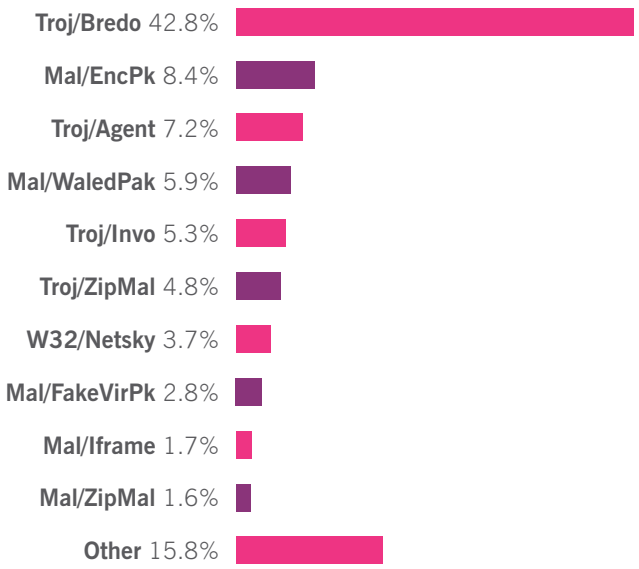
Threats spread through email attachments and embedded links has never stopped, and both saw a resurgence in 2009

A second campaign timed to coincide with the inauguration in January 2009 claimed Obama had withdrawn from the presidency and led readers to Waled-related malware attacks.[48]

Similar campaigns continued throughout the first six months of 2009. Later instances exploited fears of terrorist attacks by disseminating fake stories of a dirty bomb detonated in a nearby city,[49] using Geo-IP data to determine a suitable target close to the recipient. Some of these campaigns included malware attachments, marking the resurrection of a tactic thought at one time to have been abandoned.

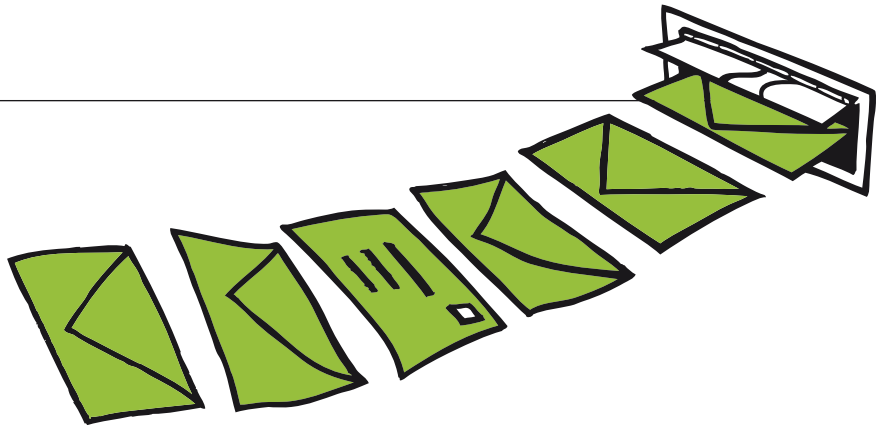
In the second half of 2009, email-borne malware such as Bredolab and related attacks surged. Bredo generally disguised itself as invoices for non-existent purchases or shipments via DHL,[50] FedEx[51] or UPS[52] to propagate. Some attacks also took advantage of the popularity of social networking sites, sending zip attachments claiming to contain new Facebook passwords.[53]

The Bredo outbreaks led to a significant increase in overall infected email. Some old faithfuls, including W32/Mytob, W32/Netsky and W32/MyDoom remained around the top 20 thanks in part to unprotected systems that continued to spread infected emails years after initial infection. However, these attacks constituted a far less significant proportion of the infected attachment problem than in previous years.



Top 10 malware spreading via email in 2009

Spam



Spam remains an important vector for malware propagation. After the takedown of the infamous McColo hosting company, along with several other spam-facilitating services, in late 2008,[54] spam levels immediately dropped by 75%, but quickly climbed back to exceed previous records.[55]

How spam spreads

The majority of spam is sent via botnets of hijacked systems in the homes and offices of innocent users who are unaware of their role in the global spam problem. Botnets represent a valuable resource for hackers, as do the hosting services that provide cybercriminals with server space and bandwidth to host their websites and control centers. And botnet controllers will do almost anything to protect their assets. For example, when the McColo network was shut down, the giant Rustock botnet lost the connection to its command and control system. However, a brief resumption in hosting services allowed just enough time for the network to be redirected to new controllers—and it caused a huge rise in spam levels within days.[56]

While these macro-level efforts have had some success at impeding the efforts of spammers, it remains vital that the controllers of spam botnets are deprived of compromised zombie computers. Everyone can help by ensuring that their computer is kept safe and prevented from assisting cybercrime.

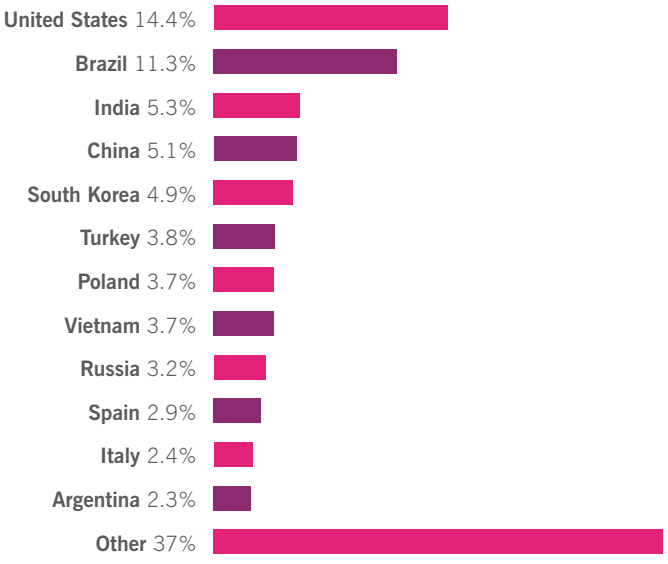
It remains vital that the controllers of spam botnets are deprived of compromised zombie computers

Webmail also continues to be a vehicle for spammers despite the efforts of webmail providers to ensure their users are not automated bots. Unfortunately, a leaked list of logon credentials was discovered in October 2009 that allowed access to tens of thousands of accounts at Hotmail,[57] Gmail, Yahoo! Mail, AOL and other popular webmail services,[58] which proves that spammers continue to develop sophisticated techniques to circumvent controls.

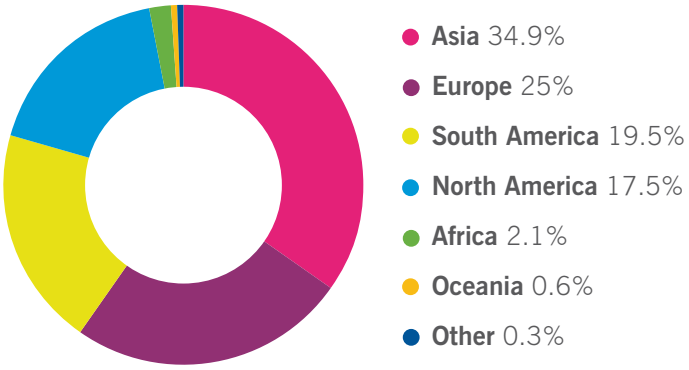
The US once again leads the field of spam-relaying countries contributing 14.4% of the the worlds spam traffic. The only country coming close to challenging American dominance is Brazil, soaring from fifth in 2008 with a mere 4.4% to a strong second in 2009, relaying more than 11% of junk emails spotted worldwide.

Farther down the list, the usual suspects China, South Korea and Turkey remain in the top 10, while India climbed past them from tenth in 2008 to third in 2009. The UK has moved sharply in the other direction, moving from eighth to sixteenth.

When viewed by continent, Asia remains in the lead with 34.9%, relaying more than a third of all spam, with Europe a strong second with 25%. However, both have lost ground to a surging South America, which surpassed North America to take third place, rising from 13.4% in 2008 to 19.5% in 2009. Africa also saw a slight rise, hinting at a growing problem in the future as the developing world becomes more connected to the web.



Dirty dozen spam-relaying countries



Spam by continent

IM and social networking spam

Instant messaging (IM) has become a serious vector for spamming, and social networking spam has also seen a boom. Spammers use hijacked user accounts to message others with phishing or malware links, or take advantage of specific interaction methods of sites such as Twitter, which has seen spammers following real users to trick them into trusting them and following their obfuscated links.[59]

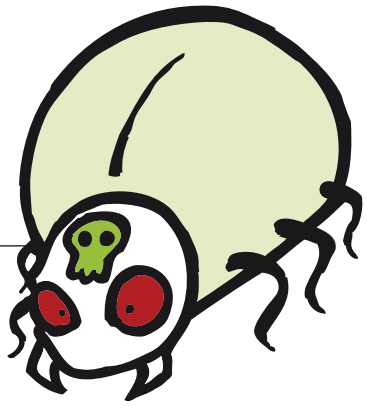
Spammers use hijacked user accounts to message others with phishing or malware links

Other forms of spam

Forum and blog comment spam have continued to be a problem, with many sites defaced with automated messages and carefully crafted attacks. According to the spam filtering service Akismet, 83% of all blog comments are spam.[60] Although sites that are trying to build an active community of participants prefer to allow unmoderated comments, this option will become untenable unless strong protection against spam comments is in place.

In January 2010, the IPv6 internet protocol was used by spammers for the first time as a method of delivering unsolicited email.[61]

Malware trends



Malware: A money-making machine

Malware remains a lucrative business; and because of this, cybercriminals put serious resources behind it.

One key profit-driven malware trend of 2009 was the boom in "scareware," or fake anti-virus security product scams

One key profit-driven malware trend of 2009 was the boom in "scareware," or fake anti-virus security product scams. These attacks 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 advertisements or disguised downloads. 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.

Such scams have taken advantage of the full gamut of vectors to reach new audiences: links sent out via email promising lottery winnings,[62] malvertising surreptitiously planted on legitimate sites[63] or even paid for,[64] messages spread via social networking sites such as Twitter[65] or Facebook,[66] and most deviously the use of search engine optimization.

SEO attacks draw users searching for trending news stories and events, such as the deaths of pop stars[67] or actors,[68] whether real or only rumored,[69] and even genuine security scares.[70] These malware threats are generally web borne, reached via email links or subverted search engine results, and this vector is now by far the dominant method of spreading malware.

Adobe Reader is a key malware target

The return of old-fashioned malicious attachments in 2009 was driven in part by a surge in document format vulnerabilities, most notably in the almost ubiquitous Adobe Reader software for viewing PDF documents.

A broad range of documents are provided in the PDF format, making Adobe Reader a standard part of most users' software battery. This has made the product and others in the company's range of popular packages a prime target for hackers.

In an effort to counteract the increased focus on Reader and Acrobat software, Adobe now issues its own set of security advisories on a routine basis, with updates provided at least every three months.[71] The need for users to keep their software up to date has become more vital than ever. In some cases, doing so has become more difficult because other providers have, knowingly or otherwise, included insecure out-of-date versions of Adobe products with new versions of their own software or OSs.[72]

Conficker worm gains notoriety in 2009

Subverting both email and web browsing protection, the threat achieving the highest profile in the world's media in 2009 was the Conficker (aka Downadup) worm. Conficker spread directly across networks using vulnerabilities in the Windows operating system.

The Conficker worm first emerged at the end of 2008,[73] picking up attention and infecting victims throughout the first few months of 2009. Media hype built up to a climax on April 1st, when some predicted it might deliver an unknown and mysterious payload. Whatever the original plan, the final event was not as devastating as some in the media claimed. Conficker's most serious payload, so far at least, seems to have been delivering scareware scams. It also distributed the Waledpak family of malware for some time.

Although the media frenzy around Conficker quietened down considerably in the second half of the year, and the main vulnerability it targeted is patched,[74] Conficker continues to represent a major issue. In Virus Bulletin's first summary of desktop detection statistics, gathered from a wide range of vendors and published in December 2009, Conficker took top place overall with more than 9% of all detections.[75]

One of the ways Conficker can spread is by exploiting the Windows AutoPlay setting for removable devices, such as USB thumb drives. In most versions of Windows, this option defaults to automatically running executables when instructed to do so by a newly connected drive. With the explosion in popularity of USB-enabled gadgets, this has been a major issue as these devices can serve as vehicles for malware distribution.

Although Microsoft has made some effort to reduce the danger in Windows 7,[76] security experts continue to urge users and admins to disable it wherever possible. Device control mechanisms can protect systems from unauthorized and risky devices, supporting corporate usage policies.

Conficker: One year on

October 2008: In a special out-of-band critical update notice, Microsoft releases details of the MS08-067 vulnerability in the Windows server service.[77] Sophos experts foresee the potential danger of massive worm attacks, comparing the vulnerability to the one that enabled the Sasser worm.[78]

November 2008: The first strain of the Conficker (aka Downadup) worm is spotted in the wild. [79]

January 2009: Conficker reappears with a new strain including added functionality—spreading via USB thumb drives and open network shares[80] using a wide selection of common passwords.[81] In a Sophos survey, while 53% of respondents blame the malware creators and 17% hold Microsoft at fault for allowing the vulnerability, 30% put the onus on system administrators who failed to patch systems rapidly enough to stem the flood of infections.

February 2009: Microsoft offers a $250,000 bounty on the creators of the worm.[82]

March 2009: As details emerge of Conficker-infected systems being set to connect to base on April 1st,[83] media hype begins to build surrounding a potential internet Armageddon on April Fool's Day. [84] Sophos describes the surge in interest as a "hystericane."[85]

April 2009: As media hype turns to scorn following the April 1st non-event,[86] Sophos experts release detailed analysis of the latest variant, Conficker-C.[87] Figures from Sophos show that 10% of systems still haven't applied the MS08-067 patch. [88]

May 2009: Microsoft announces plans to make the AutoPlay system in Windows 7 more secure to counter the use of auto-running by worms such as Conficker.[89]

October 2009: A spam campaign poses as an alert from Microsoft concerning Conficker-B. Links in the emails lead to other malware but keep the Conficker name in the news.[90]

December 2009: Prevalence data reported by Virus Bulletin, aggregated from many different monitoring systems, shows that more than a year after its first appearance, Conficker remains the most commonly detected item by desktop-level anti-malware software.[91]

Other malware vehicles

Not every malware incident in 2009 was entirely malicious or profit-driven. A few incidents unleashed during the year were proofs of concept, or created to show off the creator's skills and knowledge.

The W32/Induc virus, discovered in August, introduced a whole new concept in file-infecting malware in that it spread by infecting compiler software for the Delphi programming language. With no other payload, the malware apparently only targeted software developers.

There's no such thing as harmless malware

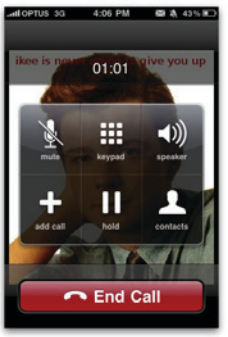
[92] [93] But large numbers of infected files were discovered in the wild after it managed to penetrate some serious software houses[94] and infected packages made their way onto magazine CD covers.[95]

The "Rickrolling" phenomenon, which tricks web users into watching a famous clip of 1980s British crooner Rick Astley, also caused quite a stir in 2009. A Trojan found in February opened the now infamous YouTube clip on a regular basis on infected systems,[96] while a worm heralded as the first to hit iPhones changed users' wallpaper to show a picture of Astley.[97]

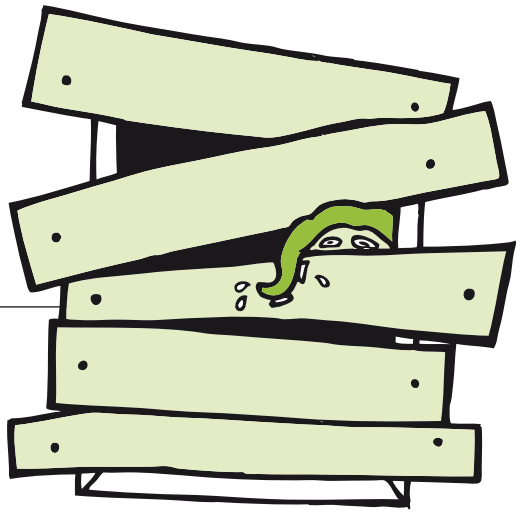
Such incidents may seem innocent and funny to their creators, but there's no such thing as harmless malware. Lack of testing and quality assurance by virus writers can lead to serious damage even if there is no malicious intent. Any malware capable of spreading, for instance, can end up draining bandwidth and CPU resources.

At the very least, the ever-growing explosion in malware numbers adds to the workload of security research teams, and may increase the size of updates for customers.

Sophos's global network of labs received around 50,000 new malware samples every day during 2009.



iPhone worm



Windows 7

New platforms, new challenges

In late 2009, Microsoft released its latest operating system, Windows 7, putting itself in the firing line for future malware attacks.

Windows received a major upgrade a couple of years ago with Windows Vista, but adoption by consumers means that most are still running Windows XP. Released in 2001 and the dominant computing platform of the entire decade, XP remains the key target for cybercriminals, hosts most of the malware infections, contributes computing power to the botnets and sends out most of the spam.

So the release of Windows 7 as a replacement—one that should hopefully eliminate the problems that dogged Vista and break through to mass acceptance as the platform of the future—presents a great opportunity to reduce the security vulnerabilities that led to the malware and cybercrime explosion of the past decade.

Windows 7's main security shortcomings are few, but significant

Windows 7 security features

A glance through Windows 7 features reveals that Microsoft has paid serious attention to security issues:

- The User Account Control (UAC) system has been reworked to produce fewer irritating popups. Microsoft hopes that this will reduce users' reflex response to simply click on anything to make popups go away. Although a clear improvement, the UAC still places a great deal of responsibility for securing systems on untrained end users.
- Disk-level encryption is provided via BitLocker. However, because BitLocker is only available in the most recent and more expensive Windows platforms, there is still great risk for data loss.
- The firewall is now a fully featured protective barrier, and should offer good protection for home users lacking the gumption to source and manage their own firewall. However, corporate security admins may find the learning curve of a new style of group management a little steep compared to tried-and-trusted third-party methods applicable across multi-platform networks.

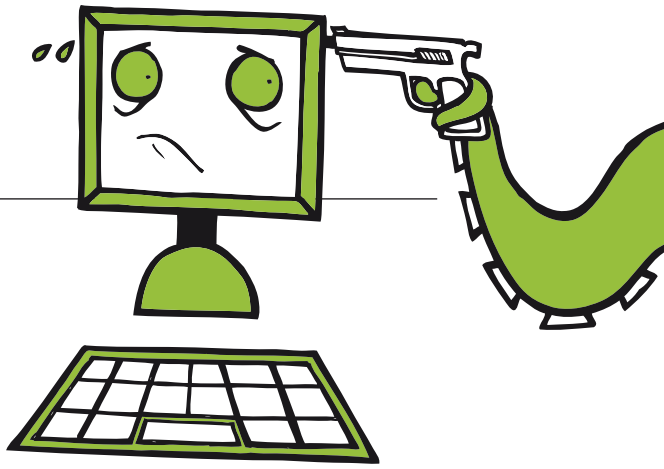
Windows 7's main security shortcomings are few but significant. The changes to the former Security Center, now called the Action Center, are mainly positive, with more granularity provided for security solutions to keep the OS informed of their status, and more detailed alerts provided to keep users up to date on what problems they may face.

But the alerts—notably the system tray icons used to replace the old shields—may be too obscure and subtle for users to take notice. An old issue also recurs: The file extensions are hidden by default. This has been a problem for many years, and many security experts have called on Microsoft to fix it. The default behavior allows malware writers to disguise executables as files such as FriendlyPicture.jpeg.exe—with the .exe part invisible to most users.

Overall, Windows 7 provides a more secure environment but there is still room for improvement

Overall, Windows 7 provides a more secure environment, but there is still room for improvement. When the first few versions of Windows XP came out, there were some much more serious issues than those seen with Windows 7—and many were fixed with Service Pack 2. Whether Windows 7's security will be properly completed with its first service pack remains to be seen.

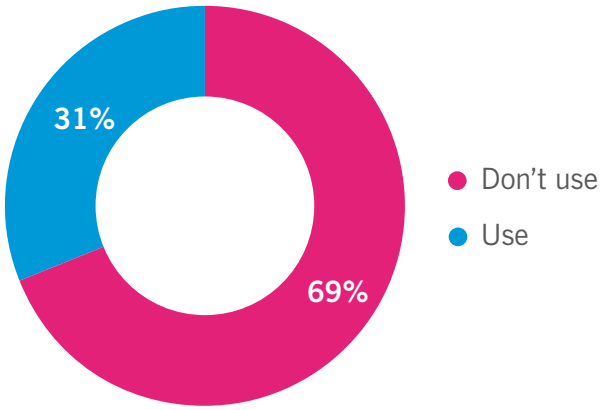
Apple Macs



Soft but significant targets

Microsoft was not the only company to release a new OS in 2009. Apple's release of Mac OS X v10.6, or Snow Leopard, brought the tacit acknowledgement by Apple that malware does affect its platform when it introduced rudimentary anti-malware protection.[98] [99] Although Snow Leopard only prevents installation of a small selection of known Trojans via a limited set of vectors,[100] it does show a slight thaw in Apple's attitudes toward malware.

However, with 69% of Mac users surveyed by Sophos in mid-2009 not using any anti-virus software to protect themselves, their systems and their data, the issue of Mac malware and phishing remains a serious one.



Do you use anti-virus to protect your Mac?

Timeline of Mac malware 2009

Malware targeting Macs discovered during 2009 included:

January: The OSX/iWorkS family of Trojans, which posed as pirated copies of Apple's iWork [101] and Adobe's Photoshop CS4[102]

March: OSX/RSPlug-F, again posing as hacked/cracked files[103] using social engineering to get users to install it[104]

May: OSX/Tored, an email worm claiming to be building the first Mac OS X Botnet[105]

June: Trojans posing as ActiveX components required to view pornographic videos[106]

June: Links sent via Twitter leading to a supposed sex tape featuring TV star Leighton Meester, actually Trojan OSX/Jahlav-C[107]

July: OSX/Jahlav-C again, this time placed on sites created to take advantage of widespread rumors of a peephole video featuring ESPN TV reporter Erin Andrews [108]

August: OSX/Jahlav-C returns, disguised as an installer for MacCinema software[109]

August: OSX/Jahlav-C once more, this time hooking on Twilight movie star Ashley Greene and posing as QuickTime updates[110]

November: OSX/LoseGame-A, a bizarre example of malware that posed as an old-fashioned Space Invaders game and openly deletes users' files (It is not exactly a Trojan as it is open about its intentions, but nevertheless is a hazard to the unwary user, or non-English speakers.)[111]

All of this malware relies heavily on social engineering and hammers home the message to Mac users that they cannot afford to depend on their operating system's reputation for safety. Anyone can be tricked by subtle scams, and running quality, up-to-date anti-malware software is by far the safest option.

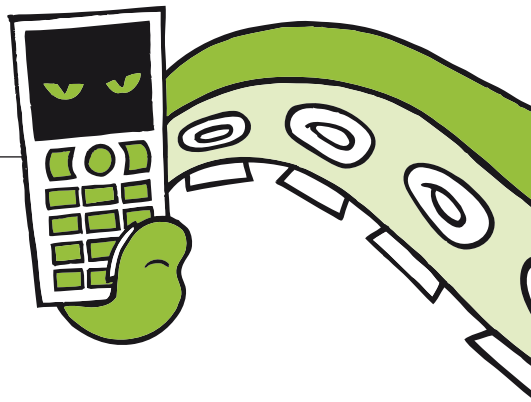
With the release of Snow Leopard, the need for patching software and keeping up to date with the latest vulnerabilities emerged. The Snow Leopard build included a version of Adobe's Flash Player software that contained a known vulnerability, and one that had been previously patched by Adobe.[112]

Snow Leopard included a version of Adobe's Flash Player software that contained a known vulnerability

Adobe® flash®

Because Adobe Flash vulnerabilities are widely targeted for exploit attacks from malicious or compromised websites, this could have opened up users to attack when they rightly believed they were protected. Mac users, like everyone else, need to stay on their toes and give their security the priority it deserves.

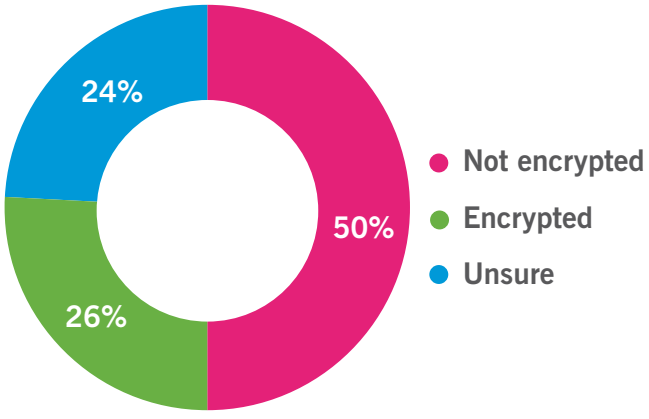
Mobile devices



Mobile devices achieved further market penetration in 2009, with the user base of Apple's iPhone particularly booming. Even without truly common or widespread malicious attacks, mobile device users are still vulnerable to social engineering attacks phishing their sensitive data:

- Touch screens and small displays can assist tricksters by limiting the information available to users, leading users to accept deceptive offers.
- Mobile devices are also commonly lost or stolen. If not properly secured and encrypted, hackers can access the data that's stored on them.

A survey conducted by Sophos in late 2009 asked respondents whether their smartphone was encrypted. Twenty-six percent of survey respondents replied that their data was encrypted, 50% said they were not protected in the event of theft or loss of the device, and 24% of respondents were not sure whether their smartphone was encrypted. These results show that further education on the security dangers of mobile devices is required.



Is your smartphone encrypted?

BlackBerry malware

The leading mobile device brands at the moment remain the BlackBerry and the iPhone, and their user base remains largely divided between corporate and home users. The BlackBerry was designed with security much more at the fore and consequently remains the choice for most business purposes. Nevertheless, flaws have been found.

In 2009, a vulnerability in PDF processing was found that could allow code to run on servers hosting BlackBerry services if BlackBerry users attempted to open malicious PDFs.[113] A similar problem emerged—and again had to be patched by BlackBerry developers Research In Motion (RIM)—just a few months later.[114]

In July, the danger of trusting code sent to phones by service providers was highlighted once again, when a firm in the United Arab Emirates planted spyware software on devices. RIM responded with patches to remove the offending software, but user confidence was heavily shaken.[115] BlackBerry devices also have been found playing host to malware that can transfer to Windows systems when the device is connected for updates or charging.[116]

iPhone malware

There is still a need for user education as some iPhone users and members of the Mac community believe Apple's built-in security to be impenetrable, despite clear evidence to the contrary. Theoretical attacks on devices, generally focused on exploiting vulnerable software, have already been posited by researchers.[117]

Some iPhone users believe Apple's built-in security to be impenetrable, despite clear evidence to the contrary

Standard iPhones are sold with a locked-down operating system, allowing only approved software to be installed. However, not all users are content to limit themselves to the capabilities of these locked-down phones, and unlocking, known as jailbreaking, has become a fairly common practice. The dangers of this were brought to the fore in November with the Ikee worm that spread in the wild.

Subsequently, more malicious attacks on jailbroken iPhones highlighted the risks posed by unskilled users hacking their devices. Apple continues to notify users that jailbreaking violates the user agreement and engaging in this activity places the user at risk.

Ikee and Duh timeline 2009

November 8: The first reports of the Ikee worm emerge from Australia—jailbroken phones with unchanged SSH passwords have wallpaper set to an image of former pop heartthrob Rick Astley.[118]

November 9: With reports of the world's first iPhone worm rife, Ikee author Ashley Towns tells the media via Twitter that he initially infected 100 phones.[119] A Sophos poll reveals 75% of respondents believe Towns did iPhone users a favor by pointing out the danger.[120]

November 11: Tools to exploit unprotected SSH services on jailbroken iPhones to steal data are discovered.[121]

November 23: A malicious take on the Ikee attack begins to spread, connecting hijacked devices to a botnet of iPhones.[122] The worm is dubbed "Duh" thanks to comments in the code.

November 26: Towns is offered a job with iPhone app firm Mogeneration.[123]

```
/*
  People are stupid, and this is to prove it so
  RTFM. its not thats hard guys
  But hey who cares its only your bank details at stake.
*/

// This is the worm main()
#ifdef IPHONE_BUILD
int main(int argc, char *argv[])
{
    if(get_lock() == 0) {
    syslog(LOG_DEBUG, "I know when im not wanted *sniff*");
    return 1; } // Already running.
    sleep(60); // Lets wait for the network to come up 2 MINS
    syslog(LOG_DEBUG, "IIIIIII Just want to tell you how im feeling");
    char *locRanges = getAddrRange();
    // Why did i do it like this i hear you ask.
    // because i wrote a simple python script to parse ranges
    // and output them like this
    // THATS WHY.
```

Ikee code

Towns is offered a job with iPhone app firm

Google Android, Palm Pre and Nokia Maemo

The rival platforms challenging the big two are led by devices running Google's Android OS, the Palm Pre and Nokia's full-blown Linux variant Maemo. The degree to which hackers will focus on them will be determined by the growth of their user base. Only time will tell whether they will prove more or less secure than the current smartphone market leaders.

Early Android malware is already being encountered. In January 2010, an app developer called 09Droid created applications that posed as a shell for mobile banking applications, and in the process phished personal information about the user's bank accounts.[124] The information presumably would have been used for the purposes of identity theft.

The Android marketplace is not as closely monitored as Apple's and it adopts an "anything goes" philosophy. This, combined with the current buzz around new phones running Android such as the Motorola DROID and the Google Nexus One, may make the platform more attractive to cybercriminals in the future.

The "anything goes" philosophy may make Android more attractive to cybercriminals in the future

As more users inevitably take advantage of smartphones to access their bank accounts, the temptation for hackers to exploit systems may become greater.

One thing is certain: Whatever protective features are put in place, users will remain vulnerable to social engineering and—as devices become more feature rich and valuable, and especially as direct mobile payment becomes more mainstream—simple theft. The future may well be mobile, but it certainly will be fraught with cyberdanger.

Cybercrime

Malware has evolved throughout the past decade to become a major industry in itself. It has a complicated economic infrastructure and a population of well-organized, well-funded criminal gangs; highly motivated and highly trained programmers churning out massive volumes of malicious code and exploits; and talented creatives thinking up new and more sophisticated methods of bypassing the weakest link in any electronic security system—the human mind.

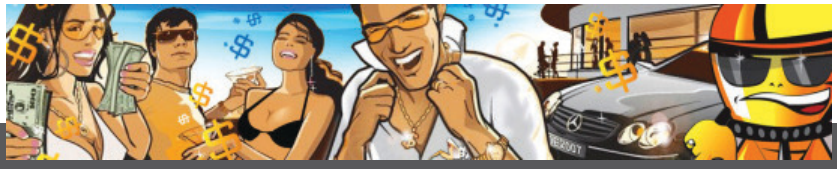
The cybercrime economy

The monetary profits from cybercrime are immense. Because of this, the amount of resources dedicated to cybercrime increases enormously each year. With the economic troubles facing the world, the problem has only grown. Honest money is harder to come by, more people are being lured into the world of crime, and programmers who cannot find jobs in legitimate software houses are more easily recruited by criminal gangs.

In addition, it's easier for hackers to trick everyday folks into becoming mules for money laundering, and to cheat them out of their cash or valuable data. Cybercriminals scare people into believing their banking information has been exposed, often through emails. These techniques have risen in tandem with those promising great bargains, such as the online pharmacy and fake deluxe merchandise spam campaigns.

With this ever-growing menace to society becoming more visible to the masses, police around the world have stepped up efforts to combat cybercrime and take down the gangs profiting from it. With coordinated international efforts still hampered by the lack of a global approach to the problem, frameworks for sharing information and resources are showing signs of improving, and a number of arrests and successful prosecutions took place in 2009.

You too can become rich according to the cybercrime affiliate network



Partnerka: Criminal affiliate networks

- Partnerka is a Russian term referring to complex networks of affiliates, all linked by a common desire to make money from the internet. These groups are well organized, dominated by Russians and responsible for a very high proportion of spam campaigns and malware attacks.
- The biggest area of partnerka activity is in online pharmacies promoted through spam and SEO, selling illegal, off-prescription and often unsafe pharmaceuticals. The Canadian Pharmacy group is one of the best known partnerka.
- Partnerka affiliate networks operate businesses focused on all the main underworld money-makers. However, many scareware fake anti-virus scams are run by partnerka organizations, as are many counterfeit goods sites selling fake Rolexes and other high-end merchandise, online casinos (a favorite method for laundering money), adult sites and even dating sites.
- Cash is made directly from sales of fake or illegal goods, and from complex affiliations with pay-per-click or pay-per-install marketing firms, who in turn get paid by often legitimate companies hoping to drive traffic from their own sites.
- Cash also moves around inside the partnerka network, as spammers hire botnets, phishers sell data to carders who process and leverage stolen credit card details, and malware creators sell Trojans and tools, such as automated systems for spamming forums or building websites for SEO manipulation.
- SophosLabs presented groundbreaking research on the scale and breadth of partnerka activity at the 2009 Virus Bulletin conference. Data revealed that a single Canadian Pharmacy spam campaign can net 200 purchases, or $16,000 in revenues, per day, while a successful affiliate webmaster redirecting 10,000 hits per day to a single scareware site can earn up to $180,000 in a year.[125]

The biggest area of partnerka activity is in online pharmacies promoted through spam and SEO, selling illegal, off-prescription and often unsafe pharmaceuticals

Partnerka pharmacy spam

Timeline of cybercrime incidents, arrests and sentencings in 2009

January: A New Zealand safe-cracker is tracked down after police post photos on Facebook.[126]

January: A fired worker at a US restaurant systems company is found guilty of planting malware on his former employer's network. [127]

January: A worker at failed US financial giant Fannie Mae is accused of planting a logic bomb designed to destroy company data. [128]

February: The FBI releases details of a cash machine heist netting $9 million, using cloned cards created with data stolen from hacked WorldPay payment systems. [129]

February: Microsoft offers a $250,000 reward for information on Conficker authors.[130]

March: Members of a UK gang who used keyloggers and spyware in a failed heist of Sumitomo Bank are sent to jail. [131]

March: A Romanian man is arrested in the US and suspected of hacking into Pentagon systems.[132]

March: A member of a gang who sent phishing emails to AOL customers is sentenced to four years in jail.[133]

April: UK police round up a gang of Eastern Europeans and Russians accused of involvement with siphoning money out of banks using Trojan horses.[134]

May: The UK's Serious Organised Crime Agency (SOCA) releases an annual report with details of successes combating cybercrime.[135]

June: In the trial of a Louisiana teacher accused of having sex with an underage pupil, evidence gathered by the girl's mother using spyware is ruled admissible as evidence in court.[136]

July: An Indian man is extradited from Hong Kong to the US, accused of running pump-and-dump spam scams.[137]

July: A 39-year-old Korean man is arrested in connection with denial-of-service attacks on a game ratings board website.[138]

July: Former South Carolina council official Tony Trout is sentenced to 366 days in jail for installing spyware on a colleague's systems.[139]

August: Albert Gonzalez and two Russians are charged with stealing 130 million sets of credit and debit card information from Heartland and others.[140] Gonzalez's plea bargain led to confiscation of property, cars and $1.65 million in cash, and a sentence of 15 to 25 years in jail.[141]

August: Hacker Ehun Tenenbaum pleads guilty to stealing $10 million from US banks.[142]

October: An Australian ATM hacker steals $30,000, but gets two years of probation, community service and fines.[143]

October: Facebook is awarded $711 million in damages from notorious spammer Sanford "Spamford" Wallace, but is unlikely to see the cash.[144]

October: The FBI indicted 53 people in three US states and began arresting them for phishing users' bank credentials[145] and stealing their funds from Bank of America and Wells Fargo Bank as part of Operation Phish Phry.[146]

November: Four men are sentenced to 13 years in jail in the UK for their part in thefts carried out using online banking Trojans.[147]

November: A UK couple is arrested in connection with creating the Zbot (aka Zeus) Trojan.[148]

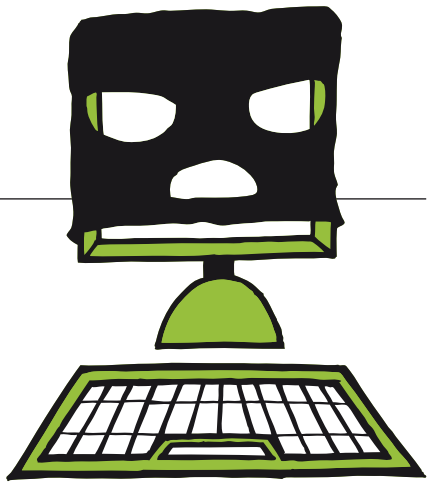
November: The "Godfather of spam" Alan Ralsky is sentenced to four years in prison in the US.[149]

November: The FBI indicts hackers behind a scheme that stole more than $9.4 million from credit card processor RBS WorldPay.[150]

December: Albert Gonzalez pleads guilty to charges related to masterminding the hack into the systems of T.J. Maxx, Heartland Payment Systems, 7-Eleven and supermarket chain Hannaford Bros. Gonzalez is facing a prison sentence of at least 17 years for his crimes.[151]

Albert Gonzalez and two Russians are charged with stealing 130 million sets of credit and debit card information

Cyberwar and cyberterror



Financial gain is not the only motivation behind cybercrime. There are growing fears that crucial infrastructures may be vulnerable to remote hijacking, unauthorized control and potentially devastating damage, as terrorists shift their focus to new areas to spread panic.

There have been no confirmed incidents of core physical services such as power and water supplies, nuclear power stations or traffic control systems being exploited by cyberterrorists to date. However, some hints of the potential danger of such attacks have been hypothesized by researchers.[152]

There are growing fears that crucial infrastructures may be vulnerable to remote hijacking, unauthorized control and potentially devastating damage

In some countries, the use of computer technologies, hacking and malicious code has become part of the military arsenal. Stolen data has been used to target suspected nuclear sites in Syria[153] and North Korea.[154]

The requirement for such measures has been evidenced by small-scale operations against the websites of government institutions, such as embassies, police and governmental branches, conducted without official sanction or any acknowledged involvement. Nevertheless, many of these incidents have been attributed to agencies of rival nations by those under attack, and by the media of the world at large.

July 2009 saw a major incident as the White House, the Defense Department and the New York Stock Exchange were all apparently targeted by the same attackers who were responsible for problems with equivalent institutions in South Korea.[155] All of these incidents led to accusations of involvement from the North Korean government, but may just as easily have been the work of disgruntled activists acting on their own.

Government involvement in cyberwar in 2009

Several countries already have taken serious steps toward closer policing and protection of internal networks, and potentially building up their own cyber-deterrents:

April: The UK government confirms plans for a £2 billion tracking system to snoop network traffic for criminal or dangerous activity, known as the Interception Modernisation Programme (IMP).[156]

June: The US announces the formation of the US Cyber Command, an official military body dedicated to both defense against cyber-invasion and attacks against enemy computer networks.[157]

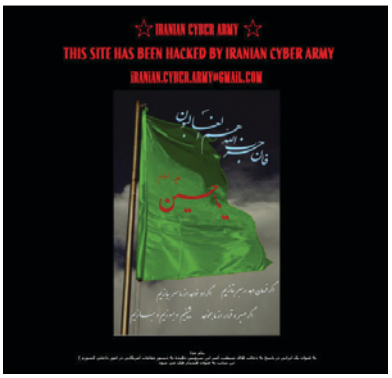
June: The UK announces intentions to form its own equivalent of the US Cyber Command, to be known as the Office for Cyber Security, and refuses to deny that it attacks other countries in cyberspace.[158]

July: A Republican congressman, prominent in the House Intelligence Committee, urges President Obama to take strong cyber-action against North Korea in retaliation for its assumed part in cyberattacks on the US and South Korea.[159]

November: India announces similar plans to the UK's IMP, partly in response to reports that terrorists involved in massive attacks in Mumbai used VoIP and Google Earth to plan and coordinate them.[160] India also suffered spyware attacks at its Education Ministry earlier in the year, which many blamed on China.[161]

December: US President Obama appoints Howard Schmidt as Cyberspace Czar.[162]

In January 2010, Google shocked the internet community by announcing that it (and more than 30 other companies) had been the victim of a targeted hack attack, seemingly focused against the Gmail accounts of Chinese human rights activists.[163] As a result, Google said it was no longer prepared to censor the Chinese edition of its search engine, and would consider quitting the Chinese market if it could not come to an agreement about how to provide uncensored services to the Chinese people.[164]



Twitter hacked

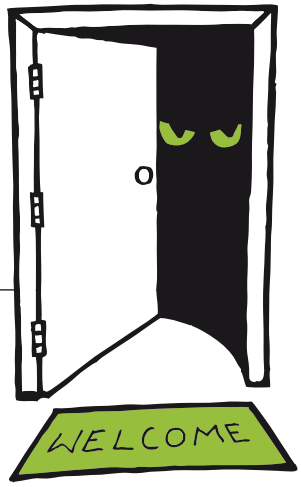
Although the alleged activities of governments have grabbed many headlines in this area, the internet has proved itself to be a viable means of protest for individuals too. Twitter became a vital tool in bringing the views of the opposition to Iranian election results to worldwide attention,[165] apparently with active encouragement from the US State Department.[166]

In December 2009, Twitter Domain Name System (DNS) records were compromised and visitors were redirected to a site claiming to have been hacked by the "Iranian Cyber Army," with many commentators assuming a direct link to the earlier election reports.[167]

Twitter was also hit by political fallout in August 2009, when a major DDoS attack against the site appeared to be targeting a specific anti-Russian blogger based in Tblisi, Georgia.[168]

Governments and political activists alike appear to view the internet as the next major battleground, while both legitimate and more forceful types of political protest have found new homes online. With the web penetrating all areas of our lives, it seems that crime, terrorism and warfare will follow humanity wherever it turns.

The future: What does 2010 hold?



When analyzing the events and incidents of 2009, and those of the past decade, some clear trends and patterns emerge—few of which are encouraging.

The volume of malicious programs, spam emails and infected web pages is increasing, and SophosLabs is seeing a wide variety of techniques being used to penetrate systems.

Hackers will continue to increase the speed and efficiency with which they develop and hone new attacks

Computers and the internet have become so tightly entwined into everyday life that few in the developed world can get by without modern technology. And as the developing world catches up, computers will become even more common.

As a result of the explosion in technology use in the developing world, a significant short-term threat is the increasing number of unprotected, or at least under-protected, systems connected to the global network. This will increase the pool of systems open to infection and available for absorption into botnets pumping out spam and carrying out DDoS attacks. These zombie networks will continue to be a major resource for cybercriminals, providing computing power for a diverse range of malicious and duplicitous activities, and their growth will signal concomitant rises in spamming especially.

Many online computer users may be slow to properly defend themselves, and hackers will continue to increase the speed and efficiency with which they develop and hone new attacks as the cybercrime economy continues to grow.

There is more evidence than ever before that a third motivation is driving cybercrime: using malware and the internet to gain commercial, political, economic and military advantage

Social networking is the current major trend in computer use. It is already heavily under attack and seems likely to continue to become more of a target as its popularity grows. Whether users eventually will be turned off by the rising tide of malware and spam may depend on how providers react and implement measures to ensure security and privacy.

Governments will also play a major role in how secure the networks of the future are, with much greater efforts required to crack down on current cybercriminals and discourage new blood from joining the dark side. These efforts must be implemented at both a local and global level to ensure that crimes and criminals cannot be harbored and abetted by rogue nation states ignoring global regulation. New laws must provide protection from criminals but also ensure secure behavior by those entrusted with sensitive data—who will doubtless continue to leak information in ever-greater amounts, as we have observed throughout the past decade.

The other major power in providing a more secure future comprises the creators and developers of the software and operating systems we use. As technology grows more complicated, the likelihood of mistakes grows with it—and such mistakes in software can often lead to vulnerabilities that can be exploited by malicious attacks. With Google's Chrome operating system on the horizon, and the user base of Apple Mac and Linux distributions such as Ubuntu growing steadily, the global monoculture of Microsoft's Windows finally may be starting to break down. This will almost certainly be a boon for the security conscious, even if merely because of the added diversity of the internet's inhabitants.

However, the rise of cloud-based services inevitably will make users' choice of operating system less relevant to hackers. With more sensitive data being stored on the internet, and the rise of attacks that spread entirely via the internet without having to touch the user's desktop computer, there is the potential for more serious security breaches and for more information to be stolen more rapidly than ever before.

Finally, the accusation by Google that Chinese hackers had broken into its systems and those of other companies, in the hunt for information, may signal that the third age of malware has well and truly arrived.

Hacking and virus-writing began as a hobbyist activity, often designed more to prove how clever the programmer was than to cause serious long-term harm. It evolved into organized criminal activity, with the lure of huge amounts of money driving gangs to steal identities and advertise shady goods to the masses for significant financial rewards.

As we enter 2010, it can be argued that there is more evidence than ever before that a third motivation is driving cybercrime: using malware and the internet to gain commercial, political, economic and military advantage over rivals.

References

1. http://cisco.com/en/US/prod/vpndevc/annual_security_report.html
2. http://www.sophos.com/pressoffice/news/articles/2009/04/social-networking.html
3. http://www.sophos.com/blogs/sophoslabs/v/post/5431
4. http://www.sophos.com/blogs/gc/g/2009/04/12/stalkdaily-twitter-users-warn-attack/
5. http://www.sophos.com/blogs/gc/g/2009/04/12/17yearold-claims-creator-stalkdaily-twitter-worm/
6. http://www.sophos.com/blogs/gc/g/2009/04/12/mikeyy-attack-hits-twitter-users-bad-24-hours-web-20-security/
7. http://www.sophos.com/blogs/gc/g/2009/04/13/mikeyy-worm-madness-twitter/
8. http://www.sophos.com/blogs/gc/g/2009/04/17/mikeyy-worm-targets-oprah-york-times/
9. http://www.sophos.com/blogs/gc/g/2009/04/18/mikeyy-worm-jokes-twitters-expense/
10. http://www.sophos.com/blogs/gc/g/2009/08/25/chinese-social-network-hit-pink-floyd-video-worm/
11. http://www.sophos.com/blogs/sophoslabs/v/post/7248
12. http://www.sophos.com/blogs/gc/g/2009/07/05/mi6-chiefs-wife-puts-security-risk-facebook/
13. http://www.securegoose.org/2009/11/tls-renegotiation-vulnerability-cve.html
14. http://www.sophos.com/blogs/gc/g/2009/12/10/facebook-privacy/
15. http://www.sophos.com/blogs/gc/g/2009/12/01/sophos-bitly-making-short-links-safer/
16. http://www.computerweekly.com/Articles/2007/04/02/222827/tjx-hack-the-biggest-in-history.htm
17. http://www.wired.com/threatlevel/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/
18. http://datalossdb.org/
19. http://www.sophos.com/blogs/gc/g/2009/05/06/hackers-demand-10-million-ransom-wiping-patient-data/http://news.cnet.com/2100-1017-251344.html
20. http://www.sophos.com/blogs/gc/g/2009/05/25/fear-blackmail-raf-loses-sensitive-personal-data/
21. http://www.sophos.com/blogs/gc/g/2009/11/17/tmobile-customers-personal-data-sold-rivals/
22. http://www.sophos.com/blogs/gc/g/2009/11/20/hackers-steal-information-climate-research-unit/
23. http://www.sophos.com/blogs/gc/g/2009/11/27/ico-warns-tougher-penalties-future-data-leaks/l
24. http://www.sophos.com/security/topic/privacy-data-security-compliance.html
25. http://attrition.org/dataloss/2000/01/cduniv01.html
26. http://news.cnet.com/2100-1017-251344.html
27. http://news.cnet.com/2100-1017-253601.html
28. http://attrition.org/dataloss/2001/04/addr01.html
29. http://www.nytimes.com/2002/03/02/nyregion/us-says-ex-prudential-worker-stole-colleagues-id-s-and-sold-them-online.html
30. http://www.sophos.com/pressoffice/news/articles/2005/02/sa_aolemail.html/
31. http://attrition.org/dataloss/2006/06/kddi01.html/
32. http://www.sophos.com/pressoffice/news/articles/2007/03/tjx.html
33. http://www.sophos.com/pressoffice/news/articles/2007/11/hmrc-id-theft.html
34. http://www.sophos.com/blogs/gc/g/2009/08/18/men-charged-130-million-credit-card-identity-theft/
35. http://www.sophos.com/blogs/gc/g/2009/09/14/fake-antivirus-attack-hits-york-times-website-readers/

36. http://gizmodo.com/5390520/apologies-we-had-malware-running-as-ads-on-gizmodo
37. http://www.sophos.com/blogs/sophoslabs/v/post/7388
38. http://www.sophos.com/blogs/sophoslabs/v/post/7032
39. http://www.sophos.com/blogs/sophoslabs/v/post/7056
40. http://www.sophos.com/blogs/sophoslabs/v/post/2827
41. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html
42. http://www.sophos.com/blogs/sophoslabs/v/post/3564
43. http://www.sophos.com/blogs/sophoslabs/v/post/580
44. http://www.sophos.com/blogs/sophoslabs/v/post/6480
45. http://www.sophos.com/blogs/sophoslabs/v/post/4405
46. http://www.sophos.com/blogs/sophoslabs/v/post/7342
47. http://www.sophos.com/blogs/gc/g/2008/11/05/the-president-elects-first-malware-campaign
48. http://www.sophos.com/blogs/gc/g/2009/01/19/barack-obama-refused-president
49. http://www.sophos.com/blogs/gc/g/2009/03/16/dirty-bomb-news-report-leads-pc-infection/
50. http://www.sophos.com/blogs/gc/g/2009/12/08/danger-lies-bogus-emails-claiming-dhl-facebook/
51. http://www.sophos.com/blogs/gc/g/2009/10/20/malicious-bogus-dhl-fedex-emails-bombard-inboxes/
52. http://www.sophos.com/blogs/gc/g/2009/10/28/ups-invoice-5305325782943-malware-attack/
53. http://www.sophos.com/blogs/gc/g/2009/10/27/facebook-password-reset-confirmation-emails-carry-malware/
54. http://www.sophos.com/blogs/sophoslabs/v/post/1970
55. http://www.scmagazineus.com/spam-back-up-to-pre-mccolo-levels/article/129723/
56. http://www.sophos.com/blogs/sophoslabs/v/post/2028
57. http://www.sophos.com/blogs/chetw/g/2009/10/06/hotmail-heist-update-release/
58. http://www.sophos.com/blogs/sophoslabs/v/post/6330
59. http://www.sophos.com/blogs/sophoslabs/v/post/6719
60. http://www.akismet.com/stats
61. http://blog.mailchannels.com/2010/01/first-ipv6-spam-message-caught-in-wild.html
62. http://www.sophos.com/blogs/gc/g/2009/11/04/bogus-lottery-email-carries-fake-antivirus-payload/
63. http://www.sophos.com/blogs/gc/g/2009/10/27/gizmodo-hit-malware-adverts/
64. http://www.sophos.com/blogs/gc/g/2009/09/15/hackers-bought-ad-space-york-times/
65. http://www.sophos.com/blogs/gc/g/2009/09/21/fake-antivirus-attack-twitter/
66. http://www.sophos.com/blogs/gc/g/2009/02/23/sting-tail-error-check-system-facebook-scare/
67. http://www.sophos.com/blogs/gc/g/2009/10/12/stephen-gatelys-death-exploited-scareware-hackers/
68. http://www.sophos.com/blogs/gc/g/2009/03/19/natasha-richardsons-death-exploited-hackers/
69. http://www.sophos.com/blogs/gc/g/2009/10/21/kanye-west-died-car-crash-hackers-exploit-rumour/
70. http://www.sophos.com/blogs/gc/g/2009/03/10/malware-authors-jump-piftsexe-bandwagon/
71. http://www.sophos.com/blogs/gc/g/2009/05/21/adobe-announces-patch-tuesday/
72. http://www.sophos.com/blogs/gc/g/2009/09/02/apple-ships-vulnerable-version-flash-snow-leopard/
73. http://www.sophos.com/blogs/gc/g/2008/11/27/confick-worm-exploits-microsoft-ms08-067-vulnerability/
74. http://www.sophos.com/blogs/gc/g/2008/10/23/more-information-about-critical-microsoft-vulnerability/
75. http://www.virusbtn.com/resources/malwareDirectory/prevalence/index.xml?200910
76. http://www.sophos.com/blogs/gc/g/2009/05/01/microsoft-improves-autoplay-combat-usb-malware/
77. http://www.sophos.com/blogs/gc/g/2008/10/23/more-information-about-critical-microsoft-vulnerability/
78. http://www.sophos.com/blogs/sophoslabs/v/post/1878
79. http://www.sophos.com/blogs/gc/g/2008/11/27/confick-worm-exploits-microsoft-ms08-067-vulnerability/

80. http://www.sophos.com/blogs/gc/g/2009/01/15/stop-conficker-worm-unpatched-pc/
81. http://www.sophos.com/blogs/gc/g/2009/01/16/passwords-conficker-worm/
82. http://www.sophos.com/blogs/gc/g/2009/02/12/microsoft-offers-250000-head-confickers-author/
83. http://www.sophos.com/blogs/gc/g/2009/03/25/conficker-april-1st/
84. http://www.sophos.com/blogs/gc/g/2009/03/27/hype-april-fools-day-conficker-worm/
85. http://www.sophos.com/blogs/gc/g/2009/03/31/confickers-impact-google-search/
86. http://www.sophos.com/blogs/gc/g/2009/04/01/hype-conficker/
87. http://www.sophos.com/blogs/gc/g/2009/04/01/confickerc-technical-analysis/
88. http://www.sophos.com/blogs/gc/g/2009/04/10/pcs-patched-conficker-vulnerability/
89. http://www.sophos.com/blogs/gc/g/2009/05/01/microsoft-improves-autoplay-combat-usb-malware/
90. http://www.sophos.com/blogs/gc/g/2009/10/19/beware-fake-microsoft-alerts-regarding-conficker-worm/
91. http://www.virusbtn.com/resources/malwareDirectory/prevalence/index.xml?200910
92. http://www.sophos.com/blogs/sophoslabs/v/post/6117
93. http://www.sophos.com/blogs/sophoslabs/v/post/6189
94. http://www.sophos.com/blogs/gc/g/2009/08/19/w32induca-spread-delphi-software-houses/
95. http://www.sophos.com/blogs/gc/g/2009/08/20/magazine-ships-induc-delphi-virus-cover-cd-rom/
96. http://www.sophos.com/blogs/sophoslabs/v/post/3349
97. http://www.sophos.com/blogs/gc/g/2009/11/08/iphone-worm-discovered-wallpaper-rick-astley-photo/
98. http://www.sophos.com/blogs/gc/g/2009/08/25/mac-os-snow-leopard-include-antivirus-protection/
99. http://www.sophos.com/blogs/gc/g/2009/08/28/snow-leopard-malware-protection/
100. http://www.sophos.com/blogs/sophoslabs/v/post/6269
101. http://www.sophos.com/blogs/gc/g/2009/01/22/reports-mac-Trojan-horse-pirated-version-iwork-09/
102. http://www.sophos.com/blogs/sophoslabs/v/post/2778
103. http://www.sophos.com/blogs/sophoslabs/v/post/3710
104. http://www.sophos.com/blogs/gc/g/2009/03/25/apple-mac-malware-caught-camera/
105. http://www.sophos.com/blogs/gc/g/2009/05/05/lame-email-worm-mac-os/
106. http://www.sophos.com/blogs/gc/g/2009/06/10/mac-malware-adopts-porn-video-disguise/
107. http://www.sophos.com/blogs/gc/g/2009/06/24/leighton-meeter-sex-tape-lure-spread-malware-twitter-users/
108. http://www.sophos.com/blogs/gc/g/2009/07/19/erin-andrews-peephole-video-spreads-malware/
109. http://www.sophos.com/blogs/gc/g/2009/08/12/reports-apple-mac-Trojan-horse-wild/
110. http://www.sophos.com/blogs/gc/g/2009/08/14/ashley-greene-dirty-pics-lead-danger/
111. http://www.sophos.com/blogs/gc/g/2009/11/04/mac-shootemup-zaps-files-game-common-sense/
112. http://www.sophos.com/blogs/gc/g/2009/09/02/apple-ships-vulnerable-version-flash-snow-leopard/
113. http://www.sophos.com/blogs/gc/g/2009/01/14/blackberry-pdf-vulnerability/
114. http://www.sophos.com/blogs/gc/g/2009/05/27/control-blackberry-enterprise-server-pdf/
115. http://www.sophos.com/blogs/gc/g/2009/07/23/blackberry-customers-revolt-after-spyware-scandal/
116. http://www.sophos.com/blogs/chetw/g/2009/10/30/apple-antivirus-detecting-infected-blackberries/
117. http://www.theregister.co.uk/2009/07/02/critical_iphone_sms_bug/
118. http://www.sophos.com/blogs/gc/g/2009/11/08/iphone-worm-discovered-wallpaper-rick-astley-photo/
119. http://www.sophos.com/blogs/gc/g/2009/11/09/worm-author-tells-media-initially-infected-100-iphones/
120. http://www.sophos.com/blogs/gc/g/2009/11/09/75-worm-author-iphone-users-favour-poll-reveals/
121. http://www.sophos.com/blogs/gc/g/2009/11/11/tool-hacking-jailbroken-iphones-discovered/
122. http://www.sophos.com/blogs/gc/g/2009/11/23/lightning-strikes-iphone-malware-malicious/
123. http://www.sophos.com/blogs/gc/g/2009/11/26/ikee-worm-author-job-iphone-app-firm/
124. http://www.sophos.com/blogs/gc/g/2010/01/11/banking-malware-android-marketplace/

125. http://www.sophos.com/sophos/docs/eng/marketing_material/samosseiko-vb2009-paper.pdf
126. http://www.sophos.com/blogs/gc/g/2009/01/13/safecracker-arrested-police-post-cctv-photos-facebook/
127. http://www.sophos.com/blogs/gc/g/2009/01/13/safecracker-arrested-police-post-cctv-photos-facebook/
128. http://www.sophos.com/blogs/gc/g/2009/01/29/fannie-mae-worker-accused-planting-malware-timebomb/
129. http://www.sophos.com/blogs/gc/g/2009/02/05/9-million-stolen-coordinated-global-cash-machine-heist/
130. http://www.sophos.com/blogs/gc/g/2009/02/12/microsoft-offers-250000-head-confickers-author/
131. http://www.sophos.com/blogs/gc/g/2009/03/06/jail-gang-attempted-229m-bank-robbery/
132. http://www.sophos.com/blogs/gc/g/2009/03/20/suspected-pentagon-hacker-wolfenstein-arrested/
133. http://www.sophos.com/blogs/gc/g/2009/03/26/aol-phisher/
134. http://www.sophos.com/blogs/gc/g/2009/04/09/police-arrest-suspected-banking-Trojan-gang/
135. http://www.sophos.com/blogs/gc/g/2009/05/18/cybercrime-fight-successes-soca-report/
136. http://www.sophos.com/blogs/gc/g/2009/06/03/sex-trial-hear-spyware-evidence-judge-rules/
137. http://www.sophos.com/blogs/gc/g/2009/07/08/man-accused-hackpumpdump-scam-extradited-usa/
138. http://www.sophos.com/blogs/gc/g/2009/07/10/south-korean-arrested-denialofservice-attack/
139. http://www.sophos.com/blogs/gc/g/2009/07/16/trout-jail-366-days-installing-spyware/
140. http://www.sophos.com/blogs/gc/g/2009/08/18/men-charged-130-million-credit-card-identity-theft/
141. http://www.sophos.com/blogs/gc/g/2009/09/01/cybercrime-arrests-china-romania/
142. http://www.sophos.com/blogs/gc/g/2009/08/26/notorious-hacker-pleads-guilty-10-million-bank-heist-case/
143. http://www.sophos.com/blogs/gc/g/2009/10/23/pizza-boy-turned-atm-hacker-stole-30000/
144. http://www.sophos.com/blogs/gc/g/2009/10/30/facebook-wins-711-million-spam-lawsuit-money/
145. http://www.nytimes.com/2009/10/08/technology/internet/08phish.html?_r=3&ref=technology
146. http://www.sophos.com/blogs/chetw/g/2009/10/08/operation-phish-phry-hackers-drain-bank-accounts/
147. http://www.sophos.com/blogs/gc/g/2009/11/16/13-years-jail-bank-robbers-Trojan-horse/
148. http://www.sophos.com/blogs/gc/g/2009/11/18/couple-arrested-connection-zbot-Trojan-horse/
149. http://www.sophos.com/blogs/gc/g/2009/11/24/godfather-spam-jailed-years/
150. http://atlanta.fbi.gov/dojpressrel/pressrel09/atl111009.htm
151. http://www.theregister.co.uk/2009/12/30/gonzalez_cybercrime_plea/
152. http://www.infosecurity-magazine.com/view/5217/cyberterrorism-a-look-into-the-future/
153. http://www.sophos.com/blogs/gc/g/2009/11/06/mossad-hacked-syrian-laptop-bombing-nuclear-facility/
154. http://www.sophos.com/blogs/gc/g/2009/05/06/cyberwarfare-unit-operating-north-korea/
155. http://news.bbc.co.uk/2/hi/technology/8139821.stm
156. http://www.theregister.co.uk/2009/04/27/imp_consultation/
157. http://www.govexec.com/nextgov/0609/gates_cybercommand_memo.pdf
158. http://www.sophos.com/blogs/gc/g/2009/06/26/uk-attack-countries-cyberspace/
159. http://www.sophos.com/blogs/gc/g/2009/07/13/republican-urges-obama-launch-cyber-attack-north-korea/
160. http://www.theregister.co.uk/2009/11/27/imp_india/
161. http://www.sophos.com/blogs/gc/g/2009/02/16/indian-government-computers-hit-spyware-attack/
162. http://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html
163. http://www.sophos.com/blogs/gc/g/2010/01/14/google-china-censorship-hacking/
164. http://googleblog.blogspot.com/2010/01/new-approach-to-china.html
165. http://news.bbc.co.uk/1/hi/8099579.stm
166. http://news.bbc.co.uk/2/hi/8104318.stm
167. http://www.sophos.com/blogs/gc/g/2009/12/18/twitter-website-defaced-iranian-cyber-army-hackers/
168. http://www.sophos.com/blogs/gc/g/2009/08/07/twitter-denialofservice-targeting-antirussian-blogger/

Sophos frees IT managers to focus on their businesses. The company provides endpoint, encryption, email, web, and NAC security solutions that are simple to deploy, manage and use. Over 100 million users trust Sophos as the best protection against today's complex threats and analysts endorse the company as a leader.

The company has more than two decades of experience and a global network of threat analysis centers that enable it to respond rapidly to emerging threats. As a result, Sophos achieves the highest levels of customer satisfaction in the industry. The company has headquarters in Boston, Mass., and Oxford, UK.

SOPHOS