

White Paper



2008 Internet Security Outlook

Global Security Advisor Team
January 2008

It is the best of times. It is the worst of times. Whether for business or pleasure, the Internet has become an integral part of our everyday lives. For multinational corporations and individual citizens alike, the Internet has made the world a smaller place, making it easier to get information, collaborate, and keep in touch. But as more business and personal interactions move into the cyber-domain, vast amounts of personal information is being collected, stored, and analyzed. Whether we're collaborating on a strategic business project, making an online purchase, or chatting casually online, our digital footprints have great value to marketers and fraudsters. Our attitudes about protecting our Internet privacy – and the actions we take – can fundamentally change the nature of the Internet.

Malware is a serious issue, and it's getting worse. 2007 was a record year for data loss. Criminals targeted retailers, banks, and other major institutions to steal customers' and employees' personally identifiable information and corporate secrets. Criminals launched targeted attacks at well-known corporations and government entities. In the infamous TJ Maxx intrusion, more than 100 million credit card accounts were stolen. Defense contractor SAIC lost the confidential records of 580,000 military personnel. Details for 1.6 million job seekers were stolen from Monster.com. More than 216 million data records of U.S. citizens have been reported as exposed since 2005, according to the watchdog organization [Privacy Rights Clearinghouse](#).¹ That's a conservative estimate, as data theft is widely under-reported, despite myriad laws and regulations that require corporations to report data loss and security breach incidents.

¹ "A Chronology of Data Breaches," Privacy Rights Clearinghouse.
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

The CA 2008 Internet Security Outlook report is intended to inform consumers and businesses of the newest and most dangerous Internet threats, forecast Internet security trends for 2008, and provide practical advice for protection. The analysis provided in this report is based on incident information from the CA Global Security Advisor team,² submitted by CA customers and consumers from January to October 2007, as well as public information.

Digital Crime Wave

A digital crime wave is rolling over our electronic shores and, if 2007 is any indication, malware shows no signs of ebbing in 2008. Malware is growing at exponential rates. The goal of malware authors is not to create an Internet-busting worm that makes the evening news. Fraudsters use elaborate schemes involving trickery and sophisticated malicious software to steal valuable information from individuals and companies, which they can use or sell. Personal identities, Social Security numbers, credit card numbers, and account credentials for online banking and gaming sites are favorite prizes. Criminals also compromise individuals' PCs to engage in major advertising click-fraud schemes.

Malware has evolved from a cottage industry to a full-fledged fraud economy. Malware is supported by a growing ecosystem, with producers, distributors, and users who collaborate in and across their local geographies. They have adopted businesses practices and software development lifecycle practices similar to legitimate software organizations. Development frameworks allow malware creators to pump out volumes of variants, in hopes that a slightly altered version will slip past

² CA Global Security Advisor contributors to this report include: Brian Grayek, Don DeBolt, Stefan Bertau, and Mark Wade.

security protections. Botnets, or networks of zombie PCs, can be rented out to distribute spam, launch distributed denial of service (DDoS) attacks, or spread malware. Criminals can even buy malware support plans or consulting services.

Attack methods have converged, and blended threats with multiple components are the norm. For instance, a spam e-mail may contain a link to a compromised web server. When you visit a legitimate website, malicious software may be downloaded onto your computer if the site has been compromised by criminals and your browser software isn't up to date. From there, the malicious software on your computer can contact its host server to download more nasty software, such as spyware, a key logger, or a hijacker. Once executed on your computer, the malware can watch what websites you visit and communicate that information to an unseen party. It can download a different kind of malware every day – or even more frequently.

documents, spreadsheets, or videos – that have malware or links to malicious sites. Peer-to-peer file sharing networks are a major vector for malware, and as people download free games, music, or software, they may also unknowingly download harmful software. But you are at risk even if you are not lured by a too-good-to-be true offer in a spam e-mail or frequently visit questionable websites. If your web browser and security software are not up-to-date, and you visit a legitimate site that has been compromised, your computer can be infected as well.

Malware is an international issue, and stemming the tide will require international efforts. Much of the criminal activity operates out of Eastern Europe and Asia and is targeted at industrialized nations where there are large populations of Internet users. In 2007, the preponderance of malware was directed at the United States, although it is a significant issue in Australia, United Kingdom, France, and Germany. Malware is an emerging issue in Latin America, South Korea, and China.

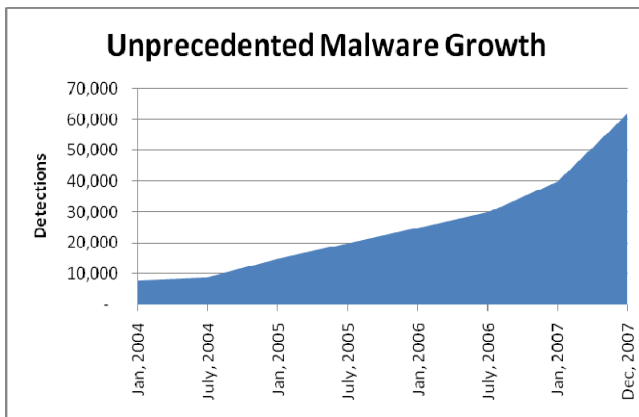


Figure 1: Malware volumes are growing exponentially.

Spam is the preferred distribution method for malware. More than 90 percent of e-mail on the Internet is spam, and 80 percent of spam contains links to malicious sites or malware. The quality of spam is increasing; spam is no longer always obviously a scam and riddled with typos. Spam is laden with attachments – images, PDFs,

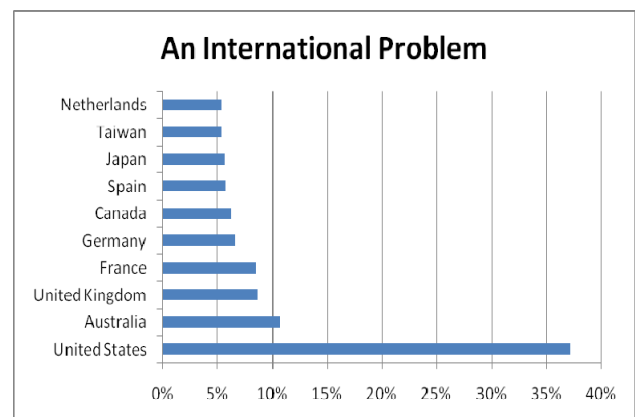


Figure 2: Malware is an international issue, and industrialized countries with large populations of Internet users are most often targeted.

The implications of malware cross economic boundaries into matters of national security. A significant instance of cyber-warfare occurred in

May 2007.³ Massive DDoS attacks were targeted against Estonia government, banking, media, and police websites, and the attacks were widely attributed to the work of the Russian government. Large parts of the Estonia digital infrastructure had to be taken offline to protect the country from attack.

Botnets Dominate

Botnets are a way for criminals to use individuals' PCs without their knowledge, and they are a particularly serious problem for home computers that do not have protected connections to the Internet. The Federal Bureau of Investigation (FBI) has identified 1 million computers across the United States that have been compromised by botnets. Other industry estimates put the figure at 100 million to 150 million PCs captured into botnets.⁴

Compromised computers are networked together in a botnet, and the bot-herder can combine their bandwidth to launch distributed denial-of-service attacks to cripple websites or for processing power for tasks such as cracking passwords. They may also use botnets to send viruses, trojans, spam, or other harmful software to other computers on the Internet.

The good news is that 2007 marks the first time that bot-herders faced real consequences from the U.S. government. The FBI launched a multi-phased program called Operation Bot Roast, which has uncovered more than \$20 million in economic losses.⁵ They've charged individuals

³ "Cyber-Attacks in Estonia: What it Really Means," *CNET*, May 29, 2007.
http://www.news.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html

⁴ "Criminals May 'Overwhelm the Web'", *BBC News*, January 25, 2007
<http://news.bbc.co.uk/2/hi/business/6298641.stm>

⁵ "Operation Bot Roast II: Cracking Down on Cyber Crime," FBI, November 29, 2007
<http://www.fbi.gov/page2/nov07/botnet112907.html>

with computer crimes using botnets to send spam, disable other computers, and infect other computers.

In response to security industry and FBI pressure, bot-herders are changing their tactics, as the explosion of the Storm worm (also known as Tibs) this year, indicates. Botnets are traditionally hierarchical, with a central command-and-control point. But having a single point of control makes it easier for security software detect a botnet. In defense, botnets are shifting to peer-to-peer architectures, because a decentralized bot is much more difficult to detect and ultimately shut down.

In a peer-to-peer botnet, commands and information spread organically. The behavior of a peer-to-peer botnet is akin to ant colony, with specialized functions that adapt on an emergent basis. Each node can see only a few other nodes, and they communicate new information to those nodes. Individual nodes are often highly specialized, and their behavior can change spontaneously as needed. Some nodes may be responsible for the day-to-day work of spamming and attacks. Others may update other members with the latest infections. Others may provide defenses and launch attacks against intruders, which in this case are security researchers or other bot-herders trying to capture machines.

Several bots used instant messaging as their main form of spreading, which proved to be an effective distribution mechanism this year. Prominent families include: Win32/Pushbot, Win32/Weapbot, Win32/Slenfbot, and Win32/Checkout.

The Malware Mix

In 2007, CA Global Security Advisor saw a major shift to malware that is designed to capture private information without the individual's knowledge. The goal is to silently steal credit card numbers, bank account contents, or

gaming accounts. By distributing spam, spyware, and malware, the criminals can further perpetuate their activities. These goals can be accomplished with a variety of types of malware, but most notably with malicious spyware.

For the first time, malicious spyware has bypassed trojans as the most prevalent form of malware. In 2007, 56 percent of the total malware seen by CA Global Security Advisor and CA customers were malicious spyware, 32 percent were trojans, 9 percent were worms, and 2 percent were viruses. In 2006, trojans dominated, at 62 percent of the total malware, followed by worms at 24 percent, malicious spyware at 10 percent, and viruses at 3 percent.

Trojans are highly flexible and they can deliver a variety of payloads. A trojan is software that does something that their programmers intended but that the user would not approve of if he or she knew about it. (CA classifies trojans as malware when they have a payload, similar to viruses or worms and classifies trojans as spyware when the primary activity is to spy on your activities.) Unlike worms, trojans can't spread on their own, so criminals use spam, social engineering, and other tactics to gain access to computers to plant trojans. Worms can be particularly dangerous as they can spread on their own very quickly across the Internet. The most widespread worms this year were simple network and removable drive worms. Some worms cripple computers as they go. Others worms drop additional malware or open the compromised computers to backdoor control by a malicious attacker. A virus is self-replicating code that requires a host (which is usually a file) to "infect." Viruses may delete files, crash your computer, or cause your computer to act strangely. Most viruses today are non-parasitic and use encryption to make it more difficult for security software to detect them.

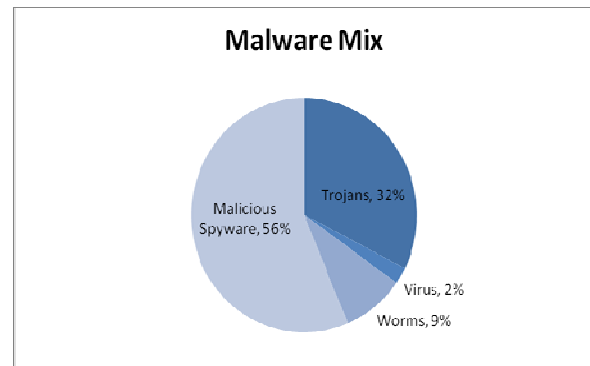


Figure 3: In 2007, malicious spyware overtook trojans as the most prevalent form of malware.

The most common in 2007 was [Win32/Luder](#) (see Table: Top Ten Malware), which is a family of worms that spreads via e-mail and parasitic infection of Windows executable files.⁶ It is a major source of distributing the Win32/Sinteri trojan, which sends spam. Newer variants of this family drop Win32/Pecoan, which receives URLs to download via a peer-to-peer network.

Stealing passwords for online gaming accounts can be more profitable than stealing bank accounts. Gamers use high-performance computers with speedy broadband connections, and they tend to take fewer security precautions than someone who is managing their finances online. Characters, virtual money, and other goods for online games like World of Warcraft are bought and sold in underground websites. The Frethog trojan (No. 2 on the Top 10), which is designed to steal passwords and other information relating to online games, is evidence of the big business of stealing gaming accounts and either using the accounts themselves or selling them to willing buyers on the black market.

Win32/Tibs and Win32/Sintun (both part of the Storm family) took the No. 4 and 6 spots, respectively, in the Top Ten Malware list. The Storm worm began infecting computers in

⁶ Win32/Luder Family, CA Global Security Advisor. <http://ca.com/us/securityadvisor/virusinfo/virus.aspx?id=61119>

Europe and the U.S. in January, 2007, using an e-mail message about a damaging storm in Europe. If the attachment were opened, the computer could be compromised and harnessed into a peer-to-peer botnet. The Storm worm can also install a rootkit. Sintun was prominent this year for its widespread text and image spamming and DOS attacks. Sintun has a distributed command and control structure using peer-to-peer networking protocols as earlier seen in Win32/Pecoan. The trojan also extensively uses social engineering techniques to spread and infiltrate systems. Sintun

also demonstrates server-side polymorphism.

Attackers commonly use packers and encryptors to evade detection by security software. When used for nefarious purposes, packers and encryptors can make a program's contents and structure unrecognizable. For security software to detect a packed program, it must unpack it or contain a separate signature in its database for the program's packed state. Win32/NSAnti, which is No. 7 on the list, detects files that have been packed with NSAnti packer.

Top Ten Malware of 2007				
	Malware Name	Type	Prevalence	What It Does
1.	Win32/Luder	Worm	12.3%	Spreads via e-mail and infection of Windows executables
2.	Win32/Frethog	Trojan	7.3%	Steals online game passwords
3.	Win32/Storark	Trojan	6.4%	Changes system configuration without clear notice to the user, including hooking into the mouse and keyboard, attempting to turn off the Windows Firewall, and altering Windows Automatic Update setting
4.	Win32/Tibs	Trojan	4.1%	Detects Windows executables encrypted with a method known to be associated with Luder, Sinteri and Pecoan
5.	Win32/Pecoan	Trojan	3.6%	P2P file downloader
6.	Win32/Sintun	Trojan	2.8%	Can send spam e-mail and download files
7.	Win32/NSAnti	Trojan	2.5%	Detects files that have been packed with NSAnti packer
8.	HTML/Mallar	Virus	2.4%	Detects HTML files been modified by Win32/Mallar, a polymorphic worm that replicates by exploiting Windows vulnerabilities
9.	Java/ByteVerify!exploit	Trojan	2.4%	Method to exploit a security vulnerability in the Microsoft Virtual Machine
10.	Win32/SQLSlammer	Worm	2.3%	Exploits a buffer overrun security vulnerability in Microsoft SQL Server 2000. Scans randomly generated IP addresses for vulnerable systems and sends out numerous UDP packets, which may cause a denial of service attack on the infected network.

Spyware Dominates

Spyware goes by many forms and names, but its intent is to steal private information and conduct other nefarious activity. That's why spyware has become such a popular tool for cyber-criminals. Adware, trojans and downloaders dominated the spyware scene in 2007. (CA classifies trojans as malware when they have a payload, similar to viruses or worms and as spyware when the primary activity is to spy on your activities.) Adware continues to hold its lead as the most prevalent pest, but last year, hijackers and trojans held the No. 2 and No. 3 spots, respectively.

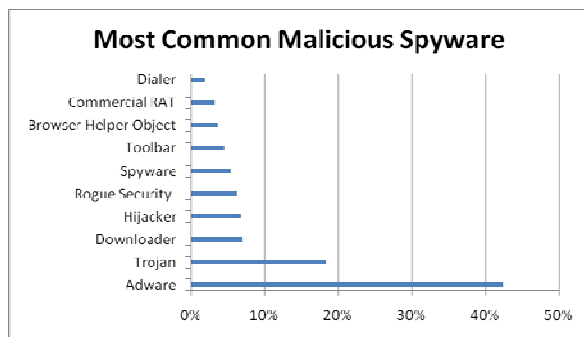


Figure 4: Adware is the most prevalent type of spyware pest in 2007. Trojans moved into the No. 2 spot for the first time.

- Adware.** Adware displays pop-up/pop-under ads where the primary user interface isn't visible or that do not appear to be associated with the product. In 2007, adware accounted for 42 percent of total spyware, which was down slightly from 2006 (at 45 percent). Although there's still plenty of money to be made in adware, the increased use of security software and pop-up blockers in browsers is helping to tamp down this issue. The most common adware in 2007 was Trymedia, which offers games for trial, download, and purchase.
- Trojans.** Trojans comprised 18 percent of all spyware in 2007, which was up from 11 percent in 2006. Trojans are a critical element in many blended attacks, and their popularity among attackers continues to rise. The most

common trojan was Nuvens, which poses as fake applications to download and execute variants of other malware. Nuvens usually appears on websites that promote them as video file-format decoders and applications for obtaining pornography.

- Downloaders.** Downloaders are growing in prevalence because they allow distributors to change the malware more readily. Some downloaders not only distribute spyware and other harmful software, but they also defend against their removal, which allows criminals to extend the lifespan of the malware they distribute. Downloaders accounted for 7 percent of all spyware in 2007. Zlob was the most prevalent, and it is backdoor software that can provide hackers with remote access to your computer.
- Hijackers.** Hijacking is a type of network security attack in which the attacker takes control of a communication. In respect to malware, there are many forms of hijackers, including DNS, browser, error, and homepage hijackers. Each form of the hijacker attacks or takes control of a different type, path, or kind of software. A browser hijacker is a type of harmful program that alters your computer's browser settings so that you may be redirected to websites that you had no intention of visiting, such as resetting your home page. Hijackers accounted for 7 percent of spyware in 2007.
- Rogue Security Software.** Rogue – or fake – security software has been an ongoing problem, and it's indicative of the rising tide of misleading applications. Rogue security made up 6 percent of the total spyware volume in 2007. Rogue security software is typically distributed via online ads for free anti-spyware software. Some of these programs do in fact contain malware or are simply relatively useless against the majority of spyware threats that exist today. After scaring you into believing that your computer has security problems, the rogue security software offers to sell you a license that enables the removal of the supposed problem. After you pay up, the scheme will either undo the threat it installed or offer no fix at all.

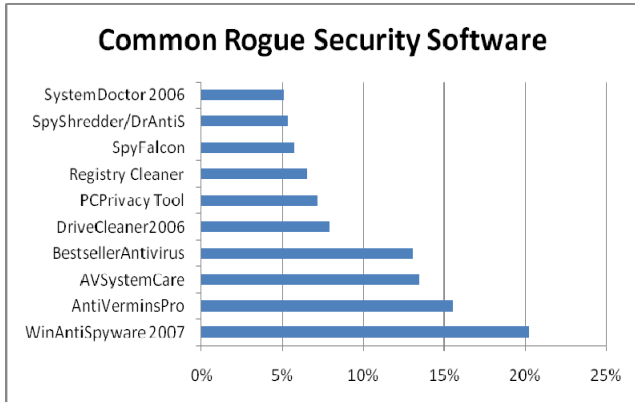


Figure 5: Criminals are increasingly using misleading applications to trick users. Fake security applications purport to remove security threats, but they often do nothing at all – or worse.

More Sophisticated Malware

As the malware industry specializes, the sophistication of malware is rising. Attackers commonly use advanced anti-detection and removal techniques, including polymorphism, packers, and encryptors. They are using misleading applications, such as video players and rogue security software, which actually contain malware to trick users into installing harmful software.

Cyber-criminals are not only more brazen, but also they are cleverer. Another trend is the development of “polite” malware, which doesn’t “kill” its host. A computer may be captured into a botnet, but the malware doesn’t obviously annoy the user, by delivering a multitude of popup ads or downloading multiple toolbars, which may grind system performance to a halt and indicate its presence. Like a symbiotic parasite, polite malware maintains its host, so it can use the computer for longer periods of time to send spam, launch attacks against other computers, or conduct other malicious activities.

Criminals use obfuscation techniques to hide in plain sight, and one growing technique is steganography, which is akin to digital invisible ink. Steganography is a way to write hidden messages so that only the sender and the

intended recipient even realizes that there is a hidden message.⁷ Steganography is often used to hide information in an image by altering the pixels. Criminals are using steganography to smuggle out personal information in innocent-looking e-mail attachments, which can later be sold for identity theft.

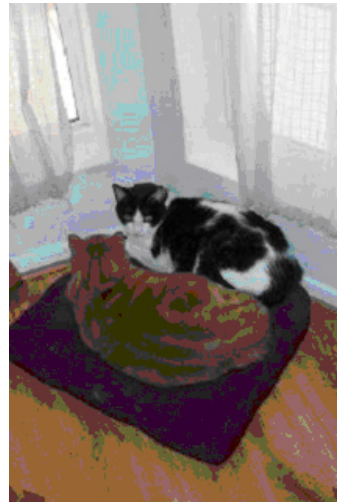


Figure 6: Criminals use steganography to hide personal information in e-mail attachments. This JPEG does not have a hidden message.

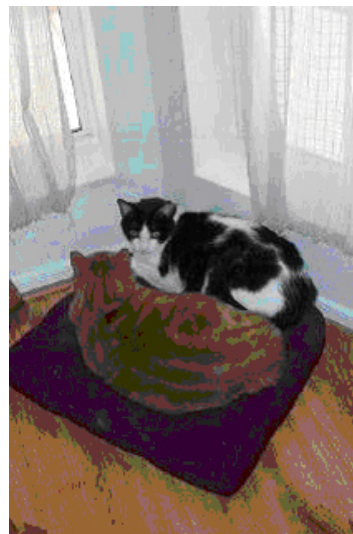


Figure 7: This JPEG has the hidden message: “This is a test. This is a test. This is a test.”⁸

⁷ “Steganography,” Wikipedia. <http://en.wikipedia.org/wiki/Steganography>

⁸ “Steganography Revealed,” Kristy Westphal, Security Focus. <http://www.securityfocus.com/infocus/1684>

Malware authors are increasingly attuned to the work of security researchers, and they are altering their attack techniques in response. Some malware will detect whether it is on a virtualized computer, which security researchers commonly use, but is less often used by consumers. If the malware detects a virtualized machine, it may change its behavior. It may pretend to be broken or do something good. But if that same malware is on a user's machine, it will deliver a nasty payload.

Another rising tactic is the use of fast-flux service networks,⁹ which are networks of compromised computer systems with public DNS records that constantly change, which makes it more difficult to track down criminal activities. A domain name may have hundreds (or potentially thousands) of IP addresses assigned to it. When a person types in the name of the domain, a different IP address may be returned every few minutes. The IP addresses are for compromised computers which host their scams. The scheme is quite advanced, and they often take into account the health of the infected system, so unresponsive systems are taken out of rotation. The Honeynet Project estimates that there are more than 40,000 domains and 150,000 flux IP addresses.¹⁰

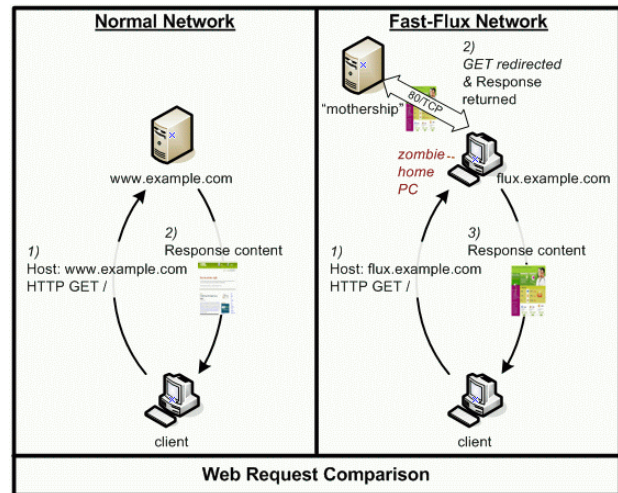


Figure 8: Cyber-criminals are increasingly using fast-flux networks. In such a network, multiple IP addresses are assigned to a fully qualified domain name such as <http://www.example.com>.

Tricked by Social Engineering

As security protections advance, criminals are turning to indirect attacks such as tricking staff into revealing information in social engineering attacks. SANS has placed social engineering attacks on its list of top 20 attack targets.¹¹ The admonitions about not clicking on e-mail attachments unless you are sure they are legitimate ring all the more true with the rise in social engineering techniques. Malware is being incorporated into video players, PDFs, and many other types of attachments. Even experienced users may experience a moment of inattention that can lead to stolen information.

Phishing has evolved into spear-phishing and into "whaling" when aimed at executives. A spear-phishing or whaling attack is a highly targeted phishing attack. The phishing e-mails include information about staff or current organizational issues that make it appear genuine to employees or members within a company, government agency, or organization. The message may look like it comes from the person's employer or a coworker and it could

⁹ "Know Your Enemy: Fast-Flux Service Networks," The Honeynet Project & Research Alliance. <http://www.honeynet.org/papers/ff/fast-flux.html>

¹⁰ "Fast Flux Networks Presentation," The Honeynet Project and Research Alliance. <http://www.honeynet.org/papers/ff/index.html>

¹¹ "SANS Top-20 2007 Security Risks (2007 Annual Update)," SANS Institute. <http://www.sans.org/top20/>

include requests for user names, passwords, or instructions to download malicious attachments from infected websites. Spear-phishing attacks require more research and effort on the part of the criminals, but the rewards are greater. Many of the spear-phishing attacks have been targeted at senior executives at corporations as well as the U.S. military.

Criminals also take advantage of natural disasters and other tragic events that may capture the world's eye. Criminals took advantage of a winter storm in Europe to unleash Tibs, and one can imagine that the U.S. Presidential elections and the Beijing Olympics will present similar opportunities in 2008.

Vulnerabilities Grow

The number of software vulnerabilities is also increasing. Criminals will take advantage of unpatched software, including operating systems, web browsers, Microsoft Office applications, Adobe Acrobat, Adobe Flash video players, and more. In 2007, the NIST National Vulnerability Database reported 6410 software vulnerabilities, which is only slightly less than the 6,600 vulnerabilities reported in 2006.¹²

2007 saw the rise of Apple vulnerabilities. The Mac platform hasn't been a traditional target of attackers, leaving Mac users with a false sense of security. That is changing as Mac market share grows and the platform becomes a viable target for attackers. In 2007, 179 Apple® vulnerabilities were reported, according to NIST. While that's still less than half the number of Microsoft vulnerabilities reported (there were 245 reported Microsoft® vulnerabilities in 2007), it's especially concerning that the Mac holds only 8 percent of the personal computer market (up from 6 percent in 2006).¹³In looking closer at

¹² National Vulnerability Database, National Institutes of Standards and Technology. <http://nvd.nist.gov/>

¹³ "Apple's U.S. Mac Market Share Rises to 8.1 Percent in Q3," AppleInsider. http://www.appleinsider.com/articles/07/10/17/apples_u_s_mac_market_share_rises_to_8_1_percent_in_q3.html

the numbers, Apple Mac® OS X had 78 vulnerabilities in 2007, compared to 28 vulnerabilities in Microsoft Windows® XP and 19 Vista vulnerabilities in 2007. QuickTime® had many more vulnerabilities (34 in 2007) than Windows Media Player (two in 2007). Apple Safari® had only 37 vulnerabilities in 2007 whereas Internet Explorer® had 69 in 2007.

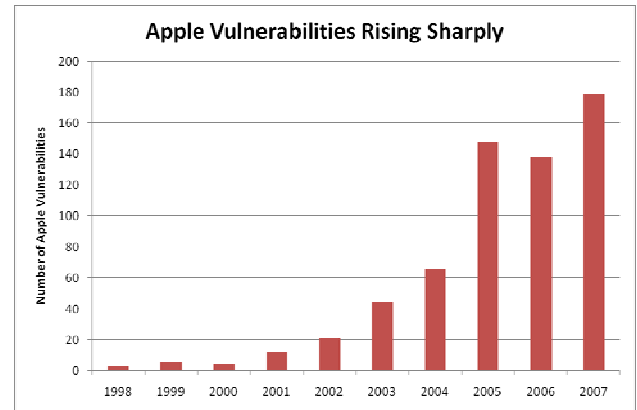


Figure 9: As the popularity of the Apple platforms grow, so do the number of vulnerabilities. Mac users are no longer immune from dealing with attacks.

As the dominant platform, Microsoft Windows represents the richest target for cybercriminals. Windows XP is still the major target, as it is used by many businesses and gamers. However, as Microsoft Vista's market share grows, it too will be in the cross-hairs of cyber-criminals. In 2007, 19 vulnerabilities were reported for Vista, bringing the total reported vulnerabilities to 20. And XP had 28 reported vulnerabilities – which is an improvement over last year's number of 55. It's also important to note that XP vulnerabilities generally also apply to Vista.

Protect Your Privacy and Stay Safe

Much of this report has focused on malware unleashed by criminals, but individuals can protect themselves by making their Internet privacy a priority. Information about who you are, what you're interested in, what you buy, what you look like, and where you are can be recorded forever on the Internet. Your digital

footprints are valuable and deserve more than a second thought.

Facebook, MySpace, YouTube, Flickr, and Dodgeball, just to name a few. Documenting their lives on their favorite social networks has become an obsession with many teens and young adults, and they don't place the same values on their personal information as their parents may. Perhaps it's because they have grown up with technology that they are less wary of it. The social network phenomenon continues to expand. Sites like Club Penguin and Webkinz are targeted toward grade-school kids. LinkedIn, Spock, and others are aimed at business professionals.

Revenues have not been a priority for many of the corporations that run social networking sites, but as they need to develop viable revenue streams they will logically turn to monetizing their audience. Marketing on social networks is uncharted territory, and today's established norms and expectations of advertising and marketing don't apply. It's critical that social networks inform their users how their personal information will be used – and provide them with an explicit choice to participate or not. Individuals need to know what information is truly being collected about them and how it will be used. From a privacy perspective, a program's behavior poses a risk if it involves a user losing control of his or her information.

For instance, Facebook introduced Beacon in late 2007, which feeds information about users' external web usage back to their profile under the 'News Feeds' section. It met with an outcry from privacy advocates.¹⁴ In December 2007, Facebook announced that it will discard user data coming from users who are logged out or who are not Facebook users. Still, in the case of Facebook users, users who have logged in or have selected "Remember me" while logging-in in the past have a higher risk. Facebook

continues to silently transmit data, but with recent changes in their policies, this data is now deleted. (For more on the privacy implications of Beacon, see the CA Global Security Advisor Blog at <http://www.ca.com/us/RSS/preview.aspx?ID=blogs>).

We're in the earliest days of understanding the long-term impacts to privacy in a digital age. If the wrong information is digitized and made publicly available, it can create risks not only to individuals and corporations but to entire governments as well.

Protecting individuals, businesses and even our country's national security against the explosion of Internet crime will take concerted, coordinated efforts. Those efforts start with the individual: It's critical that people act as good Internet citizens. People need to be educated about the serious risks of cyber-crime, both in the workplace and at home. They need to be serious about keeping their computer software up-to-date and to use security software. They need to take their Internet privacy seriously and change unsafe Internet behavior.

Behaviorial analysis can watch systems' actions and stop behaviors that are deemed risky or bad. Enterprises will turn to network access control (NAC) solutions to ensure that computers are clean and comply with corporate security policies before they are allowed access to the corporate network. And consumers who migrate to Internet security suites from disparate point products will find themselves with more comprehensive security protection. This next-generation of computer protection will offer relief, but technology alone cannot solve this problem.

Internet crime is an international issue, and to combat the problem, law enforcement needs to span across geo-political boundaries just as the Internet does. We need the real-life equivalent of NetForce, so presciently foretold in a series of books by Tom Clancy.

¹⁴ "Facebook's Beacon is Improved, But Remains a Threat," CA Global Security Advisor Blog, December, 2007.

<http://www.ca.com/us/RSS/preview.aspx?ID=blogs>

CA Global Security Advisor Internet Security Trends and 2008 Predictions

Malware is at an all-time high. The security industry is in an arms race with malware creators and distributors. If your business or your home computers were fortunate enough to have not been attacked before, chances are increasing that you will become a victim in the coming year. Fraudsters use schemes involving trickery and malware to steal valuable information from individuals and companies, which they use themselves or sell to others in the criminal underground.

- 2007 was a record year for data loss. The personal information of more than 216 million individuals has been exposed since 2005, according to the Privacy Rights Clearinghouse.
- Malware is growing at exponential rates. For the first time, malicious spyware has bypassed trojans as the most prevalent form of malware. In 2007, 56 percent of the total malware seen by CA were malicious spyware (up from 10 percent in 2006).
- Adware, trojans and downloaders are the most common types of spyware, which can be tied to advertising click-fraud schemes and criminals' intent to silently capture personal information from compromised computers.
- Botnets are a serious threat to unprotected consumer and corporate PCs. The vast majority of spam is distributed by botnets. They are also responsible for devastating cyber-attacks and the distribution of most malware.
- Criminals are relying more heavily on social engineering tactics to trick users into giving up valuable information. Phishing attacks are increasing in sophistication and are being targeted at key individuals in corporations and the government.
- A legion of software vulnerabilities create vast opportunities for criminals to exploit and turn into attacks. In 2007, 6410 software vulnerabilities were reported, which is only slightly less than the 6,600 vulnerabilities last

year, according to the NIST National Vulnerability Database.

- Twenty vulnerabilities were reported for Apple platforms, including Mac OS X and the iPhone, according to NIST. Mac users can no longer be lulled into a sense of security.

Eight Security Predictions for 2008

- 1. Bots will be the dominant issue for 2008.** The Federal Bureau of Investigation (FBI) estimates that 1 million computers are part of botnets today, and despite the positive impact of the FBI this year, the number of computers enslaved in botnets will grow sharply in 2008. There are too many unprotected systems, and unfortunately, many consumers "believe" they are adequately protected. The mainstream anti-virus solutions don't provide that protection because of the advances from latest threats and without adequate protection, it's too easy to get infected today. Also once infected, it's very difficult to detect that infection, as botnets increasingly behave as a wolf in sheep's clothing. Not enough people are running software that will protect them, and malware authors are getting stealthier. Botnet operators are behaving more "politely" so their presence on a compromised computer is hidden better, which allows a longer period of survival and malicious action before detection. Botnets will continue to become smarter and more devastating. Consumers must continue to receive further education on the need to include anti-spyware, intrusion prevention, and website inspection solutions, as well as be more selective in their surfing habits.
- 2. Web 2.0 services and sites will come under targeted attacks.** The industry is transitioning to Web 2.0 technologies, such as AJAX, and that move will create significant security risks in the coming year. While it's relatively easy to implement Web 2.0 services, it can be quite challenging to

configure them to be completely secure. Many Internet sites that utilize Web 2.0 services are wide open and are easy to break into. And too many improperly configured implementations equals lots of targets. If a website using Web 2.0 technologies has been compromised, there's little outward indication to a site visitor, whose computer may be infected all the same. Many Web 2.0 implementations are simply not concerned with security, and just like Typhoid Mary, they will infect innocent bystanders because of their complacencies.

3. Gamers will be the "lambs" of 2008.

Even the technically savvy users are currently being victimized in new ways never before considered possible. Online gamers are already a prized target, and stealing account credentials for online games is a primary objective of Internet criminals. Gamers typically run high-end gaming computers with high-bandwidth Internet connections – and they're usually not concerned about protecting themselves or their systems in the same way a business owner would protect theirs. Studies show that the typical online gamer is 26 years old and technically savvy, yet most don't realize the value of their virtual assets until those assets have been stolen. And virtual money isn't recognized by the authorities as something to protect. In 2008, we will see an increase in thefts of virtual assets, which are currently being sold for real life money.

4. Social networking sites will continue to provide helpless victims. MySpace, Facebook, and YouTube will continue to be in the cross-hairs of criminals, because the number of potential victims is large and the average computer security knowledge of the individual is low. Social networking sites will continue to increase in number of users, but there will be a consolidation in the number of sites frequented, largely due to highly publicized intrusions that will continue to attack users. There will be continued controversy about users' privacy rights as social networks figure out how to make money from their members.

5. Windows Vista will become a more appealing target to attackers.

Microsoft Windows Vista has been available for a full year and as businesses and consumers buy new computers, Vista's marketshare will grow. Although Microsoft designed Vista as its most secure operating system, 20 vulnerabilities were reported in 2007, according to NIST. To make matters worse, Vista inherits many of the security vulnerabilities of Windows XP. Additionally, many users find the security precautions overwhelming and they turn them off, which puts them at an even greater risk. As with any other platform, as more people use it, the more attacks will focus on it.

6. Mobile malware will be a no-show.

Mobile devices are more and more safe and despite the rumors of mobile malware on the horizon, smartphones and other mobile devices will not represent a real opportunity for criminals in 2008. Proof-of-concept malware for mobile devices has not yet translated into any meaningful attacks. The only significant mobile vulnerability issue reported in 2007 related to the Apple iPhone.

7. Smarter malware. As the malware industry becomes increasingly specialized, we'll continue to see new levels of sophistication in malware. Peer-to-peer botnets will grow. More malware that targets virtualized computers are in the cards for 2008. We expect to see increasing use of obfuscation techniques, including steganography and encryption, as criminals hide their activities. The CA Global Security Advisor expects to see more malware using distributed or peer-to-peer protocols, such as Win32/Pecoan, uses. We also expect to see more malware implemented in kernel mode or system driver, as seen with Win32/Sintun. This means that instead of seeing malware doing its work as an executable or DDL file, as we commonly see today, we'll see more malware wreaking havoc on system drivers. As a system driver, the malware has more access and can do more damage to a computer.

8. Take advantage of opportunity. As Willie Sutton is reported to have said when asked why he robbed banks, "Because that's where the money is." Cyber-criminals go where the opportunity lies and take advantage of any and all circumstances. As security protections become better and better at detecting malware, criminals will rely more heavily on trickery to spread malware and steal information. Add to the rise of well-researched spear-phishing attacks the potential for politically motivated attacks. The presidential elections in the US and the Olympics in Beijing both offer a high-profile opportunity for destructive attacks and corruption or outright theft of information.