TREND MICRO™

Securing Your Web World

Trend Micro 2008 Annual Threat Roundup and 2009 Forecast

Table of Contents

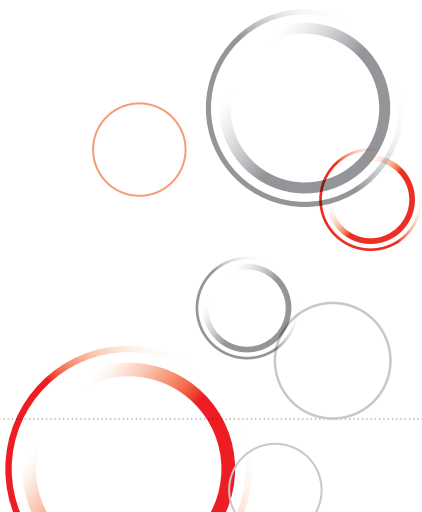
Introduction

Trend Micro publishes its Annual Threat Roundup and Forecast based on information from TrendLabs, Trend Micro's global network of research, service, and support centers committed to constant threat surveillance and attack prevention. With accurate, real-time data, TrendLabs delivers effective, timely security measures designed to detect, pre-empt, and eliminate attacks.

With more than 800 security experts worldwide and 24x7 operations, TrendLabs is headquartered in the Philippines with regional labs in Europe and China. TrendLabs' regional presence and round-the-clock operations enable immediate identification and timely response to targeted, regional threats. As a result, businesses can minimize damages, reduce costs, and ensure business continuity while consumers can protect personal information on home networks.

TrendLabs monitors potential security threats and conducts research and analysis to develop technologies that identify, detect, and eliminate new threats. Using a combination of technologies and data collection methods including "honey pots" for email and network worms, web crawlers, as well as web, email, and IP reputation services, Trend Micro researchers and global, multilingual staff proactively gain intelligence about the latest threats.

By tracking important security threats that impact a worldwide customer base, TrendLabs and Trend Micro technologies detect many threat varieties. A sampling of the most severe and impactful threats that occurred in 2008 are discussed in this report, together with a look forward at the trends and emerging, new threat categories that will make headlines in 2009.



Executive Summary

In the past few years, the number and type of new malware agents have expanded beyond imagination. Approximately 700,000 new malware are identified per month—posing a challenge for security vendors and the traditional pattern file.[1] With the increase in malware has come a dramatic rise in Internet crime. According to a study by the Organization for Economic Cooperation and Development (OECD) into online crime released last summer, an estimated one-in-four U.S. computers is infected with malware.[2] In addition to the staggering number, many threat types have morphed into targeted, combined attacks, rendering sample collection almost impossible.

Unlike the old days when hackers created viruses to be mischievous and to "show they could," modern-day malware authors create threats primarily to make a profit. As the Underground Economy has grown and flourished into a multi-billion dollar industry, cybercriminals have developed new methods for tricking PC users.

In 2008, a series of mass compromises showcased the dangerous potential of today's criminals to launch wide-scale attacks that affect a range of innocent-looking sites. Gone are the days when users could simply refuse to open attachments from unknown senders to avoid infection. The majority of today's infections arrive via the web—hiding on legitimate-looking web pages, lurking behind convincing warnings for fake antivirus software, hidden under fake digital certificates that once indicated sites were safe.

Dramatic and daring exploits were revealed in 2008, such as DNS changing malware that exploits a recently revealed vulnerability that can literally route any machine to any other site. The zero-day bug found in Microsoft Internet Explorer in December was similarly shocking in its scope. The identified vulnerability affects almost all versions of Internet Explorer and Microsoft security researchers estimated that as many as one in 500 Internet Explorer users could have been exposed to malware attempting to exploit the flaw.[3]

Ransomware also made a splash in 2008, with a Trojan that encrypts files, making them inaccessible without an encryption key. Experts predict more ransomware in the future, capitalizing on small to medium-sized businesses that lack the IT resources to combat such threats, particularly in a down economy.

In 2008, removable, physical drives became a popular threat vector, especially in Asia. Autorun malware, which infect removable drives, was also on the rise last year. In addition, a rash of incidents involving infected USB sticks are causing companies throughout the world to create new, more stringent policies about the kinds of devices allowed to access the corporate network.

Threat Landscape

Not all threats were new last year, however. The Master Boot Record (MBR) rootkit made a spectacular comeback, with new technology that helps prevent detection. Another oldie—backscatter spam—also reappeared as a recycled threat that became newly effective in 2008.

Predictions for 2009 call for more of the same threats that plagued both home users and businesses in 2008, with new events and occurrences in the New Year that will shape the social engineering techniques that make today's spam so believable. In an effort to help customers prepare for the newest threats, Trend Micro provides the following *Annual Threat Roundup and Forecast* to showcase the malware that made headlines in 2008 and to deliver predictions for 2009. Knowledge of the threat landscape is the most important layer of defense—both for home and business networks. This report serves as a roadmap for all users to better understand both new and existing threats with helpful tips to protect against tomorrow's new malware attacks.

Figure 1: Threat volume continues to increase exponentially

For security-minded IT network managers and individual computer users alike, the digital threat landscape is undergoing radical change. Simply stated, the sheer volume of new threats is overwhelming traditional protection methods. At the same time, the source or direction from which threats attack computers is predominantly via the Internet. By the end of 2008, less than 10 percent of all malicious attacks arrived by threat vectors other than the web.

Meanwhile, the perpetrators of digital threats have become increasingly well organized. The underlying crimes carried out by digital threats are part of larger mass criminal enterprises that rely on quiet, continued operation on a huge scale. Gone are the days when the threat landscape was defined by the occurrences of high impact, single event outbreaks.

Not only are the individual crimes associated with digital threats part of larger criminal operations, an increasing fraction of digital threats themselves are merely piece-parts in composite threat mechanisms that utilize several stealth techniques together to overcome threat protection.

Threat Volume

In the last two years, the perpetrators of digital threats have automated the processes of producing new threat variants. The number of new, unique threats introduced each day has grown so dramatically that some now consider the issue of "threat volume" to rank as high in importance as the growing variety of viruses, worms, and Trojans, etc. (see Figure 1).

Malicious Methods

Historically, cybercriminals have continued to advance their malware development skills, and the security industry has responded with new technologies to combat threats. Most recently, however, cybercriminals have exploited an inherent weakness in the traditional approach to protection. As content security companies discover new threats and develop countermeasures, this newly acquired threat knowledge must be deployed to all protected computers and networks. Even if the threat discovery process could keep up with the increasing volume of new threats, eventually it becomes logistically overwhelming to deploy updated protection throughout the world.

Conventional malware protection involves gathering samples of malware, developing pattern file fixes, and then quickly distributing these pattern files to protect users. Because many Web threats are targeted, combined attacks, collecting samples is becoming almost impossible. Also, the huge and growing number of variants uses multiple delivery vehicles (i.e., spam, instant messaging, and websites), rendering standard sample collection, pattern creation, and deployment insufficient.

Traditional virus detection processes are also challenged by a fundamental difference between viruses and evolving web threats. Viruses were originally designed to spread as quickly as possible and were therefore easy to spot. With the advent of web threats, malware has evolved from an outbreak model to stealthy "sleeper" infections that are more difficult to detect using conventional protection techniques.

Cybercriminals realize they can overwhelm content protection efforts with the sheer volume of new threats. The volume of new threats is easily increased because of variants—i.e., the same Trojan can change hourly or daily in an attempt to fool security scanners. This means that millions of unique malware can, in fact, represent variants of the same piece of malware. Cybercriminals are also fully aware of the difficulty in issuing updates, and they use this fact to their advantage, creating new malware en masse and as quickly as possible.

Threat Volume Metrics

According to AV-Test GmbH, security vendors collected 1,738 unique threat samples in 1988. At that time, security professionals monitored approximately 30 signatures because samples were easily grouped into patterns.

Ten years later, the number of unique malware samples had risen to 177,615. By 2005, more than double this number were being added every year. But the huge explosion in the volume of unique malware threats has come in just the last two years. In early 2008, the total number of unique threats exceeded 10,000,000, and by the end of 2008 it had reached 20,000,000. On average, over 2,000 new, unique malware threats hit the Internet every hour. It now takes less than a week to produce the entire malware output of 2005.[4]

Findings from TrendLabs confirm these observations. TrendLabs reports more than a twenty-fold (2000 percent) increase in web threats between the beginning of 2005 and the end of 2008 (see Figure 2).

Implications for IT Security

The security industry reacted to the increasing number of malware by issuing more frequent updates. Some vendors switched from weekly updates to daily or even half-hourly updates. The consequent volume of updates has significantly impacted the system and network resources required to manage pattern downloads, often leading to critical performance and cost issues.

For example, imagine the bandwidth required to issue frequent updates to users' machines in a company with 250,000 global employees. A single pattern file update requires at least five hours for deployment throughout the company, and some companies receive updates as often as eight times per day to ensure the latest threat protection. Additionally, many large organizations first test pattern files in a lab or controlled environment before deploying them across the network.

As updates grow more numerous, network administrators spend greater amounts of time managing updates. Remote or mobile workers are particularly vulnerable as they may not receive pattern file updates for hours or days, depending upon how long they are off the company network. Clearly, continual pattern file updates of this magnitude are not sustainable over time.

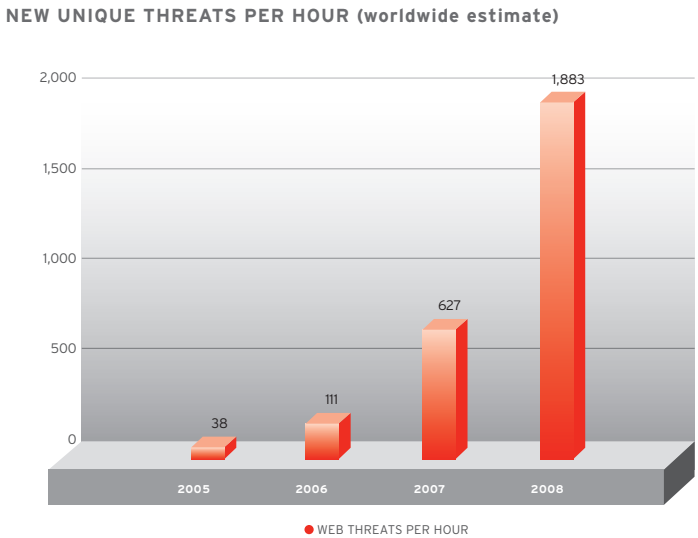


Figure 2: Steady increase in web threats

Threat Vectors

In the old days, digital threats propagated through computer networks using self-replication methods that have come to define the concepts of "computer virus" and "computer worm." With the near universal connectivity of computers via the Internet, this process of self-replication is largely superfluous. Most malware files today contain some form of non-replicating Trojan. Each instance of a Trojan or a Trojan-like malware infects an individual computer. If the Trojan needs help updating or requires a place to send stolen information, it simply uses the Internet to accomplish these additional malicious purposes.

In late 2008, a TrendLabs study tracing threat vectors of a large number of computer infections showed that over 90 percent of all digital threats arrive at their targets via the Internet through a multiplicity of methods. Next to the Internet, the second most common physical threat vector is via file transfer using removable media like USB drives. These account for approximately eight percent of all threat vectors. (see Figure 3).

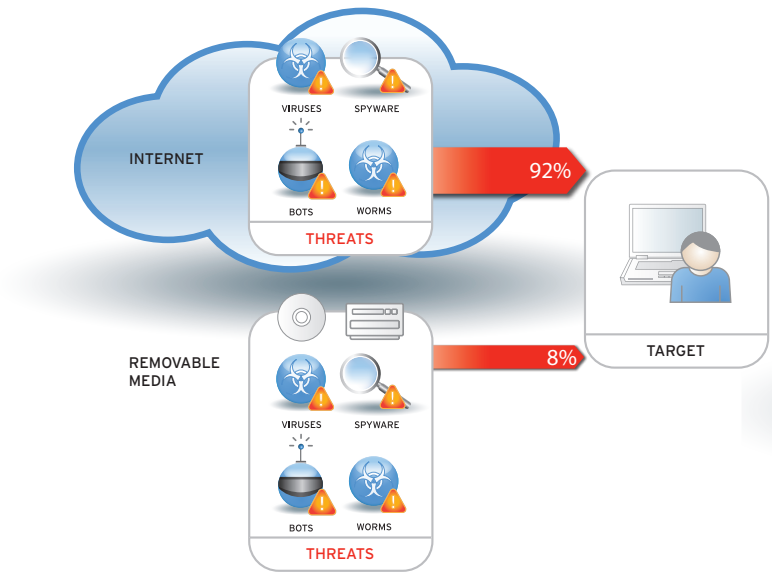


Figure 3: Most threats arrive via the Internet

Malicious Methods

Today's web threats frequently combine a number of seemingly innocent programs to create an infection chain. For example, individual downloader programs, commonly used as part of web threats, may appear benign. Yet when used to download malware onto an unsuspecting user's PC, the program becomes malicious, rendering file-based heuristic scanning ineffective.

Web threats often expand this technique to include multilayered, multiprotocol coordinated attacks to avoid detection by conventional means. For instance, a cybercriminal embeds a URL in an email or instant message. The user clicks on the link to a legitimate URL that was hijacked by the cybercriminal for a few days or hours. Then an ActiveX control tests the vulnerability of the user's browser. If a vulnerability is detected, the malware attacks. If not, it downloads a file, tests for another vulnerability, downloads other files, and so on. Each session appears to be benign, but the combined activities become a coordinated attack (see Figure 4).

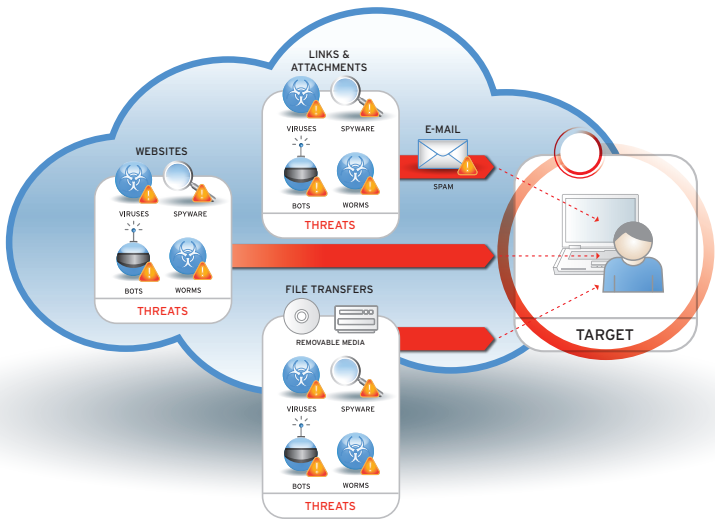


Figure 4: Multilayered, multiprotocol attack

Implications for IT Security

From a protection perspective, web threat vectors possess an inherent weakness in that security researchers can discover their origin. Whether they originate as emails, web pages or downloaded files, web threats originate from a computer connected to the Internet via a knowable domain or IP address—much like the return address on a postal letter or the handshake signature on a fax transmission.

In-the-cloud protection, like Trend Micro's Smart Protection Network, allows for the comparison of this information to known domains and IP addresses. The reputation of the source domain of an incoming email or web page host or server of a downloadable file can be stored in the reputation service as

"good", "bad," or "unknown." If the reputation is "good," the transmission is allowed to proceed. If "bad," it is blocked. If it is "unknown," it becomes a trigger to the security vendor's threat research algorithms and researchers to rapidly establish whether it is, in fact, "good" or "bad".

The Underground Economy

In 2008, Trend Micro researchers observed the continuation of a pattern established in 2007 in which cybercriminals employ an increasingly professional approach toward creating schemes and using malware to make a profit in what experts call "the Underground Economy." Unlike the suffering, real-world economy, the Underground Economy continues to thrive and prosper. Criminals were observed in 2008 using more sophisticated techniques than ever before to steal and sell victims' personal information including email logins, credit card numbers, social security numbers, account passwords, PIN numbers, and gaming passwords.

Stolen information is big business for today's cybercriminals. Prices vary based on type of data, time of year sold, valuation of currency, account balances, credit limits, and other complicated criteria. According to a recent article in the Chicago Tribune, some estimate the global cyber-crime business to be generating $100 billion-a-year in profits.[5]

Motivation is simple—online crime pays. For example, the average salary for a Russian professional is approximately $640 per month yet cyber-crime gangs are offering computer programming graduates from Moscow's technical universities up to $5,000 to $7,000 a month.[6] As in the past, Russia continues to be a hotspot for cyber crime. Russian malware is bought and sold for as much as $15,000 and rogue Russian Internet service providers charge $1,000 a month for bulletproof server access.[7]

According to a recent article in *The Independent*, off-the-shelf malware is sold for $50 to $3,500, depending upon its sophistication, its ability to target victims, the kind of information it steals, and how well it evades security software. Criminals can even subscribe to a service to monitor antivirus developments and tweak malware accordingly for $25 to $60 per month, or can purchase a "premium service" to avoid detection.[8]

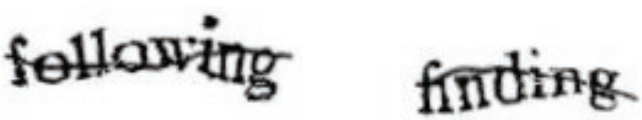


Figure 5: Example of CAPTCHA

Additionally, the article reports that a basic list of unqualified email addresses costs about 1/10th of a cent per address, while botnet services cost about $10 for a million emails.[9] Botnets can also be rented and used for spamming, hacking, and denial of service attacks. An hour of usage on a network of 8,000 to 10,000 computers costs approximately $200.[10]

Credit card details are the most common item bought and sold in the underground. Criminals either use the numbers on their own to exploit victims or sell the numbers on a Black Market online forum for two to five percent of their remaining balances. For example, if the average card on the list had remaining credit of $1,000, each set of details would be worth approximately $25.[11]

Geography also influences criminal booty. For example in Asia, online gaming passwords are all-the-rage and command top dollar. When the Internet Explorer zero-day vulnerability was identified in December, Chinese hackers used the security hole to steal login credentials to online gaming platforms and then sell them online for profit. In addition, virtual gaming is so popular in China that people have actually been murdered for their virtual goods. In Eastern Europe, hackers use the same vulnerabilities for different purposes—usually to steal online banking logins and credit card information. PayPal and eBay accounts are also being bought and traded online. Criminals locate users with high reputation ratings then steal their login data and leverage victims' high ratings to scam consumers.

The methods employed to make money in the underground are growing more sophisticated, actually mimicking the real world. An entire industry of malware software programmers exists, for example, who sell code online just like any real-world software development firm. In addition, cyber crooks employ a small army of work-at-home employees who receive payment for accepting funds from Western Union, for example, or for receiving then re-sending shipments of stolen goods—essentially money-laundering operations. FBI officials are reportedly tracking the correlation between rising unemployment and an increase in web-related schemes that promise large paychecks for a few hours of work per week from home.[12]

Criminal firms also offer money for people who break CAPTCHAs (see Figure 5). The cracked CAPTCHAs are fed into a database that is used to break into Hotmail or Yahoo! accounts or to create fake blogger pages. In this way, criminals can use these accounts to send spam or create fake blog pages that advertise porn, or other desirable web content, for the purpose of enticing users to download Trojans or spyware.

Fake mortgage refinance schemes are also being used to bilk money from already hard-hit homeowners. The spam campaigns promise a better mortgage rate if recipients send money for an appraisal then the criminal makes off with the fake appraisal fee.

Email Threats

One of the reasons for the growing prevalence and profit of cyber crime is the ease with which criminals can launch operations. Free tools abound to create a variety of nasty web threats—from free, pre-made phishing kits to free spam templates that exactly replicate the appearance of popular banking web sites. In March, a slew of phishing kits were discovered built to target top Web 2.0 sites for social networking, video sharing, free email service providers, banks, and popular e-commerce sites.

Many of the kits originated from "Mr. Brain"—a group of Moroccan fraudsters who launched a dedicated web site that advertises free, easy-to-use phishing kits (see Figure 6). Mr. Brain kits have been used to target several well-known banks and other organizations, including Bank of America, Chase, eBay, HSBC, PayPal, Wachovia, Western Union, and many others.

The underground economy will continue to prosper as long as cybercriminals develop increasingly sophisticated malware tools and as long as consumers and businesses lack the proper protections. According to the 2008 breach report from Identity Theft Resource Center, 35 million data records were compromised last year in 656 admitted incidents, compared to the 446 data loss cases reported in 2007.[13]

Computer malware, hacking, and insider theft made up 29.6 percent of overall recorded breaches, while data losses due to human error accounted for 35.2 percent.[14] Businesses and consumers alike will continue to suffer from data leaks, financial losses, identity theft, and damaged reputations in 2009, creating a security environment that is ripe for change.

Implications for IT Security

As cybercriminals employ increasingly complex and distributed methods of attack, defense methods require a wider security net. Understanding the inner workings of single pieces of new malware code is insufficient for creating adequate protection. Just as critical is solving the puzzle of interactions among the malicious piece-parts of malicious spam, compromised web sites, and downloaded malware files.

Figure 6: New threats composed of multiple components

The evolution of threats from mere files transferred through floppy disks to the sophisticated, blended web threats of today poses a unique challenge for the content security industry. New threats are now composed of multiple components, some of which may be non-malicious on their own. These threats are hard to detect since they require catching the malicious aspects of each and every component.

While malicious spam attachments have been infecting users for years, 2008 saw a huge increase in spam that employed social engineering techniques. In January and February, for example, several targeted attacks occurred using Trojanized Microsoft Word files embedded with malicious code. The files (in reality, Trojan downloaders) were sent as attachments with related spam that supported the Tibetan government in exile. The file names were lifted from actual press releases and news headlines, such as "Free Tibet Olympics Protest on Mount Everest.doc" and "CHINA'S OLYMPIC TORCH OUT OF TIBET 1.doc." The technique is familiar, dredging up memories of WORM_NUWAR and leveraging headline-grabbing events to facilitate propagation.

In the middle of the year and toward the end, .ZIP files were spammers' malicious attachments of choice, used to evade text-based spam filtering technologies. Examples included bogus UPS and FedEx email notifications containing a tracking number (to make the message appear authentic) with a message body informing recipients of a package delivery problem and a message urging the recipient to print the attached "invoice" to claim the "package." The attachment was the same file type as those seen in previous spam runs. The .ZIP file contained an information-stealer detected by Trend Micro as TSPY_ZBOT.MCS. ZBOT spyware—infamous keyloggers known to steal confidential information, such as those related to online banking credentials.

The increase in malicious attachments may be attributed to the ease they provide cybercriminals in altering tactics, such as attachments that leverage social engineering tactics and the ease with which payloads are delivered in the form of vulnerabilities that can be exploited. As shown in Figure 7, a huge spike in malicious attachments occurred in September and October 2008.

MALICIOUS ATTACHMENTS

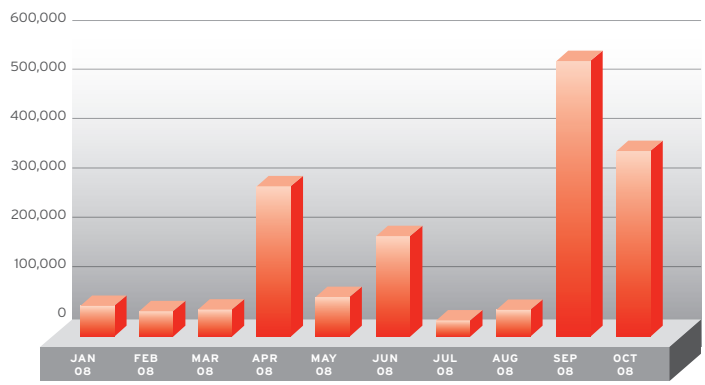


Figure 7: Spike in malicious attachments in 2008

Spam

Spam has consistently risen over the years and the U.S. continues to be the "most spammed" country, receiving 22.5 percent of all spam, while Europe is the most spammed continent. China's percentages have been increasing lately, showing 7.7 percent of spam volume in 2008, compared to Russia at 5.23 percent, then Brazil, the Republic of Korea, and others (see Figure 8).

	Country	Volume
1	United States	22.50%
2	China	7.74%
3	Russian Federation	5.23%
4	Unknown	5.09%
5	Brazil	5.05%
6	Republic of Korea	4.07%
7	Turkey	3.22%
8	Canada	2.71%
9	Argentina	2.52%
10	Colombia	2.41%

Figure 8: Top 10 in spam volume for 2008

Spam is predominantly written in English—at 93 percent of all spam tracked by TrendLabs. The next highest spam language is Russian at 3 percent and after that, several languages attribute 1 percent to spam, including Japanese, German, Chinese, and others (see Figure 9)

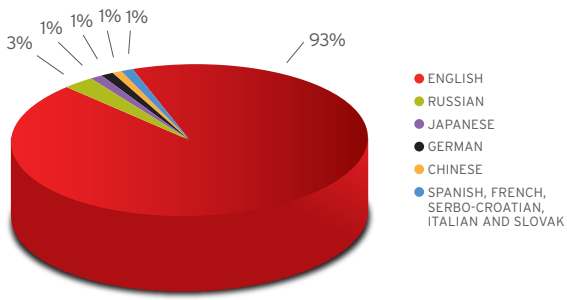


Figure 9 Spam language trends in 2008

Although still the spam leader in volume, English is slowly decreasing as a percentage of overall spam (see Figure 10.)

ANTI-SPAM

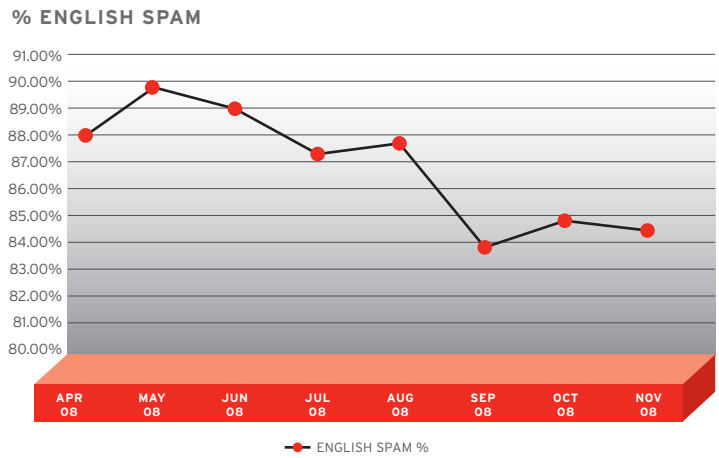


Figure 10: Percentage of English spam drops in 2008

Spam was in the news in April when "backscatter spam" reinvented itself. "Backscatter" is a term coined to refer to the intended effect of sending spam using forged sender addresses. Spammers who send email messages with different sender names in the *From* field are in fact counting on certain types of mail transfer agent (MTA) programs that return the entire text or message to the forged sender (as in *Message Sending Failure* messages or bounced email notifications) instead of truncating the messages. MTAs that are configured like this inadvertently cause a spam run, because they "send back" message to users who did not send these messages in the first place. Similar to malware attacks that reuse old exploits, this recycled technique is as effective today as when it first appeared, as long as the conditions that allow it persist.

Another spam trend is the increasing use of malicious URLs embedded in spam to snag victims. In Figure 13, 30.3 percent of domains named in spam were registered in the past 60 days—implying their shady nature—with 10.8 percent registered in the five days prior.

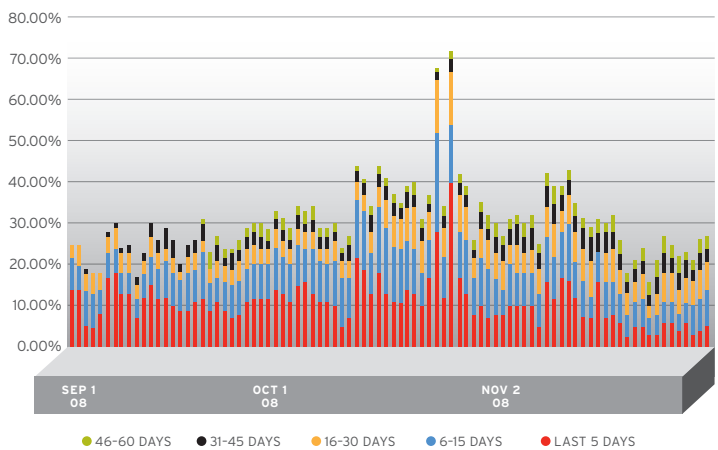


Figure 11: Percentage of spam domains registered in past five to 60 days

In November, a group of security researchers blew the whistle on San Jose-based McColo Corporation—one of the world's most disreputable hosting providers and one of the world's largest sources of spam. With suspected links to the Russian Business Network (RBN) in St. Petersburg, McColo was believed to have hosted some of the command and control (C&C) infrastructure for several of the world's largest identified botnets, including Srizbi, Rustock, Mega-D, and Cutwail. These botnets were controlling hundreds of thousands of zombie PCs involved in email spam, spamvertising, malware, child porn, credit card theft, fraud, and get-rich-quick scams.

As a "bulletproof" hosting provider, McColo was known to be unresponsive to complaints about its hosted sites, collecting a premium from criminal operators for turning a blind eye when notified of infractions.

McColo was finally disconnected from the Internet after years of investigation culminated in a complete shutdown, eliminating an unbelievable 50 to 75 percent of the world's junk email in a single day (see Figure 12). Unfortunately, the spam reprieve was temporary and spam counts are again inching back up. In particular, Srizbi—one of the largest known botnets with links to McColo—appears to be regaining strength. The McColo shutdown indicates that botnets have been and will continue to be the biggest spam producers. Continued vigilance within the security, law enforcement, and business communities will be critical in spam control in the years ahead.

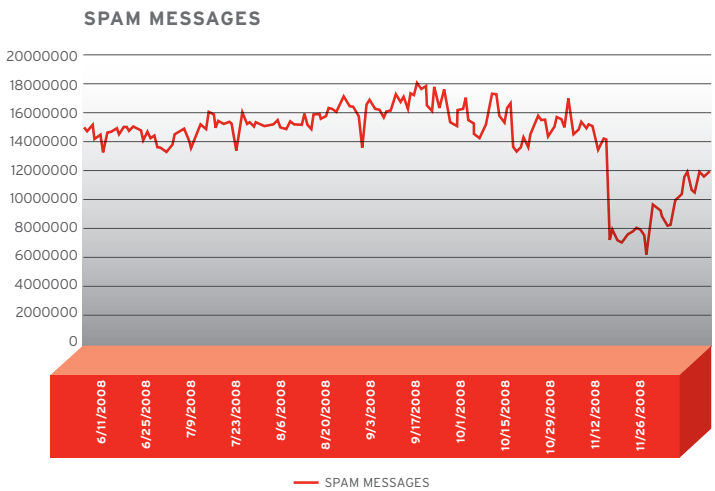


Figure 12: The McColo effect

Phishing

In 2008, phishers became even more adept at using social engineering techniques to fool victims into falling for phishing schemes. In addition to targeting financial institutions and banks, a new twist on phishing was discovered in November involving a fake *McDonald's Member Satisfaction Survey* that promised a $75 credit for completing the survey. After completion, users were asked for full name, email address, credit card number, and electronic signature (see Figure 13).

Bogus surveys related to Wal-Mart, American Airlines, and U.S. President-Elect Barack Obama were used in several phishing attacks this year to collect personal information from potential victims. The surveys usually promise some form of reward to participants, clearly demonstrating that cybercriminals are leveraging users' increasing need to save money this past year.

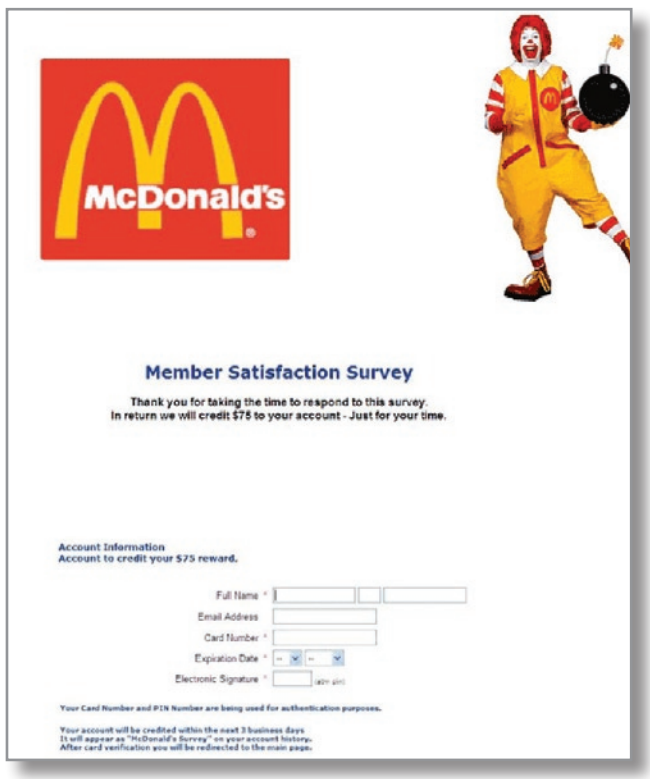


Figure 13: Phishing McDonald's customers

As one of the most popular online retailers, eBay has consistently topped the "most spoofed" list of web sites over the past few years. This past year, however, witnessed a different trend emerging as eBay and PayPal—the most popular spoofed companies in phishing attacks—slipped from 50 percent of all phished sites to 29 percent in March and down to only 4 percent in November (see Figure 14).

MARCH 2008	OCTOBER 2008	NOVEMBER 2008
eBay	Abbey National PLC	Google
PayPal	Wachovia	Abbey National PLC
Halifax Bank	Lloyds TSB	PayPal
Wachovia	Bank of America	Lloyds TSB
Citibank	PayPal	Wachovia
Bank of America	HSBC	eBay
Posteitaliane	eBay	Alliance & Leicester
HSBC	Ocean Bank	ANZ Bank
St. George Bank	Halifax Bank	Chase
NatWest	ANZ Bank	Posteitaliane

Figure 14: Most spoofed companies in phishing attacks in 2008

Although other sites are also prominent phishing targets, such as Wachovia, Halifax Bank, and Bank of America, the greatest area of growth is among lesser known sites, indicating that phishers are diversifying their efforts to avoid detection and increase their number of phishing nets (see Figure 15).

SEPTEMBER 2008	OCTOBER 2008	NOVEMBER 2008
Grow Financial FCU	AMP Banknet	Coventry Credit Union
Banca CR Firenze	Banco Galicia	Colorado Business Bank
Ice Save	Banco Ganadero	The Rock Building Society Limited
Royal Bank of Canada (USA)	Banco Mercantil	Orient Corporation (Orico)
Telstra Corporation	Bank 21	Federal Reserve Bank
MBNA Europe Bank	BANKINTER	Ministerio Publico Brazil
Savings & Loans	Bank of Scotland Halifax	Bank Americard
Wepco Federal Credit Union	Canada Revenue Agency	Slingshot Communications, Inc
Federal Choice Credit Union	City of Boston Credit Union	Telecom N.Z.
First National Bank of DeRidder, Louisiana	Coventery Credit Union	Community Driven Credit Union
City-County Federal Credit Union	Eastern Bank	San Bernardino School Employees Federal Credit Union
American Airlines	Fidelity Investments	Banca del Piemonte

Figure 15: Sample of new companies used in phishing attacks in 2008

In 2008, alternate phishing methods, such as spy-phishing, appeared. Traditional phishing involves sending out email messages that lead users to a fake web site that resembles the login pages of certain institutions or companies. Spy-phishing is a blended threat that combines both phishing and data-stealing malware to prolong attacks beyond the point of availability of a phishing web site. In this way, criminals can obtain sensitive user information without enticing users to log on to a fake page. They accomplish this by planting a spy in users' systems so any relevant user action can be transmitted to a remote server. Unprotected users thus stand to lose sensitive information.

Spear phishing, in which spam is personalized and targeted at a specific group of people or organizations, also occurred in 2008. Targeted phishing attacks on senior executives are called "whaling." An example of whale phishing occurred in May when phony subpoenas were sent to a targeted set of CEOs. Email messages were sent as notices of deficiency or tax petitions supposedly coming from the United States Tax Court. When victims clicked on the link in the message body, they were directed to the site *www.ustax-courts.com*—the purported US Tax Court site—and asked to download a higher version of Internet Explorer to further view court details. By string manipulation (in this case, adding a dash to the actual domain name of the actual site), unknowing users were convinced into thinking that the bogus site was legitimate, increasing the chance they would click on the link and be vulnerable to the phishing attack. The legitimate for the U.S. Tax Court site is actually *www.ustaxcourt.gov*.

In April, the Rock Phish gang (best known for their easy-to-use kits that yield professional looking phishing pages) introduced information-stealing malware dubbed as the Zeus Trojan. In this attack, users were prompted to install a "digital certificate" in order to access the bank's online login page. Unfortunately, the accessibility and abundance of phishing kits are making the setup and maintenance of phishing operations increasingly elementary.

ANTI-PHISHING

Web Threats

Mass Compromises

As the Internet Gold Rush subsides and almost every business and individual in the world seemingly boasts a website or personal web page, many of these older sites are falling prey to attack as they were built with tools and software code that have grown outdated.

Small businesses and individuals are particularly at risk, lacking the proper IT resources and funding to properly maintain, patch, and upgrade these sites. Cybercriminals find weaknesses to exploit—often using automated tools that crawl the Internet looking for poorly configured pages and sites.

Exploits occur in the form of SQL injection, a technique that exploits a security vulnerability occurring in the database layer of an application. Web sites are also falling prey to cross-site scripting (XSS) attacks, in which a web application vulnerability allows malicious code injection onto web pages. Vulnerabilities of this kind have been exploited to create nasty phishing attacks and browser exploits. Unfortunately, when users visit these sites they become infected.

Massive attacks targeting specific user groups and popular web sites grew more common in 2008. A diverse range of web sites—entertainment, political, online shopping, social networking—were used to spread malware. Compromises were at their height in May when web sites from around the world were injected with malicious code that infected unknowing Internet users. This trend, unfortunately, seems to be continuing at an extremely rapid pace.

In 2008, a perfect storm of outdated, vulnerable web sites and extremely clever criminals opened the door to mass web site compromises on a scale never seen before. Dubbed "Mass Compromise May" at Trend Micro, the month of May saw a rash of large-scale attacks.

Also in May, approximately 9,000 web sites were compromised via SQL injection with embedded malicious JavaScript redirecting users to two major malicious URLs. Among these web sites were legitimate medical, educational, government, and entertainment sites from around the world, including. A survey of the site locations included India, UK, Canada, France, and China, suggesting the attack was the work of an automated Chinese hack tool programmed to search through web sites for vulnerabilities.

A few days later, a malicious script was injected into half a million web sites. This event involved a ZLOB Trojan that changes an affected system's local DNS and Internet browser settings. Also on the same date, Chinese-language web sites were targeted in an attack meant specifically against China, Taiwan, Singapore, and Hong Kong. Google search results at the time of the attack showed 327,000 pages containing the malicious script tag.

Another string of web site compromises was discovered the following week, involving at least four web sites of various affiliations and different countries. These were injected with malicious JavaScript that redirected to two sites. Both eventually led to their own series of redirections and finally the download and execution of a backdoor and a Trojan.

Two days later, hundreds of thousands of web sites were again found compromised and inserted with malicious JavaScript, some of which were sites from the Asia-Pacific region. Hackers had apparently conducted another massive SQL injection attack. A Google search for the malicious URL turned up 197,000 results.

The next day—May 22nd—several web sites in Japan (including a popular music download site and a music company site) were found injected with malicious code. The massive scale of these attacks indicates a trend toward automated, large-scale compromises. Trend Micro researchers believe mass compromises are actually quite common but are usually found quickly and handled or they remain unnoticed and consequently unreported.

In retrospect, the documented compromises in May appear to have been part of a single, large-scale attack that involved different domains. However, it is also possible that different groups used the same tool, or that a large, organized, cyber crime group outsourced the job to small-time hackers. Although May saw the most activity for mass compromises, the trend, unfortunately, seems to be continuing.

Zero-day Bug in Internet Explorer

Malware criminals were quick to pounce on the recently identified Internet Explorer (IE) zero-day exploit to mount massive SQL injection attacks on some 6,000 web sites. Hackers wait for vulnerability information to be revealed on Patch Tuesday, immediately after Microsoft releases its latest round of patches for the month, providing attackers with a full 30 days to use the exploit before Microsoft can issue a fix.

Researchers correctly warned it was only a matter of time before the publicly available exploit was used for a wider scope of attack. Microsoft confirmed the bug's presence within all its browsers, including those currently supported (IE5.01, IE6 and IE7, and IE8 Beta 2). The browser bug—a flaw in the data-binding function of IE—was prominently featured in several massive cybercriminal threats in 2008, including an information-stealing operation targeting Chinese gamers.

As of December, Trend Micro researchers estimated the number of infected sites to be at 6,000 and quickly increasing in number. The final payload is a worm detected by Trend Micro as WORM_AUTORUN.BSE. Other exploits that also lead to the worm include HTML_IFRAME.ZM, JS_DLOADER.QGV, and HTML_AGENT.CPZZ.

Obfuscated JavaScript in HTML web pages are also detected as JS_DLOAD.MD—the same malicious script found to exploit the zero-day vulnerability in Internet Explorer 7 (IE7).

The identified scripts trigger a series of redirections to multiple URLs that finally connect to one of several malicious domains. Simply visiting the site was enough to completely compromise a victim's machine. Experts estimate that up to 75 percent of the world's Internet users could be completely comprised with no interactions on their part, due to the prevalence of Internet Explorer and the vulnerabilities' impact on all versions of Internet Explorer, not just version 7.0, as was originally believed. The severity of the problem required Microsoft to post an out-of-band security patch.

Browser exploits became a favorite of cybercriminals in 2008 and Internet Explorer was only one of the browser applications targeted. Additional attacks were launched against Mozilla Firefox, Opera, Google Chrome, and Safari.

Game Password Stealers

Posing a larger problem in Asia than the U.S., the game password theft continued into 2008 from 2007. Malware writers continue to design web threats that steal login credentials to some of the most popular online gaming sites such as World of Warcraft, Gamania, and Lineage. Virtual items in the games are sold in the real world for real cash, providing a powerful lure for criminals to hack into users' accounts, steal virtual items, and then sell them on the Black Market. China is an especially active market for these items.

In January, Trend Micro reported on a phishing scheme targeting gamers in World of Warcraft and Tibia. Cybercriminals devised spam that requested users to click a link where they were redirected to a page requesting an account name and password. The phishers made no attempt to hide the actual phishing URL *hxxp://jungkyukimphoto.com/bgm/.../*, even displaying it on the address bar.

Rogue Antivirus

"Rogue antivirus" software convinces users they are infected with malware by spoofing infection symptoms then lures them into downloading fake antivirus programs to clean the supposed infection. These threats leveraged a variety of arrival and infection channels in 2008—from spam to mass search engine optimization (SEO) poisoning—compromising many web sites in the process.

Figure 16: Rogue antivirus interface

Several independent malware families became visible this year posing as fake antivirus or antispyware vendors. These scams entice users to a website offering a free online antivirus scan. If users agree to run the supposed scan, the rogue software invariably detects a problem, prompting the download of fake antivirus software or other malware, which is actually a clever front for nasty malware. These threats use a variety of arrival and infection channels—from spam to search engine poisoning—and usually involve several, compromised web sites.

In December, Trend Micro reported on a version of this scam called *Virus Remover 2008* (see Figure 16). First spotted in the wild in early July, the threat arrived just ten days after its predecessor, *Antivirus 2009*, was spotted. *Antivirus 2009* and *Virus Remover 2008* are fairly similar in routines, except that *Virus Remover 2008*, unlike its predecessor, arrived with a licensing agreement that mentions what it can and will do to systems once installed. System slowdown and several program terminations due to incompatibilities are a few effects users may encounter. *Virus Remover 2008* featured pages built for specific languages and countries implying that criminals are attempting to widen their scope by targeting clients from specific regions and geographies.

Search Engine Poisoning

Poisoned search results tricked a number of unsuspecting users in 2008. The technique plays on the popularity of search engines and manipulates search results based on users' trust in these search tools. Early in the year, malware writers were quick to use the death of actor Heath Ledger in a search engine poisoning scheme. Users who Googled Ledger's name were led to a poisoned web page, then redirected to a malicious web site. Super Bowl fans were also victims of search engine poisoning in 2008.

WEB FILTERING

In August, a mass search engine poisoning campaign involved several compromised web sites to push rogue antispyware. The final agenda for most rogue antispyware scams is extortion. Users who fall for this scam pay a certain amount of money to malware writers to purchase the full version of fake antispyware.

According to Trend Micro researchers, search engine poisoning currently compromises several dozen domains. The hackers upload PHP scripts that contain various text strings designed for search engine poisoning, manipulating the natural page rankings of search results in order to get more hits than a page truly deserves.

In November, Trend Micro's HouseCall virus scanner was served up as poisoned results. When users searched on "free online virus scan by Trend Micro" in Google, they were sent to a fake page that pointed to a file detected by Trend Micro as ADW_FAKEAV. This software tries to dupe victims into believing their systems are infected with bogus malware then prompts them to pay for a full license of a fake antivirus application in order to remove the fake threat. ADW_FAKEAV also connects to a remote web site that downloads another adware program detected as ADW_FAKEAV.O, exposing victims to additional adware threats.

Cybersquatting

Cybersquatting refers to a technique to exploit users' perceptions of web sites' legitimacy, usually aiming to fool them into believing that fake or malicious sites are real. For example, scammers used cybersquatting in 2008 to extort money from unknowing users after Hurricane Gustav in September. Similar to parked sites last year, domain names that appeared related to Gustav relief efforts were registered immediately after the disaster. The list of newly registered sites had the words Gustav with aid, relief, or recovery attached. Suspicions were validated when several domains were discovered that tricked users into giving away money for supposed aid.

Typosquatting is the most popular form, relying on users' errors when typing URLs in browsers' address bars. Figure 17 provides an example of several fake addresses that lead to a completely different site when users type the wrong search term.

WEBSITE	REAL LINK	FAKE URL
Google	google.com	goglez.com
		googler.com
ImageShack	imageshack.us	imageshack.org
Windows Update	update.microsoft.com	windowsupdate.com
Facebook	facebook.com	facebook.com

Figure 17: Typos can lead to malicious sites

Google's fame made it a prime target for this attack in 2008. From the millions of users who access the site, chances are that users will eventually make spelling errors and the resulting fake pages are where the threats occur.

According to TrendLabs data, global distribution of malicious URLs is heavily weighted toward the U.S., with Canada in second place, China in third and additional countries reporting far less (see Figure 18).

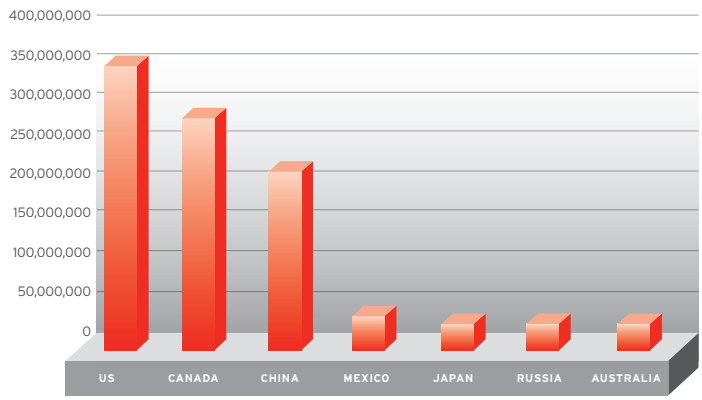


Figure 18: Global distribution of malicious URLs for 2008

WEB REPUTATION

DNS Changers

DNS changing malware, detected by Trend Micro as TROJ_AGENT.NDT and BKDR_AGENT.CAHZ, poisoned other hosts on the local subnet by installing a rogue Dynamic Host Configuration Protocol (DHCP) server on the network. These malware monitor traffic and intercept request packets from other network computers. They reply to intercepted requests with packets containing pointers to malicious DNS servers causing recipients to be redirected to malicious sites without their consent.

Automated Exploits

A .DLL worm, WORM_DOWNAD.A, which exploits the MS08-067 vulnerability, exhibited routines that led security analysts to postulate its role in the development of a new botnet. The automation occurs as a default Windows operating system setting and includes the automatic start that occurs when Autorun.inf. is initially dropped. The system's own vulnerability also generates an automated event, which allows the worm to spread via memory and network. The threat has been discovered to have already infected more than 500,000 unique hosts, spread across different countries.

Autorun Malware

Although they use techniques from an older generation of viruses, autorun malware (worms and Trojans) are alive and kicking, relying on users who exchange information through infected USB drives. Autorun malware propagate using the autorun feature of removable devices. Windows "auto-executes" certain programs when CD/DVD units and USB drives are inserted. This malware uses the Windows auto-execute feature to infect a computer as soon as a USB drive or CD is inserted. When a user is infected through the web, the infection eventually spreads to other networked PCs (in the office, at home, etc.) as users exchange files between PCs via USB devices. Interestingly, most Asian countries list autorun malware as their top infectors—the highest concentration compared to other regions. The top malware infecting PCs in Europe, Middle East, and Africa (EMEA) also include several autorun malware.

Removable and physical drives are the fourth highest source of infection globally. Of the total infections in Asia and Australia, 15 percent originate from malware borne by removable drives. Most Asian countries feature autorun malware as their top infector and the top malware infecting PCs in Europe, Middle East and Africa (EMEA) also include several autorun malware. Autorun malware are so successful in propagation that they have infiltrated networks at NASA and the U.S. Department of Defense.

Ransomware

Spotted in November, a new version of the GPcode ransomware, which Trend Micro detects as TROJ_RANDSOM.A, searches and encrypts files found on any readable and writable system drive, rendering it inaccessible without the encryption key. Victims are informed that a decrypting tool must be purchased to unlock the files. This is accomplished by dropping a text file in each folder containing an encrypted file.

USB Sticks Bearing Threats

News of pre-shipped malware on USB sticks reinforces the increasing threat these devices represent. The most recent product reportedly carrying worms was Hewlett-Packard's Proliant USB keys, which are used to install optional floppy-disc drives into server devices. The malware bear file names that could be mistaken for legitimate system files (such as WinUpdter and ctfmon) and can be transmitted onto a system once the keys are plugged in. In November, the U.S. Army reportedly suspended the use of USB and removable media devices after a worm began spreading across its network.

MBR Rootkit

As one of the most technologically advanced web threats of the year, the MBR (Master Boot Record) rootkit threat has been recycled yet again. After successful infiltration using popular web threat exploits, malicious code is downloaded and executed, and the rootkit is installed via the MBR. The Trojan, detected by Trend Micro as TROJ_SINOWAL.AD, ensures that only one instance of itself is running on the affected system, and then looks for the bootable portion of the affected system. Once found, this Trojan creates a new malicious MBR that loads the rootkit component of this Trojan. The rootkit component, detected as RTKT_AGENT.CAV, is then saved in an arbitrary sector within the bootable partition. After performing its malicious routines, the Trojan restarts the affected system. The new version allows a Trojan to load before the operating system even starts. This level of camouflage indicates high levels of programming expertise, raising the bar of all antivirus software due to the difficulties in cleaning these rootkits.

Windows Server Service

As the first "old style" worm identified in some time, the Windows Server Service vulnerability appeared at the end of November. A worm detected by Trend Micro as WORM_DOWNAD.A leveraged the MS08-067 vulnerability to propagate via networks. Trend Micro researchers also noticed high traffic on an affected system's port 445 upon successful exploitation, after which the worm connected to a certain IP address to download a copy of itself. Like the worms of old, the vulnerability was observed to spread from machine to machine through the

Windows Server Service, which is responsible for file and printer sharing. Reminiscent of worms popular in 2003 and 2004, the vulnerability affects almost all Windows operating systems since 2000, including Vista.

Several days after identifying the worm, Trend Micro researchers speculated the worm might be a key component in the development of a new botnet. Initially thought to be working in conjunction with a networm variant, WORM_DOWNAD.A is now believed to be an updated version of an attack from the same criminal botnet gang. The threat seems to have since spread wider, extending its reach around the globe. As of the end of November, more than 500,000 unique hosts had been discovered to have fallen victim to this threat. Infected hosts were spread across different countries and were found in service provider networks in the U.S., China, India, the Middle East, Europe, and Latin America. Several residential broadband providers also appear to have a large number of infected customers.

Data-stealing Malware

Data-stealing malware experienced tremendous growth in 2008. Initiated by a Trojan attack, the primary goal of data-stealing malware is to capture sensitive data from users' PCs then send it back to a bot herder or other criminal operators either for direct exploitation or for resale on the digital Black Market.

For example, Microsoft's zero-day vulnerability provided ample opportunity for cybercriminals to compromise PCs. In December, several web sites were found rigged with a malicious JavaScript detected by Trend Micro as JS_DLOAD.MD, which exploits the Internet Explorer zero-day vulnerability. After a successful exploit, it triggers a series of redirections to multiple URLs then finally connects to one of several different domains. Trend Micro detected the downloaded files as *TSPY_ONLINEG.EJH, TSPY_ONLINEG.EJG, TSPY_ONLINEG.HAV*, and *TSPY_ONLINEG.ADR*.

The toolkit related to this exploit was reportedly being sold in the China underground community. This is logical, since TSPY_ONLINEG variants are notorious data-stealers—particularly credentials related to online games, which are popular in China.

These threats bore a strong resemblance to other data-stealing malware attacks that occurred in May when several thousand web sites were compromised via SQL injection and Trend Micro researchers were alerted to malicious URLs that supposedly exploited a certain Chinese gaming application.

Endpoint Security Risks

The easy availability and wide usage of USB-capable devices is wreaking havoc on the information security landscape. The proliferation and large variety of devices—USB flash drives, digital cameras, digital frames, mobile phones, PDAs, laptops, recordable CD/DVDs, iPods, flash drives—makes it increasingly difficult to secure the endpoint.

An Amazon.com report in December informed consumers regarding the discovery of a Sality worm on the product installer disc of a digital frame (Samsung Frame Manager XP version 1.08). The infected installer disc is needed to use a specific Samsung digital photo frames as a USB monitor.

HP Australia warned the public in April about an undisclosed number of 256 MB and 1 GB USB flash drives shipped with some of its Proliant servers that arrive infected with malware that can be transmitted onto the system once the flash drives are plugged in. The USB flash drives are intended for those who want to install optional floppy-disc drives into their server devices. The malware file names can be mistaken for legitimate system files (such as WinUpdter and ctfmon) and were detected by Trend Micro as WORM_AUTORUN.AZB and WORM_VB.BDN. Although HP reassured users this was a low-level threat given the nature of the USB flash drive's purpose, the incident highlighted the growing use of USB devices as malware carriers.

In January, three digital photo frames, were discovered to contain a malware that installed malicious code. All three cases involved the same product and chain of stores, suggesting the infection occurred either during shipping or at the factory. This hitchhiker malware, detected by Trend Micro as WORM_AGENT.TBH, dropped malicious files on affected systems as well as an AUTORUN.INF file to execute the dropped files.

Mobile Malware

Mobile phones play a critical role in our lives today, making them a favorable target for malware authors. Because mobile phones contain confidential, personal information, it is not surprising to see mobile malware enter the threat landscape.

Mobile worms and viruses are similar to those that infect PCs. An unsuspecting user can be tricked into installing a harmless looking file that infects a device and seeks additional mobile phones to target, often disrupting the phone's operations. One of the oldest mobile threats, the Cabir or Caribe worm, was first identified on the Symbian OS in 2004. Symbian is still targeted most by mobile malware writers because it enjoys the majority of worldwide market share.

More recently Trend Micro researchers detected malware targeting the Windows Mobile PocketPC. Detected as WINCE_INFOJACK.A, the worm runs on a Windows CE environment and steals information like the serial number, OS version, model, platform, and host's name then relays it to the malware author. WINCE_INFOJACK.A also changes security settings on the affected phone. The worm originates from an infected memory card on a mobile device or through SMS.

	Infection Count
Symbian OS	17,246
PALM	217
EPOC	7
WINCE	72

Figure 19: Most attacked mobile operating systems for 2008

In 2008, the most widely attacked mobile operating system was again SYMBOS, followed by Palm (see Figure 19). Figure 23 shows the top ten mobile malware identified by Trend Labs in 2008. The top, three mobile malware detected are variants of ComWAR—the first worm for mobiles phones—which propagates via MMS and infects telephones running under the Symbian Series 60.

Detection Name	Infection Count
SymbOS_ComWAR.A	9474
SYMBOS_Comwar.C	3873
SymbOS_ComWAR.B	868
SYMBOS_BESELO.A	790
SymbOS_Skulls.I	421
SYMBOS_DISABLE.A	355
PALM_FATAL.A	211
SYMBOS_CABIR.A	196
SYMBOS_CARDTRP.U	154
SYMBOS_CMWAR.GEN	123

Figure 20: Top ten mobile malware in 2008

Botnets

Botnets played a big part in spreading web threats in 2008. Giants like Storm, Kraken, Mega-D/Odzok, MayDay, and ASProx—all created ripples last year, remaining consistently on the radar of botnet researchers. The shutdown of McColo, a major cyber crime hoster in November, only temporarily deterred bot masters from looking for alternative means to proliferate.

From January until November 2008, a staggering 34.3 million PCs were infected with malware under families that are commonly associated with bots. As shown in Figure 20, bot infections were highest in August at 7.5 million and lowest in November at 1.4 million. The biggest three-month increase occurred from June to August when there was a 476 percent spike in infections. Before and during these months there were reports of malicious activity from emerging botnets (Mega-D) and old botnets making a comeback (Kraken), possibly dethroning Storm. Used in a variety of criminal activities, the Storm botnet has been linked to the Storm Worm, a Trojan horse spread through email spam. The combined efforts of these bots to repopulate their respective armies contributed to this increase.

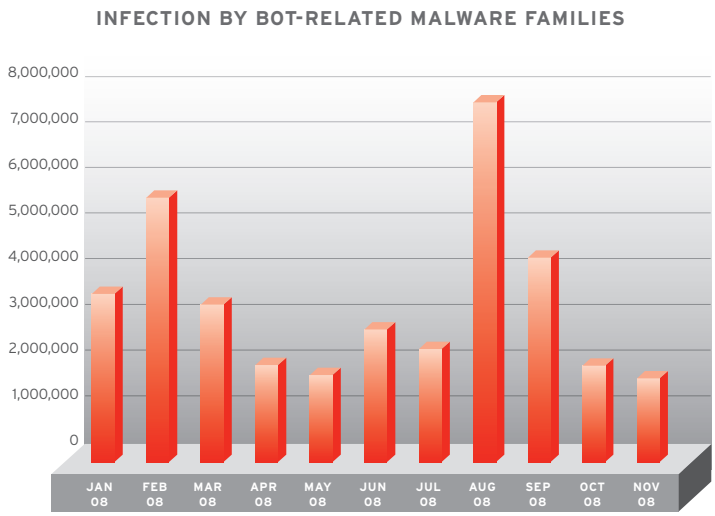


Figure 21: Botnet infections in 2008

Storm continued its path of destruction in 2008 counting even more infections than the year before. Although it is difficult to provide exact figures for the breadth of Storm's coverage, experts believe the number of infected PCs at the time to be hundreds of thousands—others believe that number to be closer to one million. Experts believe that Storm strategically split itself into pieces in 2008 for the purpose of sub-letting server space to better hide its activities.

Distributed via the web and through spam email, Storm typically works by convincing users to visit malicious sites. The Storm gang is particularly adept at using social engineering techniques to lure users to click on malicious links. The past year saw monthly examples of Storm malware writers coordinating spam around current events, holidays, news of terrorism, social networking sites, economic issues, and fake videos of popular celebrities. By using constantly changing techniques, Storm operators succeed at evading spam and URL filtering blocking.

In June, Storm malware authors resurrected a trick used on Valentine's Day, again hewing to themes of love and romance. Email subject lines read "Stand by my side," "I want to be with you," and "Lucky to have you" to hook unsuspecting users (see Figure 22).

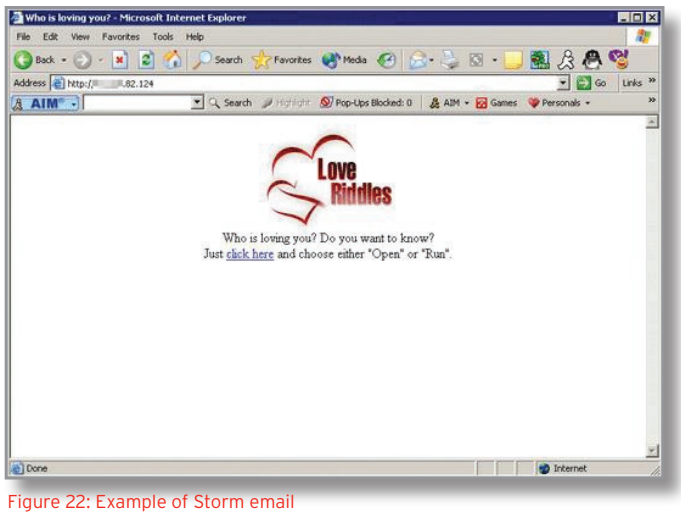


Figure 22: Example of Storm email

When the curious clicked on these links, they were redirected to a site hosting LOVEYOU.EXE, which Trend Micro detected as the Nuwar worm. Before June, reports of Storm activities included downloading info-stealers in February, advertising Canadian pharmaceutical products in January, and phishing information from Royal Bank of Scotland customers, also in January.

Storm started the year off with a New Year's emailer asking recipients to click on a link to retrieve a supposed greeting. Clicking the link led to the bogus site "*newyearwithlove.com*," built on a network that experts call "fast flux." These networks alternate the load between members, rendering them more difficult to take down without disabling the domain name. Storm operators were clever enough to choose a day the site registrar was closed for the holidays, biding the criminals more time to build a larger botnet, capable of immense attacks.

Perhaps the scariest aspect of Storm is that some experts believe the botnet may have been a large-scale test for creating an even bigger botnet, which may explain why it has now lost traction and also why new botnet giants have reared their ugly heads such as Kraken, Mega-D/Odzok, Mayday, and ASProx. The November shutdown of McColo, a notorious cyber crime hosting provider, only temporarily deterred bot masters from looking for alternative ways to proliferate.

Highly Blended, Combination Attacks

As web threats have grown increasingly sophisticated, attacks targeting a single vector are few and far between. Web threat activity continues to encompass blended, multi pronged attacks—a virtual cocktail of the best malware techniques that hit users on several fronts to increase the probability of a successful infection. Although web threats occur throughout the world, the majority continue to originate in the U.S. According to data from TrendLabs, 69 percent of domains blocked by Trend Micro security systems are in the U.S. with 24 percent blocked in China, three percent blocked from Canada, and three percent from the Netherland.

Blended attacks are launched in a variety of ways. A user may open a (spam) email and follow a malicious link or encounter malware through a compromised web page. Regardless of the delivery mechanism the next step almost always involves a Trojan, which is used to compromise the PC and allow a criminal to control its operations. The Trojan can then download additional software—usually malware—to conduct its business. The intention may be to steal login credentials or passwords or to monitor credit card transactions or online banking sessions or the PC may be assimilated into a botnet for the purpose of delivering spam or participating in distributed denial of service (DDoS) attacks.

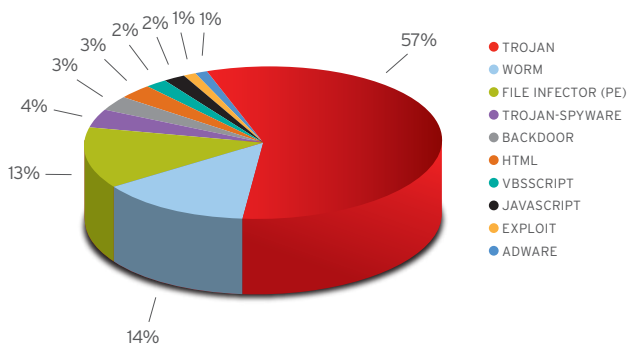


Figure 23: Percentage of all infections in 2008

Once downloaded, malware continues its trail of destruction—changing the DNS settings of other computers on the network to malicious DNS servers, an example of a popular technique used frequently in 2008. Or the malware might, in fact, be a worm that hops from computer to computer on the network.

According to TrendLabs, 57 percent of all infections in 2008 were Trojans with worms making up 14 percent and file infectors at 13 percent. The remaining 16 percent of infections tracked by Trend Labs are characterized by Trojan-spyware, backdoor attacks and others (see Figure 23).

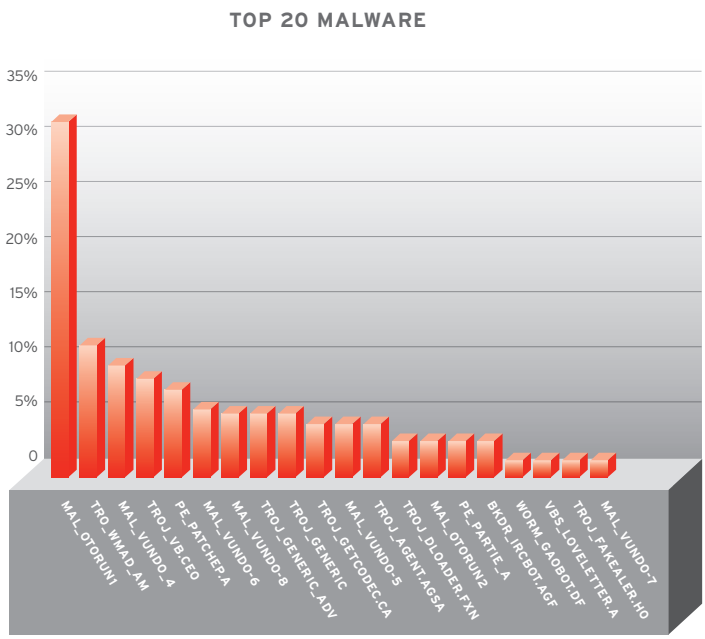


Figure 24: Top 20 malware by name in 2008

As in years past, the U.S. continues to report the most infections by far. Next ranks Japan, then Taiwan, then China. Figure 25 shows the number of infections per country in ranked order.

Top Most Infected Countries		
1	United States	373,689,902
2	Japan	96,787,968
3	Taiwan	73,517,376
4	China	30,256,433
5	Australia	17,692,567
6	Spain	8,621,550
7	France	8,346,656
8	Germany	4,557,972
9	Canada	3,598,830
10	Turkey	3,361,939

Figure 25: Most infected countries in 2008

Application Vulnerabilities

Application vulnerabilities continue to harbor malware infections. The increase in targeted attacks using malicious attachments—with most of the attachments identified as malicious Microsoft Office files—making the application suite one of the infection vectors of choice for cybercriminals. Microsoft Office exploits allow threats to drop embedded code, which delivers damaging payloads via backdoor routines and information theft—for example.

Adobe Reader vulnerabilities, meanwhile, were also served up different ways in 2008, which may explain their effectiveness. Exploits were placed in banner ads, as a downloaded payload from spam claiming to come from the Federal Reserve Bank.

Another attack triggered fake "bluescreens" and compromised system security. An exploit for Adobe Flash vulnerability was used to download malicious SWF files in a mass compromise (see Figure 26).

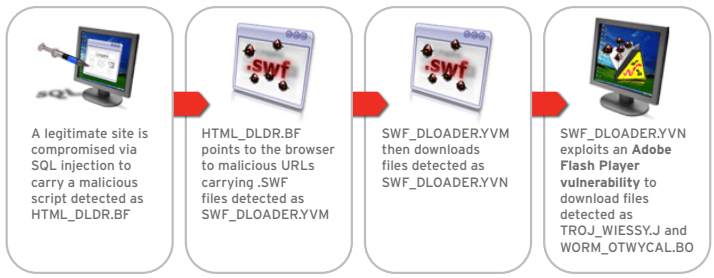


Figure 26: Adobe Flash vulnerability

ANTI-VIRUS

Looking Forward

Predictions for 2009

Amazingly, one in ten web sites is believed to be infected with malware, spyware, or some other content security threat.[15] In addition to the increase in sheer numbers of malware, advancements in malware technologies are a sure bet as malware authors continue to develop and release code that aims to avoid detection and consequent removal. Thus, users will see more malware families but fewer variants, making it more and more difficult for security companies to create heuristic patterns to detect them. The bigger problem is the sheer size and frequency of updating these pattern files—actually a greater problem than the malware itself.

The pattern file dilemma is not unique to any one vendor; rather, it is an industry-wide problem shared by all. To counteract this problem, Trend Micro is moving more detection technologies into the cloud. An example includes Trend Micro's Smart Protection Network—a cloud-client content security infrastructure that blocks the latest threats before they reach a user's PC or a company's network. By checking URLs, emails, and files against threat databases in the cloud, customers have access to continuous updates wherever they connect—from home, within the company network, or on the go.

Additional predictions about new and existing threats are discussed in greater detail below.

Sophisticated blended threats are the new frontier.
Web threats will continue to involve multiple vectors, blending attacks to avoid detection. These threats will also grow increasingly sophisticated—employing the latest tricks and techniques in the coming year, such as DNS Changer, as malware writers continue to leverage the best tools available. Taking a page from Storm's book, criminals will create new threat models and architectures in their continuous effort to make a profit. Expect botnets and attacks similar to the likes of *FAKEAV* and *MEBROOT* to flourish in 2009. Threat models will try to join the "in-the-cloud" bandwagon and set their eyes to software and services that offer such features (e.g., Microsoft Azure).

Social networking sites will grow as targets.
Social networking sites like Facebook, My Space, and Bebo will become prime targets for malware authors. In 2008, Trend Micro identified several threats targeting Facebook users such as spam, worms, and phishing. As social networking sites steadily increase in visitor traffic, the number of malicious activities will continue to proliferate. Therefore, users of these community sites should continue to be wary of messages received, even if supposedly sent from friends.

For example, a new hacking tool circulating on the Internet allows malicious users to create fake *YouTube* pages designed to deliver malware. The tool, detected by Trend Micro as HKTL_FAKEYOUT in October features a Spanish-language, user-friendly console that a hacker could use to create a pair of web pages that look eerily identical to legitimate *YouTube* pages (see Figure 27).

Figure 27: Tool used to create fake *YouTube* pages

With some crafty social engineering, unsuspecting users may visit the first of the fake pages, where they discover they cannot view their video and are told to download an updated version of Adobe Flash Player or another plugin or codec. A link is handily provided, and clicking the link leads users to the hacker's file of choice—usually something malicious. A second fake page informs users that the video they were trying to view cannot be shown, making users think nothing has occurred when, in fact, downloading the supposed plugin imported malware.

Ransomware and ransom attacks will occur in Q3 and Q4.
A rise in ransomware will occur in the second half of the year, targeting small to medium-sized companies rather than individual home users. Small to medium-sized companies are large enough to have money worth extorting, but small enough that they cannot cope with threats of an IT disaster or large amounts of downtime. These attacks materialize as distributed

denial of service (DDoS) attacks, which can literally shut down an e-commerce site, or as encrypted company files. As organizations tighten their belts during the current financial crisis, ransomware attacks could cause fragile companies to succumb to criminals who request massive pay-offs to avoid devastating consequences.

Mac attacks will increase.
As iPhones and iPods continue to proliferate and Mac computers grow increasingly popular and enjoy increased market share, the Mac world offers the next frontier for cybercriminals. An increase in attacks targeting Apple computers will likely occur in the second half of the year. And the icing on the cake for malware writers is that the majority of Macs do not arrive with antivirus applications installed by default, like most Windows PCs. Recently, Apple suggested that Mac users install antivirus programs on their systems, creating buzz in the online community and surprising those who noted Apple's past advertising about safety from malicious software. Some users dismissed the announcement as Apple's admission that Mac is also susceptible to malware attacks. Rumors spread further after the antivirus suggestion post was deleted from the Apple web site.

Ironically, had they not retracted their previous statement, Apple's concern for users' security would have been perfectly timed with a recently reported web threat targeting Mac users. The malware, detected as OSX_JAHLAV.A, is reported to come from spammed messages and poses as an application to distribute itself. Links on the spammed message lead to a site that supposedly contained an enticing video. Instead of downloading a codec to view the video, users receive malware instead. In November, Trend Micro reported another new threat affecting the Mac OS. Detected as OSX_LAMZEV.A, it reportedly allowed hackers to take control of an infected system.

Conventional spyware is dying while malicious spyware is thriving.
Spyware and adware have shown a steady decline in recent years. According to Trend Micro research, 2008 showed a sharp regression in adware infections—a 500 percent decrease since 2007. A similar trend was observed in spyware with a 400 percent regression in PCs affected by non-malicious spyware. During this time, however, malicious adware and spyware have seemingly taken the place of previous innocuous applications, proving that spyware and adware have not disappeared but have instead morphed. 2008 showed a 600 percent increase in Trojan spyware, which usually arrived as part of a blended threat. Inserting Trojan spyware is often the intention of a blended threat in an attempt to gather information from compromised computers, such as login details, account information, and valuable passwords.

Mobile data is ripe for the picking.
Experts at Trend Micro theorize that although mobile threats are not yet considered widespread, the potential for growth is huge. PC-based threats are already appearing on smartphones and cybercriminals typically are attracted to a large target population, such as the increasing iPhone user base. Cracked iPhones are already experiencing trouble in their inability to receive updates from Apple, making them more susceptible to malware attacks.

The growth of smartphones and faster data speeds will also increase the possibility of infection. In all probability, today's most stubborn malware will reappear on tomorrow's popular smartphones. Mobile malware will likely to continue to be a problem outside the U.S. in the short term because it is more affordable to send text messages in other parts of the world. (Outside the U.S. only the sender pays for text or media messages, the receiver is not charged.) However, as criminals devise ways to make money out of exploiting mobile technologies, they will grow increasingly vulnerable, especially as mobile phones and other handheld devices become more interconnected with their desktop counterparts. Expect more threats to "cross over" to multiple machines and devices via common application platforms such as .NET and Java.

Increased collaboration will occur within the security community.
Not all news is grim. Collaborative efforts to dismantle cyber gangs are becoming increasingly well planned, coordinated, and targeted. As people become more fed up with the audacity of cybercriminals and pockets of identified criminal activity, community sourced efforts will expose more Bad Actors, such as the takedown of Atrivo/Intercage and McColo in 2008. Good news!

Web 2.Uh-Oh is (unfortunately) here to stay.
The glories (and dangers) of Web 2.0 features, technologies, and culture will continue to haunt users in 2009. Hackers will continue using techniques that resemble normal code, like IFRAMES, and will also leverage Internet browsers and other web-enabled applications (such as Flash and streaming media players, among others) as infection vectors of choice. The release of Google Chrome, the upcoming official release of Internet Explorer 8, and the rise of browser-as-a-platform applications (e.g., Microsoft Silverlight and Adobe Integrated Runtime) will serve as new avenues for exploitation.

Alternative operating systems will be hit this year.
Every good thing must come to an end, including the supposed safety of "alternative" platforms. Threats exploiting bugs on alternative operating systems will grow, especially with the increasing popularity of Mac and Linux (the latter because of the booming Netbook market).

Microsoft—the eternal target—will continue its legacy of trouble in 2009.
Malware authors just love to pick on Microsoft and 2009 promises more of the same. Look for malware activity around the release of Windows 7 as cybercriminals will undoubtedly test any claims that the new Windows is "virus-free." Proof-of-concept malware will also exploit Microsoft Surface, Silverlight, and Azure. Also, cybercriminals will continue to employ a more professional approach to leverage the exploit window of opportunity of Microsoft's monthly "Patch Tuesday" schedule, in which zero-day exploits continue to trouble Microsoft users.

As soon as Windows 64-bit operating systems will become more popular we can expect 32-bit malware that may stay undetected by 64-bit virus scanners. This would happen due to the design of the 32-bit legacy emulation on Windows 64-bit operating system. Windows 7 is expected to have the same design for 32-bit application emulation.

Social engineering will grow increasingly prevalent and cleverer.
Cybercriminals will continue to leverage events, celebrities, and political figures as social engineering bait. U.S. elections-related malware will continue after the president-elect steps into the Oval Office in January, while gamers anticipating upcoming releases of *Starcraft 2* and *WoW: Wrath of the Lich King* should also be wary. Cybercriminals will also continue to capitalize on the global financial crisis, playing on the consumer landscape of thrift by creating economically-themed emails, fake e-coupons, bogus work-at-home schemes, and other efforts to cash in on the desire to save money.

Cybergang wars will make headlines.
Security researchers are seeing virus wars, worm wars, and botnet wars—due to increasing competition for financial gains from phishing and fraud, as well as the downsizing of criminal cybergangs, and improvements in security solutions. Look for growing competition between Eastern Europe and China to determine which country's crooks will be the first to include the latest exploits in their exploit kits.

Virtual worlds will experience more real-world trouble.
Many threats encountered in the real world will also crop up in the virtual world. Since cybercriminals need large audiences to perpetrate their crimes, they have begun preying on residents in virtual worlds and players in online games, particularly in Asia where these games have become extremely popular. The number and kind of threats in virtual worlds runs the gamut of human behavior and can be as innocent as password sharing between partners, as sophisticated as real estate fraud, and as malicious as gangs hunting for newbies to kill. Look for virtual threats to become an even greater problem in 2009.

Broken DNS issues will continue to create headaches.
Cybercriminals will leverage identified loopholes in the DNS (domain name system) registry loopholes to perpetrate new schemes in 2009. According to experts, bad guys are already using the poisoned DNS cache to create covert communications channels, bypass security measures, and serve-up malicious content. Although the security community, including Trend Micro, is working closely with registries/registrars where possible, this is an issue that ICANN (Internet Corporation for Assigned Names and Numbers) must address—the sooner the better.

Unlike the global economy, the underground economy will continue to flourish.
Cyber crime has become big business and unfortunately, 2009 will witness its continued growth. Increases in info-stealing malware, geared toward stealing login credentials and banking and credit card information, will continue to thrive. In addition, rogue applications are big business in the underground, as well as malware auction sites. This business will grow, fueled by competition and price wars beginning to occur between Chinese malware writers and Eastern Europe coders.

Identity theft will increase worldwide.
The ease with which criminals can buy and sell confidential information, combined with the fact that few countries have any laws that address it, will help identify theft continue to impact unsuspecting victims in 2009. According to the Identity Theft Research Center (ITRC), reports of data breaches have reached an all-time high. The total number of reported data breaches recorded by the ITRC was 47 percent higher than the same time period in 2007. According to the report, only 2.4 percent of all breaches had encryption or other protection methods in place and only 8.5 percent were using password protections. The report also stated that 82.3 percent of all breaches are electronic, compared to paper breaches. Predictably, the financial, banking, and credit industries have remained the most proactive groups in terms of data protection, as measured over the past three years. Of all categories, the business category most needs to enhance and enforce security measures, reporting the highest number of breaches in 2008, compared to education, government/military, healthcare, and financial services.[16]

Spam volumes will continue to grow.
No surprise here—around 115 billion spammed messages are being sent every day, up from the average 75 billion in 2005 to 2006. Ninety-nine percent of spam comes from compromised computers, including those with malicious communication to and from remote users. Spam is all about numbers as the more spam sent, the greater the chance users will click. Spam will not go away but it will increasingly employ social engineering techniques to improve its conversion rates.

Best Practices—What You Can Do

Home Users

Users are the first line of defense in protecting against malware attacks. The following tips can help you stay safe in 2009.

Protect your personal information.

- Never disclose personal information in response to an email request or an online pop-up message. Banks and other companies never request sensitive, personal information such as account details and Social Security numbers over the Internet. They are also unlikely to request you call a phone number provided in an email to verify information. Instead refer to phone numbers on your financial statements or on the back of your credit card and only share credit card details with reputable online retailers and auction sites. These organizations typically provide secure internal message centers or transaction histories to check for important correspondence and transactions. Avoid using public or shared computers when accessing financial accounts or conducting online transactions and exercise caution when using a PC in a wireless hotspot.
- Avoid solicitations for donations. Limit online charitable donations to organizations you know and trust. Common donation scams include foreign lotteries, the "Nigerian" email scam, cure-all products, debt relief, and anything promising an unbelievable return on investment.

Don't talk to (virtual) strangers.

- If you are a virtual world player, never use a login or password outside of the viewer or authentic web site. Also, keep passwords and security answers secret from anyone in-world. If possible, join an in-world guild for safety when first exploring a new virtual world and read all official site bulletin board warnings.

Protect your PC from threats.

- Keep security software up to date. Regularly updated security software will catch most exploits. For example, products such as Trend Micro Internet Security Pro or Trend Micro Internet Security include integrated vulnerability and exploit prevention, firewalls, and content filtering. Download a free web site reputation service, such as TrendProtect, to help you avoid surfing to web pages that feature unwanted content and hidden threats.
- Patch Windows and keep all applications up to date. Cybercriminals target vulnerabilities in the most popular applications and operating systems—everything from Internet Explorer and Quicktime to Adobe Flash Player and Windows. For this reason, apply security updates not only on operating systems but to all often-used programs. Also, apply security updates to third party software, which can act as an attack vector for malware even when your operating system is fully patched. Enable automatic updates whenever possible.
- Disable any default automations. Default settings within operating systems or applications are the preferred method for starting or installing malware.

Be cautious when clicking on links and file attachments.

- Click only on links and email attachments from known and trusted sources. If an email seems suspicious, consider that a friend's email account may have been compromised or spoofed in a phishing attack. With cybercriminals targeting many popular social networking sites, you cannot always ensure that your "friends" are truly sending an email. Run a virus scan on a suspicious attachment and check the URL with a web reputation service. Or consider calling the sender by phone if you are unsure.
- Avoid clicking on any link displayed as a numeric IP number, rather than a domain name, as bots often use numeric links to perform malicious actions.

Browse safely.

- Disable browser scripting and avoid downloadable widgets wherever possible. Many web-based attacks use various scripting languages to run infectious programs in a browser or use downloadable "widgets" to execute infections locally.
- Download software from trusted web sites only. Free games and file-sharing software may come bundled with malware. Be cautious when downloading applications on social networking sites. The applications may be harmless but may be easily compromised.

Use PC-related devices with caution.

- Monitor where external devices are used and update all security software to combat potential threats. Digital picture frames, iPods and other MP3 players, PDAs, USB sticks, flash drives, digital cameras—all these devices can harbor malware that can cripple a home network.

Safeguard mobile devices.

- Lock your mobile phone to prevent data theft or the installation of spyware or other unscrupulous applications. Also, delete text messages from unknown senders and download ring tones and games only from legal, official web sites. If an application appears to be infected, delete it immediately. Change Bluetooth settings to "non-discoverable" or "hide" to avoid attempts to pair or connect with a mobile phone or device propagating a virus. Also, when using Bluetooth, be careful when accepting files to avoid possible infections or viruses. If a mobile phone becomes infected, turn off all Bluetooth functions so malware on the phone cannot locate new targets and "reflash" your device to return it to factory settings.

Businesses

Because Trend Micro predicts an increasingly complex and crowded threat landscape in 2009, businesses should observe the following precautions to avoid new threats and ensure a safer computing experience for all network users:

Protect proprietary information and safeguard computing assets from threats.

- Ensure security updates are installed for both operating systems and applications. Activate automatic update features and apply new updates as soon as they appear to maintain a secure configuration and remain fully patched with the latest versioning.
- For the enterprise, deploy vulnerability scanning software on the network then schedule it to run weekly, at a minimum. Using Microsoft Update instead of the Windows Update service (which only updates the operating system) ensures all registered Windows desktop programs remain current.
- Regularly update media play plug-ins such as Windows Media Player, Apple QuickTime, VLC, Adobe Flash Player, and Adobe Shockwave.

Safeguard browser applications.

- Deploy the most recent versions of all browser software, such as Internet Explorer 7.0. For users who prefer Mozilla Firefox, an add-on called "noscript" protects the browser by allowing JavaScript, Java, and other executable content to run only from chosen, trusted domains while guarding against cross-site scripting attacks (XSS). This helps prevent exploitation of security vulnerabilities without sacrificing browsing functionality.

Create workplace policies.

- Clearly dictate security policies regarding data access and distribute and enforce the policies across the enterprise. For example, some IT departments prevent unnecessary protocols from entering the corporate network, such as P2P programs such as Napster and IRC chat.
- Develop corporate guidelines that advise against opening attachments, clicking on malicious email links, and installing files from unknown companies or organizations.
- Coordinate policies with cross-functional teams that include IT, purchasing, human resources, and legal departments.

Educate employees.

- Protect enterprise data by educating users about emerging threats and their consequences, emphasizing business-specific outcomes such as a damaged reputation, lost customers, or regulatory fines.
- Be specific—explain to employees where they may or may not surf. For example, many employees are unaware that Trojans and other malware can appear as blog comments and other code embedded on web pages.
- Advise employees not to disclose sensitive information when receiving emails or telephone calls. Boosting safety awareness is an integral part of a layered protection strategy.

Synch safely.

- Authenticate users and devices before data can be accessed.
- Secure devices against theft and loss, using security procedures similar to those for laptops.
- Synchronize essential files only to minimize data leakage.
- Recognize that users do not require all data. A solid content management policy restricts data access, only distributing it on an as-needed basis.

Install a multi-layered protection strategy.

The constantly evolving web threat landscape creates challenges to stay up-to-date on every method and mode of protection. For this reason, Trend Micro Web Threat Protection solutions provide a multi-layered defense against malware that leverages the interactive nature of the Internet—protecting the user's information at the gateway, in the network, on the endpoint, and in the Internet cloud before threats reach the desktop. Trend Micro recommends a multi-layered protection strategy, which ideally includes the following:

- **Anti-malware protection:** Malicious software can be as damaging as a careless employee or a contractor who leaks data. For this reason, anti-malware products and services should be installed on the corporate network and network devices to prevent malicious software from entering systems. Examples include Trend Micro Enterprise Security, which correlates web, email, and file reputation data in real time and Worry Free Business security, which includes web threat protection, location awareness features, application behavior monitoring, and multilayer spam blocking. For large organizations, Trend Micro offers a Vulnerability Assessment package, which is used in tandem with the Control Manager to assess and report on the current network security level and to identify potential security vulnerabilities.

- **Data leak prevention software:** Data leak prevention software prevents leaks by filtering content to determine in real time whether an employee is working with sensitive data, and if so, which policy to invoke. For example, Trend Micro provides LeakProof,™ a software solution that prevents information leakage by combining endpoint enforcement with highly accurate fingerprinting called DataDNA.™ The anti-leak agent provides intelligent content filtering and policy enforcement, and the DataDNA server provides policy management and violation monitoring. Additionally, locate protections at the endpoint so data is analyzed on the user's PC or at the server.
- **Encryption:** Encryption is an essential component of a data protection strategy and prevents data from falling into the wrong hands. Encryption will not, however, protect against authorized insiders who accidentally or intentionally leak data.
- **Access controls:** Proper access controls provide an important framework for preventing leaks. Allowing only authorized personnel to access networks, applications, and systems reduces information leakage.
- **Web security:** To counteract malicious banner advertisements, Trend Micro URL filtering technology classifies and filters out undesirable web sites, preventing users from accessing designated web sites via policy enforcement. (Administrators should therefore block related URLs.)
- **Endpoint Protection:** To help protect mobile users on laptops, consistently update all systems and choose security products with in-the-cloud updates.
- **"In-the-cloud" protection:** Because conventional security solutions no longer adequately protect against the increasing volume of new threats, content security vendors have been forced to adopt new threat countermeasures. The most effective of the new approaches is a next-generation cloud-client content security infrastructure that blocks the latest threats before they reach a user's PC or a company's network. The next generation of web threat protection involves hosted security solutions "in the cloud," which provide constantly updated techniques for intercepting threats before they can enter a business network. By checking URLs, emails, and files against threat databases in the cloud, customers have access to continuous updates wherever they connect—from home, within the company network, or on the go. The hosting vendor conducts all updates and maintenance, allowing customers to leverage the vendor's security expertise.

  By incorporating in-the-cloud reputation, scanning, and correlation technologies, in-the-cloud protection reduces reliance on conventional pattern file downloads and eliminates the delays commonly associated with desktop updates. Businesses benefit from increased network bandwidth, reduced processing power, and associated cost savings.

At most businesses, security is not a goal in itself, but a means to accomplish the company's core competency. For this reason, relying on a trusted third party that continually upgrades its protection systems makes the most sense. In-the cloud technologies, like Trend Micro's Smart Protection Network, incorporate in-the-cloud reputation, scanning, and correlation technologies to help organizations reduce their reliance on conventional pattern file downloads and eliminate the delays commonly associated with desktop updates. Companies benefit from increased network bandwidth, reduced processing power, and a faster response against today's threats.

References

1. AV-Test GmbH, www.av-test.org
2. Ashley Clark, "Report Claims IT Underestimates Scope of Malware," IT News, June 5, 2008, http://www.itnews.com.au/News/77674,report-claims-it-underestimates-scope-of-malware.aspx
3. "The New IE exploits for Advisory 961051, Now Hosted on Pornography Sites, "Microsoft Threat Research and Response Blog, December 13, 2008, http://blogs.technet.com/mmpc/archive/2008/12/13/the-new-ie-exploits-for-advisory-961051-now-hosted-on-pornography-sites.aspx
4. AV-Test GmbH, www.av-test.org
5. Alex Rodriguez, "Russian Hackers target U.S., Europe for Profit and Politics," Chicago Tribune, December 26, 2008, http://www.chicagotribune.com/news/chi-russia-hackers2_rodriguezdec26,0,5001855.story.
6. Ibid.
7. Ibid.
8. Sarah Arnott, "How Cyber Crime Went Professional," The Independent," August 13, 2008. http://www.independent.co.uk/news/business/analysis-and-features/how-cyber-crime-went-professional-892882.html
9. Ibid.
10. Ibid.
11. Ibid.
12. Tom Ramstack, "FBI Notes 'Uptick' in Employment Scams," The Washington Times, December 28, 2008, http://www.washingtontimes.com/news/2008/dec/28/scams-target-vulnerable-job-seekers/
13. "2008 Data Breach Totals Soar," *Identity Theft Research Center web site*, January 5, 2009. http://www.idtheftcenter.org/artman2/publish/m_press/Breach_List_2008_Q2.shtml
14. Ibid.
15. Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, and Nagendra Modadugu, "The Ghost in the Browser Analysis of Web-based Malware," Usenix.org, May 2007, http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf
16. "2008 Data Breach Totals Soar," *Identity Theft Research Center web site*, January 5, 2009. http://www.idtheftcenter.org/artman2/publish/m_press/Breach_List_2008_Q2.shtml

Trend Micro Inc.
10101 N. De Anza Blvd.
Cupertino, CA, 95014, USA

- Toll free: 1+800-228-5651
- Phone: 1+408-257-1500
- Fax: 1+408-257-2003