

# State of the Internet 2009: A Report on the Ever-Changing Threat Landscape

CA Internet Security Business Unit  
Internet Security Intelligence Report

---

## About This Report

“State of the Internet 2009: A Report on the Ever-Changing Threat Landscape” (CA Internet Security Business Unit [ISBU], Internet Security Intelligence Report) is a compilation of findings offering an overall perspective of the status of the threat landscape in 2009. The report is written by CA ISBU’s global team of security researchers and threat experts, and it delivers insights and analysis based on data gathered from notable threats, trends and statistics from January to June 2009. This report also includes tips and reminders on routine PC security and safe online behavior.

For regular updates about Internet threats and timely research news, please visit the CA Global Security Advisor Web page:  
[ca.com/us/global-technology-security.aspx](http://ca.com/us/global-technology-security.aspx)

### Author

Methusela Cebrian Ferrer  
Senior Research Engineer, CA ISBU Melbourne, Australia

### Contributors

Don DeBolt  
Director of Threat Research, CA ISBU USA

Kenneth Yu  
Research Engineer, CA ISBU Melbourne, Australia

Mary Grace Gabriel  
Research Engineer, CA ISBU Melbourne, Australia

Rossano Ferraris  
Research Engineer, CA ISBU EMEA

Venkatachalabathy Sr  
Research Engineer, CA ISBU India

Zarestel Ferrer  
Senior Research Engineer, CA ISBU Melbourne, Australia

# Executive Summary

More people than ever use the Internet for work and pleasure, and most people use it frequently. With the explosion of Internet services and the evolution of Web-based communities, users spend more time online and engaging in social activities on the Internet than ever before; many consider the Internet an integral part of their daily lives. Because of the Web's immense popularity, it is no surprise that attacks that exploit these services and communities are on the rise. Cybercrime costs consumers and businesses \$5.8 billion in 2009, according to the Federal Bureau of Investigation (FBI). Billions of dollars are lost every year repairing systems hit by attacks and in lost productivity from disruptions.

In the first half of 2009, CA Internet Security Business Unit (ISBU) observed aggressive adaptation of Web-based attacks as an entry point and threat distribution vector (or method used to attack a target). The Internet has proven to be a dangerous place, and people are more likely to encounter malware through browsing, searching or merely visiting legitimate sites than ever before. Attackers go where the targets are. During the first six months of 2009, 78% of threats came from online interaction, and of those threats, 71% were trojans. Trojans are lightweight, malicious software that can be used as gateways for attackers to conduct cybercrime or gain control of users' computers remotely via global bots and botnets.

Organized cybercriminals continuously improve their attack methods, often exploiting both software and human behavior, while evading security scanners through automated repackaging and obfuscation of malicious software. News trends, search keywords and popular events are on the watch list of cybercriminals, who take advantage of Internet analytics to deploy and perpetrate massive attacks. These cybercriminals hope to persuade users to open an e-mail attachment or click on a Web link. Or they may victimize people through social networking sites or poisoned search engine results.

## REPORT HIGHLIGHTS

Web-based attacks as infection vectors are increasing and are effective gateways for distribution of threats.

- Prevalent malware families account for 71% of total infection for January through June 2009.
- Rogue security software is the most prevalent malware infection.
- Attackers take advantage of rich content and media formats such as PDF, SWF, GIF and JPEG for malware infection.
- Win32/Koobface and bogus profiles proliferate in social networking sites.
- Three variants of Win32/Conficker emerge in the first half of 2009.

Cybercriminals' extensive use of malware represents an advanced underground economy. Cybercriminals take aggressive steps to automate attacks and compromise legitimate Web sites. These threats can lead to multiple redirections and drive-by exploits—and even zero-day attacks.

Cybersquatting and typosquatting are growing threats, wherein malicious Web sites use visual mimicry to deceive users into believing their transactions and activities are taking place at reputable sites. This technique is becoming a prevalent threat distribution vector for both Windows and Macintosh computers.

Social networking sites are also attracting scammers, attackers and fraudsters who are primarily motivated by financial gain, although some are driven by curiosity or notoriety. Users' trust in these sites and the proliferation of these threats makes it easier for attackers to create malicious software that purports to have a security benefit.

Attackers can be quite sophisticated and constantly develop new tricks to scam people. Ransomware, which extorts money from its victims in order to restore or unencrypt data, is a serious threat, as it can do significant damage once a user has mistakenly installed it. Game-password stealers and banking trojans are identity-theft threats and are a common form of malware.

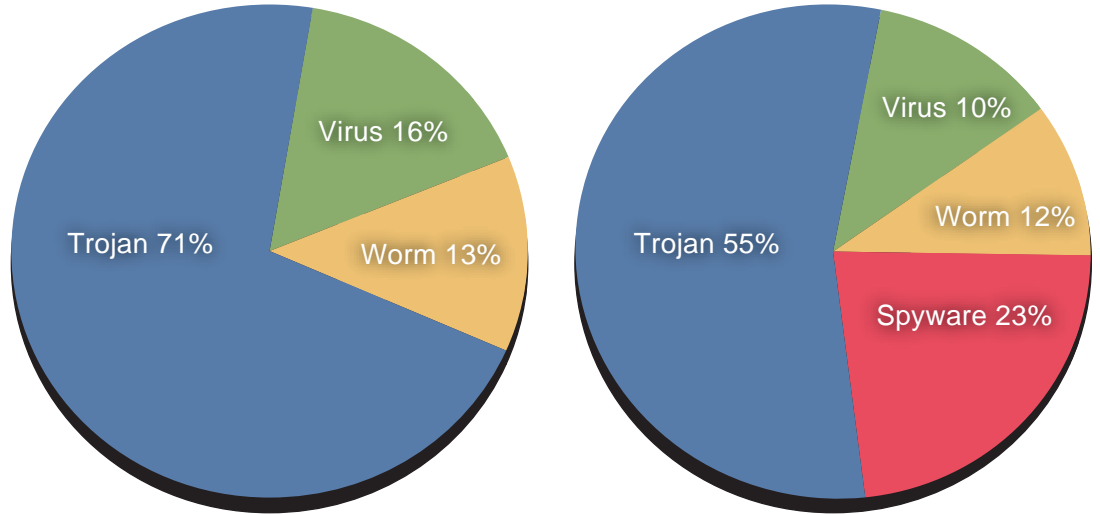
A sampling of malware file types taken during the first six months of 2009 found that Windows Portable Executable (PE) files accounted for 92% of the total collection. The use of executable files allows attackers to perpetrate further malicious activities following a successful attack. This time period also shows a significant increase in the use of rich content and media files to perform malicious activity.

The most common threats were trojans, representing 71% of the total infections for the first half of 2009. The remaining 29% of threats were emerging threats where malicious code was used for targeted attacks, new threats and zero-day threats.

This report discusses each of these attack vectors, explaining how they exploit their victims. It also discusses the prevalence of each threat type and its typical means of distribution.

## Threat Landscape

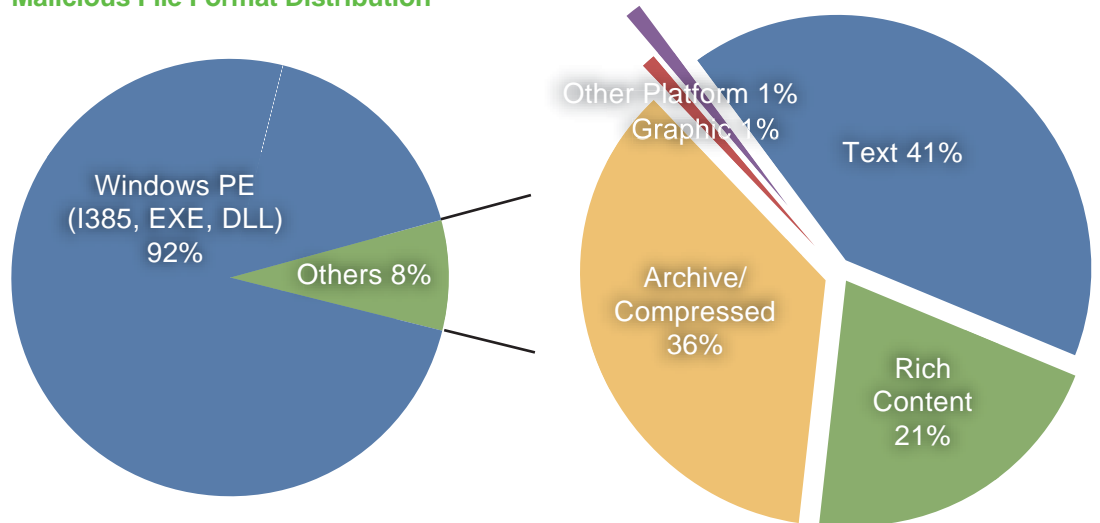
### Infection Distribution



CA ISBU receives and processes reported infections from CA customers and partners around the world. In the first half of 2009, trojans were the most prevalent malware infection, accounting for 71% of the total sample collection (see figure on left). If we define spyware separately from trojans, then spyware infections become second in rank in the overall threat landscape (see figure on right).

Additionally, more users were affected by undetected strains of known, complex viruses like Win32/Virut, which is a parasitic file infector.

### Malicious File Format Distribution



Tracking attackers' use of various file formats aids our understanding of infection and propagation. Windows PE executable is the most common form of malicious file, accounting for 92% of infections reported to CA ISBU. The use of executable files allows attackers to perpetrate further malicious activities following a successful attack.

The remaining 8% of attacks are referred to as misused and/or exploited files. Cybercriminals explore the potential for these files to carry out malicious tasks, often leading to the installation of one or more malicious Windows PE executable files.

### Distribution of Known Packed Files

While most malicious activities were carried through malicious Windows PE executable files, it is important to understand the types of packers, cryptors and compression commonly used by malware for obfuscation.

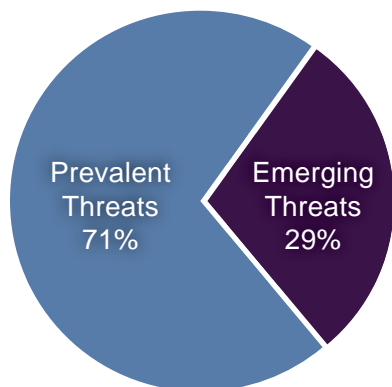
During the first half of 2009, 42% of the samples collected were identified as compressed, encrypted and/or packed files. UPX-packed files dominate, accounting for 33% of the total identified files, followed by UPolyX and Self-Extracting (SFX) files.

Self-extracting files are very common to trojan droppers, while archive files such as zip are prevalent among e-mail spammed trojans such as Win32/Mytob and Win32/Fruspam.

Packed File Name	%
UPX	33%
UPolyX	18%
SFX	11%
UPack	9%
PECompact	8%
FSG	7%
ASPack	4%
MsPack	4%
ACProtect	3%
PEncrypt	1%
Themida	1%

## Prevalence

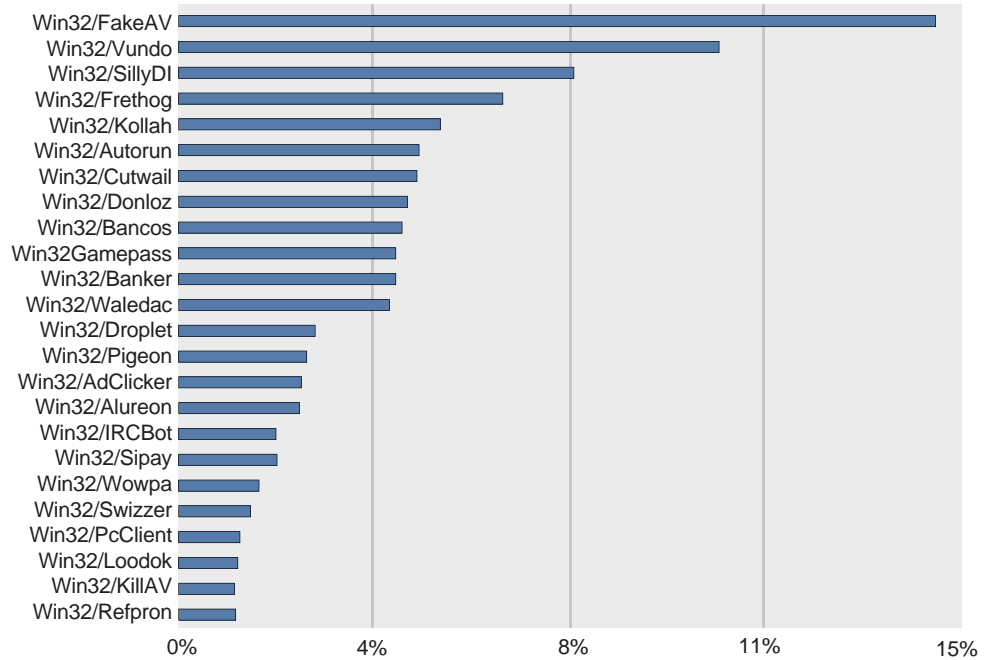
### Prevalent vs. Emerging Threats



CA ISBU handles and processes known threat families on a daily basis. These threats constantly change attack and distribution techniques, and attackers update their code to support new features and employ obfuscation to avoid detection by security scanners. This strategy is a resounding success for attackers, accounting for 71% of prevalent threats affecting users globally.

The remaining 29% of threats are emerging threats. These are generally targeted attacks, although they can also include high-profile malware such as Win32/Conficker and proof-of-concepts malcodes that are designed to display the attacker's prowess and new techniques.

## PREVALENT VS. EMERGING THREATS

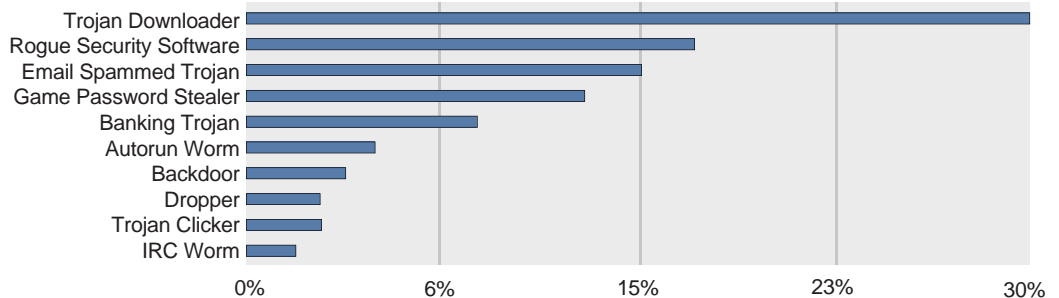


Based on the number of signatures created, Win32/FakeAV, a rogue security software, is the most prevalent malware family base, followed by known downloaders Win32/Vundo and Win32/SillyDI.

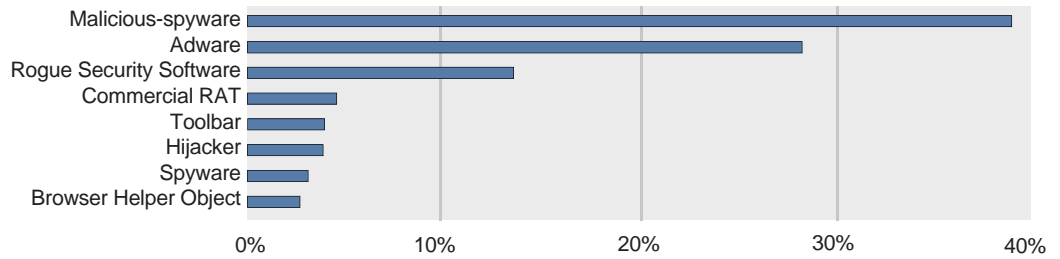
Although detection names vary by family of threat, CA ISBU classifies them to help identify the most prevalent types of malware. When all families of the same types are added together, Trojan downloader is the most prevalent type of threat, followed by rogue security software and e-mail spammed trojans, known as Win32/Waledac and Win32/Kollah.

Game-password stealers, banking trojans and autorun worms were among the most widely observed threats causing infections.

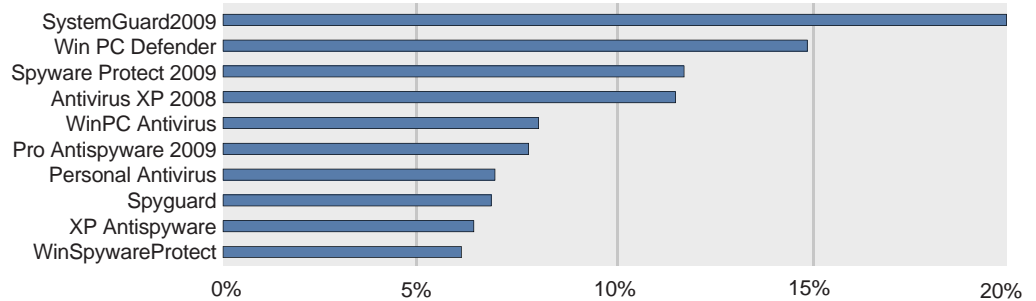
## MOST PREVALENT MALWARE FAMILY



### MOST PREVALENT SPYWARE INFECTIONS



### MOST PREVALENT ROGUE SECURITY SOFTWARE



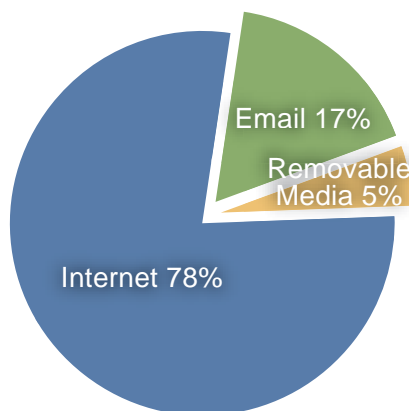
### MOST PREVALENT ADWARE FAMILIES

Adware Family	Description
Zango SA	This adware monitors users' browsing behavior and sends advertisements in the hope that users will purchase from an affiliate advertiser. Zango tempts people via pop-up advertisements, directs them to questionable Web sites, and communicates to other servers without the users' knowledge.
Trymedia	This adware agent monitors users' browsing habits to facilitate targeted pop-up ads. By adding a Browser Helper Object to the users' default browsers, Trymedia monitors Web users and communicates a profile of their banking and shopping habits to a third-party advertising server. Trymedia is known to be bundled with several free online games, including those published by MumboJumbo, Playfirst and ValuSoft.
Hotbar	Hotbar is marketed as a program that adds graphical skins to Microsoft Internet Explorer toolbars; it also adds its own toolbar. Hotbar monitors all URLs visited by users and adds link buttons to their toolbars accordingly.

CA ISBU data shows that spyware-infected systems are now mostly infected with malicious files that have been bundled and downloaded with other infections, such as adware and rogue security software. This landscape reflects the increase in organized cybercrimes, where the distribution of malware and spyware provides a gateway for further installation of threats onto the affected machines.

## Threat Vector

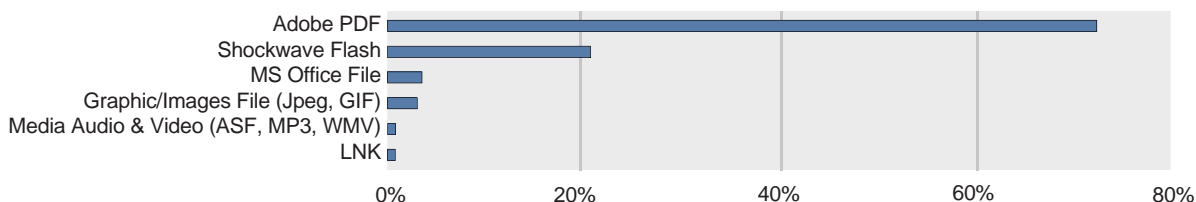
### Most Prevalent Threat Distribution Vector



The Internet is the primary threat distribution vector. Reports to CA ISBU show that the Internet accounts for 78% of infections, while e-mail and removable media account for 17% and 5% of infections, respectively. It should be noted that Conficker can spread through removable media.

Exploited and/or misused file formats are a fast-growing threat distribution vector. Adobe PDF accounts for 71% of the most exploited file formats, followed by Adobe Shockwave Flash and Microsoft Office files, including Word, Excel and PowerPoint.

### MOST EXPLOITED FILE FORMATS



## Notable Threats

### Rogue Security Software

Rogue security software has experienced a significant surge in popularity among grey-market and black-market businesses. Rogue security software is an application that appears to be beneficial but delivers a fraudulent marketing scheme; it displays fake infection results and promises to remove “infected” files if the user installs the software. It claims to provide security, while doing the opposite. Users who fall prey to such tricks are bombarded with annoying fake and erroneous alert messages, exposing them to additional Internet threats.

Rogue security software is bundled with a variety of threats, which often include downloader and rootkit components. These threats lead to the installation of additional threats, making it more difficult for most security scanners to provide a complete system-clean for these types of infections.



Rogues are perpetrated by organized cybercriminals for financial gain. The prevalence of these types of threats entices malicious users to participate, evidenced by other threat families that support rogue security software.

Malware Family	Description
Win32/FakeAV	Generic detection for the rogue's main installer
Win32/FakeAVDI	Generic detection for trojan downloaders that install rogue security software
Win32/FakeAlert	Generic detection for the rogue trojan component that displays alert messages
Win32/Clst stealth Win32/Tdst stealth	Trojan rootkit often associated with rogue security software
Win32/Bugnraw Win32/Oneraw Win32/Refpron Win32/Donloz Win32/Droplet	A family or trojans that participates and leads to rogue security software infection

### Conficker

The first half of 2009 was an active time for the Win32/Conficker family, and Conficker is believed to be the largest worm infection since 2003. In late December 2008, the second variant of Conficker, Win32/Conficker.B, was found in the wild.

Win32/Conficker.B aggressively propagates from removable drives and shared folders within the affected network. It communicates with other infected machines through its own peer-to-peer protocol while participating in a global botnet.

In late February 2009, CA ISBU received a new variant of Conficker known to most security vendors as B++ and C. The variant was also classified as Win32/Conficker.B because of its similarity to the earlier version.

Win32/Conficker.C made a dramatic debut in early March 2009. This threat was more complex because attackers added a rendezvous procedure that allowed Conficker to send and receive information via remote commands to other Conficker-infected machines. Early variants generated 250 pseudo-random domain names with which Conficker's authors would attempt to establish communication. The improved 'C' variant generates 50,000 pseudo-random domain names then communicates with 500 randomly selected domains.

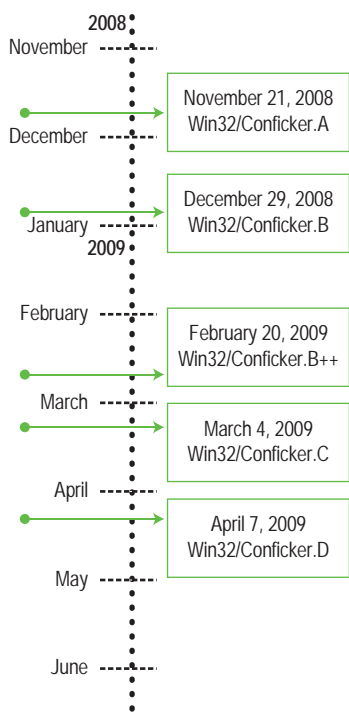
The 'C' variant became the distribution gateway for the next variant, Win32/Conficker.D, which was first deployed on April 7, 2009. Along with this Conficker update came other prevalent threats, including Win32/Waledac, Win32/FakeAV and Win32/Vundo, which are known malware families perpetrated by organized cyber-criminals.

Today, security professionals around the world are collaborating through the Conficker Working Group to monitor and mitigate issues brought about by this menacing malware.

### File Infectors

Win32/Virut is another notable threat that has been active during the first half of the year. Virut is a family of polymorphic file-infectors that attaches its code in varying ways. When an infected file is executed, Virut's code runs before any host program code. The virus decrypts and then injects parts of its code into all running processes.

Conficker Timeline



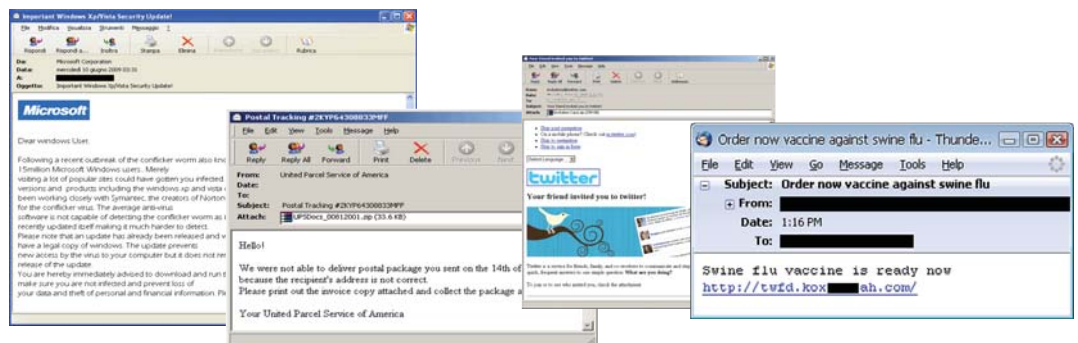
Type of Infection	Description
Appending	This type of file infector attaches its code at the end of the target file and modifies the file entry point to be able to run itself when executed.
Cavity and Appending	Cavity is a type of virus that seeks out unused space within the file and inserts its own code.  Cavity and appending viruses seek out unused space and insert their own code while other parts of the code are added at the end of the target file.
EPO, Cavity and Appending	An entry-point obscuring (EPO) virus inserts a redirection code through a jump/call routine and flows in a nonlinear direction according to the attacker's obfuscation logic. EPO viruses are regarded as complex and challenging for most security scanners to detect and cure.  EPO, cavity and appending viruses seek out unused space, insert code, and add part of their code to the end of the target file, simultaneously using an obfuscation technique.
EPO and Appending	EPO and appending viruses attach code at the end of the target file and employ an obfuscation technique.

CA ISBU infection reports are mostly dominated by viruses that use a combination of entry-point obscuring (EPO), cavity and appending infections. These types of viruses are complex and challenging to detect and cure. The second most common infection type is appending.

### E-mail Spam

After the Web, e-mail is the most common distribution method for threats. Some 80% to 90% of e-mail on the Internet is spam, and spam usually contains links to malicious or compromised Web sites. Spammers send e-mails that use social engineering techniques to persuade people to participate in their scams. By definition, e-mail spam refers to any fraudulent or unsolicited e-mail. Spam also includes e-mail where the sender's identity has been forged or that has been sent through unprotected SMTP servers, unauthorized proxies or botnets.

### SPAM LEADS TO MALWARE INFECTION



Attackers constantly change their spamming schemes and strategies to elude spam filters and exploit realistic events and topics to achieve their goal of installing a malicious program. Spam is no longer obviously spam. "UPS Postal Tracking" and "Microsoft Security Update," for example, are fraudulent e-mail messages that seem legitimate. They convince users to download and execute a malicious file that is either attached or referred to in a malicious URL.

"Twitter invitation notification" is a sample e-mail spammed by Win32/Fruspam. This type of e-mail spam forges the sender's identity or sends messages through unprotected SMTP

servers, unauthorized proxies or botnets. Another prevalent type of spam is unsolicited bulk e-mail, which is often sent in large quantities. The Win32/Waledac “Swine Flu” e-mail campaign is a good example of unsolicited bulk mail, which can be compared to the early version of the Storm worm because it generates a spam e-mail message, and then sends it in large quantities.

### Ransomware is Back

Ransomware has experienced a resurgence in popularity. New families of ransomware emerged in the first half of 2009. Ransomware is used to encrypt users’ files and data, making it unusable. Cybercriminals then offer to decrypt the locked files and data for a fee.

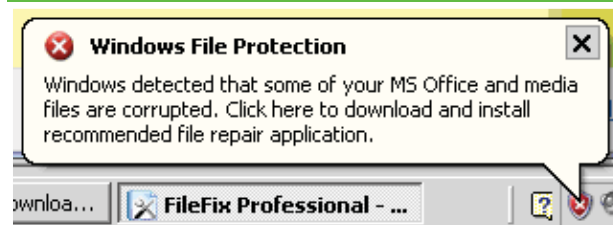
A classic example is the ransomware duo Win32/FileFixPro2009.A and Win32/RansomFix.A, widely known as “FileFix Pro 2009.” Win32/RansomFix.A encrypts media and document files on an affected system and informs the user that these files are “corrupted.”

To repair the files, Win32/RansomFix.A redirects the user’s browser to a Web site hosting Win32/FileFixPro2009.A. The user is then advised to purchase “FileFix Pro 2009” for \$49.95 to fix the “corrupted” files.

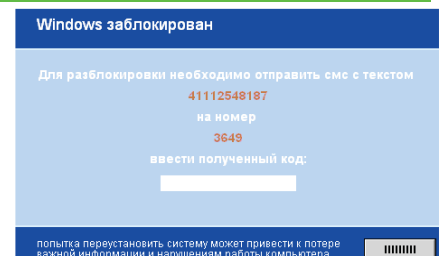
Win32/RansomSMS is different. Instead of encrypting files, this ransomware locks the system desktop and instructs the user to send a premium SMS message to a particular number to receive the unlock codes.

Ransomware families observed during January through June 2009 were extremely aggressive in their attempts to make money with “scareware” or rogue security software. Ransomware looks and behaves in a similar way to scareware, except in the background it locks the system by disabling all running applications while allowing critical system files to run. This threat then notifies the affected user to purchase the rogue security software, enabling further control of the system.

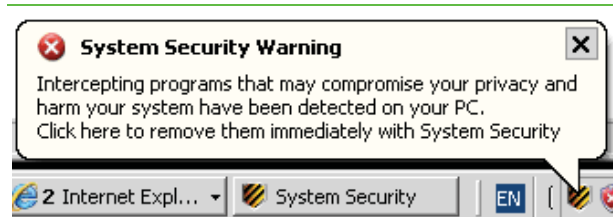
### FileFix Pro 2009



### FWin32/RansomSMS DESKTOP LOCK



### “INTERCEPTING PROGRAMS” MEANS DISABLING ALL RUNNING APPLICATIONS





### Mac OS X Threats

Security threats have come to the Mac. Zlob, a family of trojans notorious for distributing fake codecs since late 2005, has affected Window users through social engineering. As the Macintosh platform became more popular, Zlob authors developed OSX/RSPPlug (also known as “DNSChanger”) and OSX/Jahlav.

In late 2007, Zlob fake codec distribution servers served up two executables: EXE for Windows and DMG for Macs. These threats continue to proliferate, and more Mac users are reporting infections. Furthermore, during the first half of 2009, CA ISBU spotted two new, notable OS X malware threats:

- OSX/Krowi.A was discovered early this year. It uses piracy to reach OS X users looking for cracked “iWork 09” installation packages with a serial key. This threat is the first peer-to-peer-controlled bot in the Macintosh environment, with isolated incidents compared to OSX/RSPPlug infections.
- OSX/Tored is the latest OS X threat family. This malicious code is written in RealBasic and compiled specifically for Intel-based Macs. Attackers designed the threat to mass-mail a copy of itself and propagate through affected network and removable shares. However, bugs in its code render this threat incapable of performing malicious activities.

### Cybersquatting and Typosquatting

Cybersquatting refers to Web sites that intend to profit from known, legitimate products or offers by visually deceiving users into believing their transactions are real and in good faith. Typosquatting is an act of registering domain names that resemble legitimate ones by using similar-sounding words and spellings.

Attackers take advantage of legitimate Web sites like Google, Microsoft and YouTube by deploying a typosquatting attack. An unsuspecting Internet user could fall victim to the attacker’s trap by mistyping a word. Splogging, which is spam in blogs, allows these legitimate-looking URLs to reach more users and increases the chances for infection. Cybersquatting and typosquatting are becoming prevalent threat distribution vectors for both Windows and Macintosh platforms.



### Web 2.0 and Social Media

The evolution of the Web from static content to dynamic content has moved computing experiences into new dimensions. Online communities, video sharing Web sites, wikis, blogs and social media are a global phenomenon, enticing more people across a wide variety of demographics to interact, share, update and connect to the Web 2.0 world. At the same time, this dynamic environment also created new opportunities for attackers to deploy and carry out malicious activity.

Cyberbullying, pornography, hactivism, hacking, phishing, scams, hoaxes, spam and malware are examples of Internet security threats that can masquerade in online communities and on social networking sites as good and trusted pals.

Win32/Koobface is an example of a worm propagating through social networking sites. It uses the affected user's login credentials to send messages to his or her list of connected friends and family, persuading them to perform certain actions. In the first half of 2009, CA ISBU created more than 100 signatures to detect the numerous Win32/Koobface family variants.

### BOGUS BLOG PROFILE

- yetto4med47276.blogspot.com
- violetapharm26896.blogspot.com
- valoriehealth24254.blogspot.com
- tynishapharma42681.blogspot.com
- terinapharm75883.blogspot.com
- tatyannamed93826.blogspot.com
- stephenpharm11128.blogspot.com
- sigridpharm35061.blogspot.com
- shylahealth62926.blogspot.com
- savannahmeds15631.blogspot.com
- saundrahealth89547.blogspot.com
- sashapharma29013.blogspot.com
- sandihealth33373.blogspot.com
- sammed50943.blogspot.com
- rosemariepharm43244.blogspot.com
- reneapharm25418.blogspot.com
- randapharm29650.blogspot.com

### Win32/Koobface LURES FACEBOOK USERS



Financially motivated organized groups are among the aggressive attackers and they automate massive, distributed attacks on a pool of target victims. Attackers created hundreds of bogus profiles to perform various tasks, including distributing malware, spamming and stealing users' online identities to perpetrate further cybercrime.

Popular online communities, blogs and social media sites such as YouTube, MySpace, Facebook and Twitter are absolute targets, particularly as their popularity grows. These communities and sites make it easier for attackers to use social engineering to exploit vulnerable users.

### Compromised Websites

In cyberspace, attackers prey on the vulnerable, and unfortunately, many Web sites, online communities and businesses have insufficient security, which leaves them vulnerable. This lack of security has become a notable threat distribution vector in which attackers use automated Web-based attacks to inject malicious code to spread malware infection, unbeknownst to the site owners.

### MALVERTISEMENT



Attack Vector	Definition	Related Malware
Malicious Ads: "Malvertisement"	Threats distributed through advertisements.	Actns/Sif and JS/SWF!exploit
Hacked Web Server	Threats distributed by infecting every page or selected pages on the Web server.  This type of attack was used in the massive infection, Gumblar-Martuz, where attackers harvested accounts and passwords using malware. These stealing and keylogging capabilities are often found in IRC bot trojans.  From harvested credentials, attackers manipulated the Web server by accessing it through FTP.	JS/Redirector, JS/Gumblar.A)
Cross-site scripting (XSS) attack	Threats are distributed by exploiting the XSS vulnerability in Web applications. Attackers inject malicious HTML tags, IFRAME tags and/or JavaScript to a vulnerable Web application, which can infect visiting users.	HTML/iframe!exploit and JS/iframe!exploit
SQL Injection	Threats distributed by exploiting the database layer of a Web application.  SQL injection allows the attacker to query, add and modify the database.  Attackers have also used mass SQL injection methods to distribute malware.	HTML/iframe!exploit and JS/iframe!exploit

## Search Index Poisoning

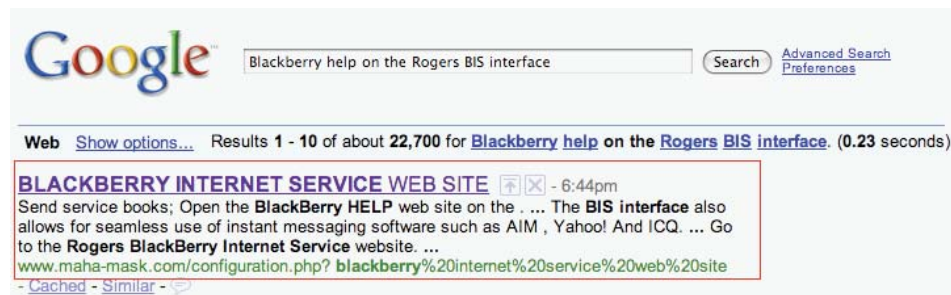
As today's most popular search engine, Google is a frequent target of online threats. Attackers employ sophisticated search engine optimization to manipulate search engine rankings and poison users' search results, which sends people to compromised Web sites and leads to malware infection. Given the vastness of Web content, it can be difficult for search engine companies to detect and control the manipulation.

### SEARCH RESULT LEADS TO ROGUE SECURITY SOFTWARE AFFECTING WINDOWS



Organized cybercriminals manipulate results by targeting specific key words in the same way rogue security software used cooking recipes as bait to lure users to infection in its "recipe campaign."

### SEARCH RESULT LEADS TO OSX/Jahlav "MacCinema" INSTALLER



Search engine manipulation also affects Macintosh users. In one example, attackers targeted people looking for Mac drivers, software, media downloads and fixes. This effective campaign gained users' trust and enticed them to click and manually install a Mac trojan.

## Rich Media and Content

Cybercriminals most commonly used Portable Document Format (PDF) and Shockwave Flash rich-media formats during the first half of 2009. Exploited PDFs first used for targeted attacks were soon adopted by organized cybercriminals for massive distribution of malware infection. These attackers implemented server-side automation to evade security scanner detection, and as a result, a malicious server generates a new file per request.

Exploited Functions	Affected	Detection
Collab.collectEmailInfo()	Acrobat and Adobe Reader 8.1.1 and earlier	PDF/Pidief
util.printf()	Acrobat and Adobe Reader 8.1.2 and earlier	PDF/Pidief and PDF/CVE-2008-2992!exploit
jbig2decode	Acrobat and Adobe Reader 9 and earlier	PDF/Pidief and PDF/CVE-2009-0658!exploit

Attackers also misused Shockwave Flash files to take advantage of the ActionScript feature to perform malicious activity on a user's system. Both the PDF and Flash threats belong to the ActnS/Swif family.

Trojanized media files such as Windows Media Video and MP3 (which CA products detect as ASF/Wimad) were another prevalent infection in the first six months of 2009. A threat detected as Win32/GetCodec discovered last year has a very notable capability: It searches for media files on the user's local and shared directories and modifies the system to invoke the user's default browser into opening a malicious Web site. CA ISBU also discovered trojanized media files being shared through media-sharing sites and communities, reaching more target users.

Image File Format	Detection and Description
GIF	GIF/iframe!generic is a detection for a family of misused GIF files where the attacker adds an iframe tag, often leading to a malicious Web site.  Win32/Gifdrop is a detection for a family of misused GIF files in which the attacker embeds a malicious executable.
JPEG	JPEG/iframe!generic is a detection for a family of misused JPEG files where the attacker takes advantage by adding an iframe tag, often leading to a malicious Web site.  Win32/Jpegdrop is a detection for a family of misused JPEG files where the attacker embeds a malicious executable.

Malicious image files such as GIF and JPEG are becoming notable malware distribution vectors, attempting to establish user trust via known file formats. The Windows shortcut LNK file was also spotted misusing legitimate features to connect and download malware; this family of threats is detected as LNK/SillyDI.

Microsoft Office files – Word documents, PowerPoint presentations and Excel spreadsheets – were also on attackers' lists. Microsoft Office files were crafted to take advantage of zero-day and known vulnerabilities and used for targeted attacks. CA ISBU detects this family of threats as PPT97/PPDropper, X97M/EXEDropper, W97M/ExeDrop for PowerPoint, Excel and Word files, respectively. Attackers' focus on targets of choice is particularly lucrative when the target is high value – say a high-ranking government official or business executive.

### Banking Trojans

The Federal Trade Commission (FTC) Consumer Sentinel Network Complaint Data Book recognizes identity theft as the number one complaint category in 2008. This theft often manifests as banking-related threats orchestrated to steal users' identities for financial gain. The organized groups behind banking trojans take advantage of compromised Web servers to carry out malicious activities. In fact, legitimate Web sites are now the target of most cybercrime attacks—they are used as a launch pad that provides the perfect platform to evade detection and network-blocking rules.

Banking trojans have been among the top malware families dominating the CA ISBU malware collection this first half of 2009. As most industrialized countries are experiencing economic crisis this year, banking trojans are flourishing.

Similar to rogue security software and pay-per-install threats (an affiliate payment model based on getting others to install a piece of software), banking trojans are financially

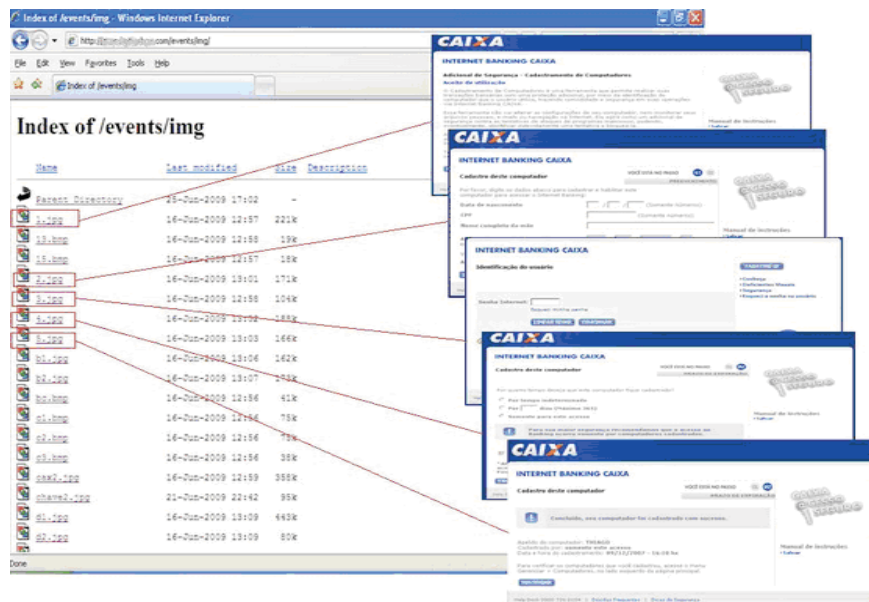
**LANGUAGE-SPECIFIC MALWARE MODIFIES BROWSER MENU, BUT THE CHANGE IS ONLY NOTICE-ABLE IF BROWSER IS IN ENGLISH**



motivated online crimes. They monitor computing activities of an infected system, waiting for the user to access banking or finance-related Web sites. They collect confidential information, including users' online credentials and credit card details.

Win32/Bancos and Win32/Banker are two prevalent banking trojan families, with most variants targeting Brazilian banks. This year, notable samples of these banking trojans came from phishing sites or attached to spam e-mails.

### A HACKED WEB SITE FOUND HOSTING BANKING TROJANS



## Safe Computing Habits

With the proliferation of Web-based attack vectors and the increase in global Internet usage, it is more important than ever to be cautious to ensure safety online. Security is a process. To be secure, you must be aware, apply the right technology, understand your daily computing activity and identify the amount of information or data you want to secure.

### Let the Technology Work for You

Here are some easy steps and reminders to ensure that your CA security product provides optimal protection for you.

1. Your security scanner must be always turned on and up-to-date with the latest signatures. Real-time scanning protects you from possible infection that you may get from compromised Web sites, network shares, e-mail and flash drives.
2. Turn on your firewall. Your firewall provides a different layer of security that guards you from network attacks and blocks unauthorized access to your machine. A firewall with real-time malware behavior intrusion detection could prevent or lessen the impact of malware infection.

3. Increase your browser security settings. You can refer to the CERT Web browser security tips at [cert.org/tech\\_tips/securing\\_browser](http://cert.org/tech_tips/securing_browser).

### Be Security-Aware

1. Do NOT open e-mail from people you don't know. Think twice and verify before clicking a URL or opening an attachment. Don't be click happy! All it takes is a moment of inattention.
2. Implement a strong password. Refer to these Microsoft tips for creating a strong password: [microsoft.com/protect/yourself/password/create.aspx](http://microsoft.com/protect/yourself/password/create.aspx)
3. When conducting online banking or financial transactions, make sure your browser connection is secure.
4. Encrypt online communication and confidential data.
5. Back up your important data. Keep a copy of all your files and store them separately.
6. Be cautious about instant messaging. Avoid chatting with people you don't know, especially if they ask for personal information such as photos or want you to do something for them.
7. Protect your identity while enjoying online social networking activities. Be wary of clicking links or suspicious profiles. Double-check the integrity of the connection or friend request before adding anyone to your network. Avoid installing extras such as third-party applications; they may lead to malware infection, or attackers could use them to steal your identity.
8. Avoid piracy by downloading from secure sources.
9. Avoid threats that use social engineering techniques by checking user feedback about a Web site before visiting it, and read feedback about an application before installing it.
10. If you are using Adobe PDF Reader, prevent your default browser from automatically opening PDF documents. Refer to our CA Security Advisor research blog entry at [community.ca.com/blogs/securityadvisor/archive/2009/02/24/attackers-love-zero-day.aspx](http://community.ca.com/blogs/securityadvisor/archive/2009/02/24/attackers-love-zero-day.aspx)
11. Check for and install security updates regularly.
12. Be careful with search engine results. Read them carefully and check to ensure that the content relates to your subject before clicking the Web site link.

Make Internet computing safe—  
report suspicious files and Web sites to [virus@ca.com](mailto:virus@ca.com)