

A background image showing a laptop on a desk with a speedometer overlay. The speedometer has numbers from 0 to 80 and a needle pointing towards 40. The scene is dimly lit, suggesting an office or laboratory setting.

2009's Most Persistent Malware Threats

Trend Micro, Incorporated 

TrendLabsSM

TrendLabs is Trend Micro's global network of research, development, and support centers committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery.

A TrendLabs Year-End Threat Roundup | 2009

2009's Most Persistent Malware Threats



CONTENTS

PERSISTENT MALWARE THREATS.....	3
PURPOSE OF THIS REPORT	4
DOWNAD/CONFICKER NETWORK WORM.....	5
<i>WHERE IS DOWNAD NOW?</i>	5
<i>WHY DOES THE THREAT PERSIST?</i>	6
<i>WHAT CAN YOU DO?</i>	6
<i>References</i>	7
KOOBFACE SOCIAL NETWORK WORM	9
<i>DISSECTING THE LARGEST WEB 2.0 BOTNET</i>	9
<i>WHY DOES THE THREAT PERSIST?</i>	10
<i>WHAT CAN YOU DO?</i>	11
<i>References</i>	11
ZEUS/ZBOT CRIMEWARE	13
<i>THE YEAR THAT WAS</i>	13
<i>WHY DOES THE THREAT PERSIST?</i>	14
<i>WHAT CAN YOU DO?</i>	15
<i>References</i>	16
ROGUE ANTIVIRUS APPLICATIONS.....	17
<i>WHY DOES THE THREAT PERSIST?</i>	19
<i>WHAT CAN YOU DO?</i>	20
<i>References</i>	20
ZERO-DAY EXPLOITS	23
<i>IE ZERO-DAY EXPLOITS</i>	23
<i>ADOBE ZERO-DAY EXPLOITS</i>	24
<i>OTHER MICROSOFT ZERO-DAY VULNERABILITIES</i>	24
<i>WHY DOES THE THREAT PERSIST?</i>	25
<i>WHAT CAN YOU DO?</i>	26
<i>References</i>	26
POSTSCRIPT	28
REFERENCES	29

PERSISTENT MALWARE THREATS

Enterprises are raring to harness the benefits of the Internet's connectivity and infrastructure for both core operations and support activities. The **generally positive response** toward moving into the cloud, the increase in the **use of social networking platforms for business**, and the continuous move toward a **mobile and interconnected workforce** gained momentum in 2009.

The risks of conducting business with the use of the Internet became readily apparent as well. According to **reports**, 18 percent of the respondents to the "Computer, Crime, and Security Survey" that reported security incidents in 2009 also experienced at least one targeted malware attack.

A separate study, the Ponemon/PGP report as reported by **CNET News** on the cost of a data breach due to criminal activity pegs loss to business at US\$215 per stolen record. Remarkably, the "criminal activities" in this report now include data-stealing malware and botnets. In fact, more of these attacks have been reported in 2009 than ever before.

A review of the *TrendLabs Malware Blog* entries in 2009 likewise calls attention to recurring themes in the security challenge for users and businesses alike. Cybercriminal organizations work hard to use old and new online platforms to trick even the more tech-savvy users into following a malicious link or into opening a malicious file. In the more insidious kinds of attack that will be discussed later (i.e., a network worm named DOWNAD), almost no user interaction is required for an attack to spread throughout a system of interconnected computers.

PURPOSE OF THIS REPORT

TrendLabs, Trend Micro's research lab, discusses 2009's most persistent threats and presents why users need to be more engaged in keeping their systems secure than ever before. These five most recurring and ever-present threats effectively challenge even the more tech-savvy businesses who encounter them either through lack of network security or of education and appreciation of the severity of threats on the part of employees. At the end of each discussion, a list of security dos are recommended for large enterprises and smaller businesses alike.

According to the Conficker Working Group, while DOWNAD has left the headlines, the worm remains quite active in the sidelines.

DOWNAD/CONFICKER NETWORK WORM

Millions of systems around the world succumbed to the infamous worm, DOWNAD. Network infections resulted in significant spikes in port 445 traffic, bandwidth issues, and inaccessible user accounts. A connection between DOWNAD, WALEDAC, and a FAKEAV has likewise been established with the WORM_DOWNAD.KK variant, making the equation more complex. Leveraging a Microsoft OS vulnerability and propagating via network shares, removable drives, and network drives, DOWNAD left an indelible mark in 2009.

Where Is DOWNAD Now?

The continuous work of the Conficker Working Group shows that while DOWNAD has left the headlines, the worm remains quite active in the sidelines. Based on available data as of January, there remains a considerable number of unique IP addresses connecting to the group's tracking systems in the first week of 2010 alone. Furthermore, a recent TrendLabs study shows that of around 100 million compromised IP addresses analyzed, 75 percent were identified as consumers while 25 percent were enterprise users. Since a single IP address can actually be connected to multiple machines, the figures used to create the graph below can possibly represent only a fraction of the entire infected population.

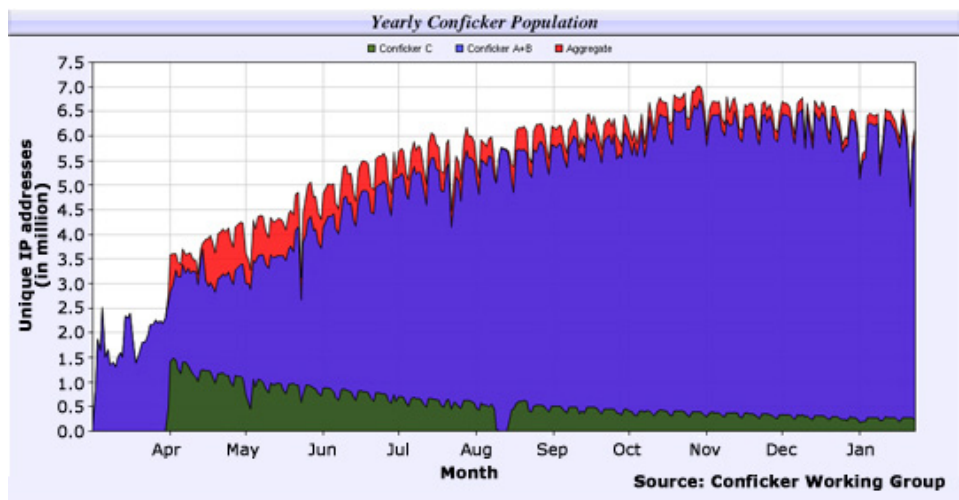


Figure 1. Number of unique IP addresses connected to the Conficker Working Group's tracking systems from April 2009 to January 2010

Furthermore, the report released by Akamai on the state of the Internet in the third quarter of 2009 reveals that there continues to be significant port 445 activity. While the port is not exclusively used by DOWNAD, high traffic in the said port has been one of the distinguishing marks of a DOWNAD infection. Furthermore, recent attack traffic shows that Russia and Brazil now account for 13 percent and 8.6 percent, respectively, of the traffic, as opposed to the United States (6.9 percent) and China (6.5 percent). If anything, these numbers show that while there has been a decline in the previous top 2 sources of attack traffic, the concentration of DOWNAD infections only moved to other parts of the globe.

Why Does the Threat Persist?

The DOWNAD network is a **very capable platform** where a code change could shift the balance of power. In 2009, DOWNAD variants made their appearance, each one with almost no similarity in terms of added registry entries. There has likewise been a consistent increase in the number of system changes triggered by each variant. These characteristics prodded security researchers to think that the creators of the worm have been working with a deliberate plan in mind.

It is also important to note that in several cases, all it took was one unpatched system for the worm to infect an entire network. Unfortunately, a significant number of unpatched systems remain even today, owing to the proliferation of pirated or unlicensed software and, in some cases, to inaction on the part of end users. It is thus highly probable that another massive infection can occur as when apparently as many as **9 million PCs were infected** in a span of only four months.

The same is true for the danger that removable drives pose. A **study** conducted as early as 2006 showed how an infected USB can easily start a network infection and a security compromise. Removable drives likewise made it to the list of **most abused infection vectors** in 2008 and continue to be **possible infection vectors** for the DOWNAD/Conficker worm.

What Can You Do?

The DOWNAD attack in 2009 has definitely set the stage for cybercriminal activities. Despite the hype that DOWNAD brought about, however, at its core, the attack was largely preventable. Trend Micro thus suggests that enterprises and individuals be proactive in battling the botnet by:

- **Identifying vulnerable machines and applying appropriate patches as soon as they are released.** Microsoft's [Windows Update page](#) provides administrators and users pertinent information on the latest patches available as well as helpful tips, especially for **enterprises**.
- Using authentic software and OSs to ensure continued protection that comes with legal licenses.
- **Utilizing strong passwords to prevent possible dictionary attacks on user accounts in networks.** Senior advanced threats researcher Robert McArdle recommends using three different passwords—one for public sites, another for laptops or desktops, and a distinct one for email accounts.
- **Protecting removable drives against worms using the AutoRun feature.** Senior advanced threats researcher Joey Costoya recommends **disabling the AutoPlay functionality** in Windows, which administrators could roll out to the entire network. Installing the patch effectively disables the AutoRun feature of all media except CD- and DVD-ROMs to prevent unwanted infections via removable drives.
- Monitoring port 445 activity, as this remains one of the more visible DOWNAD infection markers
- **Protecting systems by using a security solution that provides smarter protection against malicious files because DOWNAD is primarily a network worm.** Preventing access to compromised websites is likewise important, as peer-to-peer (P2P) sharing sites continue to be possible malware vectors.

To prevent another DOWNAD attack, users can:

- Identify vulnerable machines and apply appropriate patches as soon as they are released
- Use authentic software and OSs to ensure continued protection that comes with legal licenses
- Utilize strong passwords to prevent possible dictionary attacks on user accounts in networks
- Protect removable drives against worms using the AutoRun feature
- Monitor port 445 activity, as this remains one of the more visible DOWNAD infection markers
- Protect systems by using a security solution that provides smarter protection against malicious files because DOWNAD is primarily a network worm

References:

- Conficker Working Group. (April 1, 2009). *Conficker Working Group*. "Home Page." <http://www.confickerworkinggroup.org/wiki/pmwiki.php/Main/HomePage> (Retrieved March 2010).
- Conficker Working Group. (October 30, 2009). *Conficker Working Group*. "Infection Tracking." <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking> (Retrieved March 2010).
- Dan Raywood. (February 2, 2010). *SC Magazine*. "Greater Manchester Police Hit by Conficker from Infected USB That Leaves It Unconnected from Its Network for Three Days." <http://www.scmagazineuk.com/greater-manchester-police-hit-by-conficker-from-infected-usb-that-leaves-it-unconnected-from-its-network-for-three-days/article/162904/> (Retrieved March 2010).
- DarkReading. (June 7, 2006). *Security Dark Reading*. "Social Engineering, the USB Way." <http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634> (Retrieved March 2010).
- Det Caraig. (November 4, 2009). *TrendLabs Malware Blog*. "DOWNAD/Conficker Turns 1 Year." <http://blog.trendmicro.com/downadconficker-turns-1yr/> (Retrieved March 2010).
- Macky Cruz. (December 7, 2008). *TrendLabs Malware Blog*. "Most Abused Infection Vector." <http://blog.trendmicro.com/most-abused-infection-vector/> (Retrieved March 2010).
- Microsoft Corporation. (October 23, 2008). *Microsoft TechNet*. "Microsoft Security Bulletin MS08-067—Critical: Vulnerability in Server Service Could Allow Remote Code Execution (958644)." <http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp> (Retrieved March 2010).
- Microsoft Corporation. (January 6, 2010). *Microsoft Support*. "Update to the AutoPlay Functionality in Windows." <http://support.microsoft.com/kb/971029> (Retrieved March 2010).
- Microsoft Corporation. (2010). *Microsoft Windows Update*. "Options: Administrator Options." <http://www.update.microsoft.com/windowsupdate/v6/administrators.aspx?ln=en&lsMu=False> (Retrieved March 2010).
- Microsoft Corporation. (2010). *Microsoft Windows Update*. "Windows Update." <http://www.update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us> (Retrieved March 2010).
- Robert McArdle. (February 9, 2009). *TrendLabs Malware Blog*. "Largest Bulletin PHP Board Providers Compromised." <http://blog.trendmicro.com/largest-bulletin-php-board-providers-compromised/> (Retrieved March 2010).
- Sumner Lemon. (January 15, 2010). *PCWorld*. "Conficker Worm Hasn't Gone Away, Akamai Says." http://www.pcworld.com/article/186977/conficker_worm_hasnt_gone_away_akamai_says.html?tk=rss_news (Retrieved March 2010).
- Trend Micro. *Threat Encyclopedia*. "Threat Encyclopedia Search Results: WALEDAC." <http://threatinfo.trendmicro.com/vinfo/virusencyclo/default2.asp?m=q&virus=waledac&alt=waledac&Sect=SA> (Retrieved March 2010).

2009's Most Persistent Malware Threats

- Trend Micro. *Threat Encyclopedia*. "WORM_DOWNAD.KK." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOWNAD.KK (Retrieved March 2010).
- Trend Micro. (April 2, 2009). *TrendLabs Malware Blog*. "More DOWNAD/Conficker Questions After April 1st." <http://blog.trendmicro.com/more-downadconficker-questions-after-april-1st/> (Retrieved March 2010).

Senior advanced threats researcher Ryan Flores says SMBs are at risk (in terms of KOOBFACE) because they lack the resources needed for user education and security.

KOOBFACE SOCIAL NETWORK WORM

Since its first appearance in 2008, KOOBFACE remains the most prominent malware threat that successfully and continuously propagates via social networking sites. This may be juxtaposed to the growing popularity of social networking sites among home users as well as among companies and businesspeople. Nowadays, social networking sites do not only serve as a medium of communication but also as a marketing and networking tool.

According to senior advanced threats researcher Ryan Flores, small and medium-sized businesses (SMBs) are at risk because they lack the resources needed for user education and security. "The line between corporate network restrictions and personal use is being blurred by social networking sites. Employees can access social networking sites on corporate networks and may reveal confidential corporate information on their profile pages whether or not there are corporate restrictions. This poses risks for SMBs as they have limited IT staff to implement site restrictions and to conduct user education," he adds. With that, cybercriminals saw another avenue to further proliferate their malicious deeds.

Dissecting the Largest Web 2.0 Botnet

The KOOBFACE botnet comprises various component files, each with its own special function. These components include the KOOBFACE downloader, social network propagation components, the ad pusher and FAKEAV installer, the completely automated public Turing test to tell computers and humans apart (CAPTCHA) breaker, data stealer, Web search hijackers, and rogue domain name system changer, to name some. KOOBFACE's structure easily permits the addition of new and updated components.

Congratulations! You are on hidden camera!
;))

12:19 PM Aug 16th from web

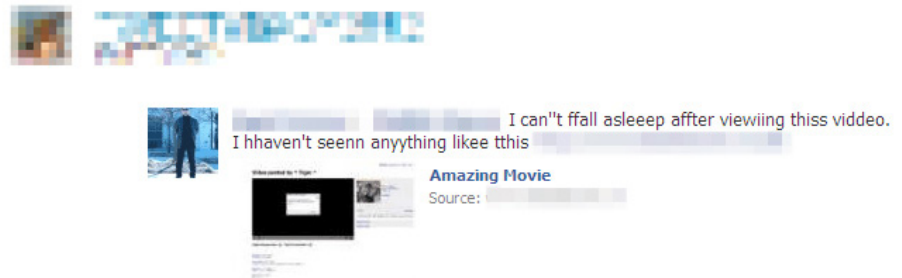


Figure 2. Sample KOOBFACE spam

Another notable KOOBFACE quality is its use of enhanced social engineering tactics. It capitalizes on the notion of trust between friends inside social networking sites and the trend of sharing links and statuses.

The KOOFACE infection chain begins with a spammed malicious link together with an enticing message. Once users click the link and install the KOOFACE loader component posing as a video codec, the affected system becomes part of the botnet. The affected users' social networking contacts are then spammed with malicious KOOFACE URLs. In addition, the affected system can be used as proxy to the botnet by installing its Web server component, which is responsible for *setup.exe* binaries and bogus *YouTube* and *Facebook* pages.

On the other hand, KOOFACE takes advantage of affected users to break CAPTCHAs. It does this by creating a false sense of panic on the users' part. Accordingly, the users must decipher the CAPTCHA image before the given time (3 minutes) expires or their systems will supposedly shut down. This tactic enabled KOOFACE to let affected users do the dirty work of breaking CAPTCHAs. As of October 2009, the **United States** posted the highest number of KOOFACE-infected systems.

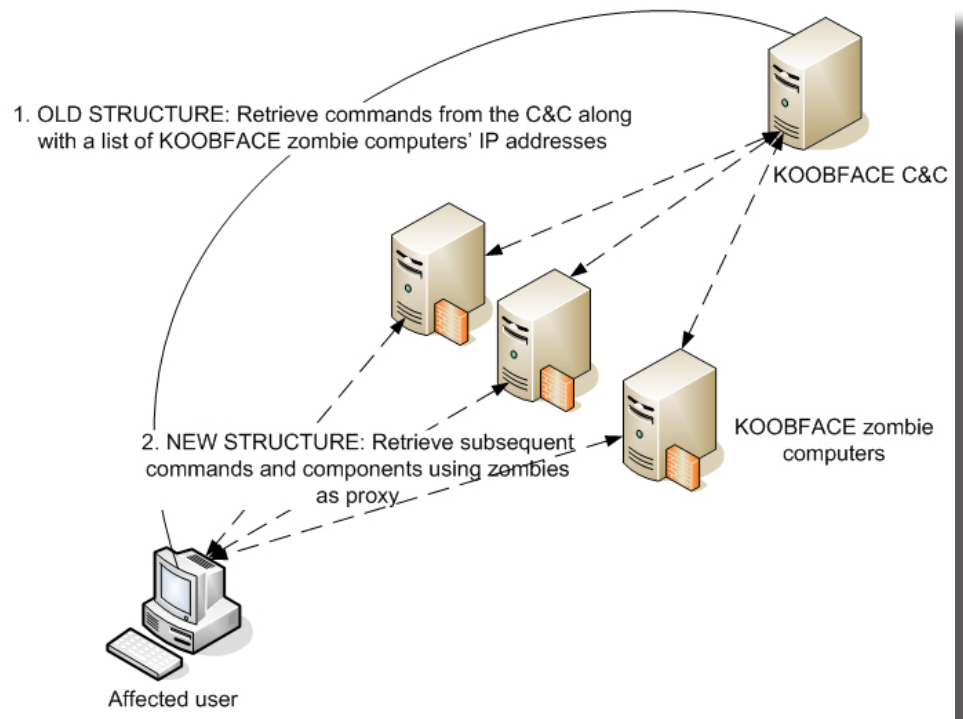


Figure 3. Command-and-control (C&C) architecture KOOFACE adapted after some domain takedowns

Why Does the Threat Persist?

Social networking sites boomed with the advent of Web 2.0. Entrepreneurs and SMBs embraced this phenomenon and used it as a tool to drive their business. Around 46 percent of the respondents of a **Facetime survey** perceived social networking sites crucial and of great value to a company or business. Clearly, social networking sites are no longer limited to just staying connected with friends.

▶ Around 46 percent of the respondents of a **Facetime survey** perceived social networking sites crucial and of great value to a company or business.

KOOBFACE's success, however, was not only a result of its robust malware architecture. The cybercriminals behind it are fully aware of social networking sites' efforts to enhance security and the current countermeasures and initiatives security researchers are coming up with. For instance, in July 2009, after some C&C domains were taken down, the KOOBFACE gang changed their botnet's architecture in such a way that the downloader component will not directly get commands from KOOBFACE C&C domains but do so from compromised websites acting as proxy C&C servers. This new structure made the botnet resilient to C&C domain takedowns.

When *Facebook* implemented a URL filtering service that blocked known spam URLs, KOOBFACE responded by updating its components with the creation of a GCHECK component. This component first tested if a certain malicious URL spammed by KOOBFACE has already been blocked or not. Along with the update, the KOOBFACE gang also sent a **message to Trend Micro security researchers** last Christmas, saying they read their research papers. Clearly, the cybercriminals behind the botnet stayed up-to-date with the latest news and researches on their malicious creation.

What Can You Do?

Given these facts, file detection alone cannot overcome a persistent threat like KOOBFACE. Users also need **multilayered protection** that breaks the infection chain by blocking spammed malicious URLs. This, in turn stops the execution of the downloader component (*setup.exe*) that eventually leads to the download of other KOOBFACE components.

According to senior advanced threats researcher Jonell Baltazar, threats that propagate via social networking sites like KOOBFACE can be mitigated with user education. "Without proper user education and understanding of current Web threats, especially in social networking sites, these will continue to act as attack vectors to enterprises and SMBs. Sufficient know-how will lead to better IT security policies and best practices for enterprises and SMBs' IT networks," he adds.

Trend Micro senior advanced threats researcher David Sancho also pointed out some useful best practices to stay secure from online threats while enjoying the benefits of social networking in the white paper, "**Security Guide to Social Networks.**"

References:

- David Sancho. (August 2009). *TrendWatch*. "Security Guide to Social Networks." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/security_guide_to_social_networks.pdf (Retrieved March 2010).
- Jonell Baltazar, Joey Costoya, and Ryan Flores. (July 2009). *TrendWatch*. "The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf (Retrieved March 2010).
- Robert McArdle. (December 31, 2009). *TrendLabs Malware Blog*. "From KOOBFACE with Love." <http://blog.trendmicro.com/from-koobface-with-love-2/> (Retrieved March 2010).
- Ryan Flores. (October 7, 2009). *TrendLabs Malware Blog*. "8 Things You Probably Didn't Know About KOOBFACE." <http://blog.trendmicro.com/8-things-you-probably-didn%E2%80%99t-know-about-koobface/> (Retrieved March 2010).

Senior advanced threats researcher Jonell Baltazar believes threats that propagate via social networking sites like KOOBFACE can be mitigated with user education.

2009's Most Persistent Malware Threats

- Sarah Perez. (July 2, 2009). *Read Write Web*. "A Growing Acceptance of Social Networking in the Workplace." http://www.readwriteweb.com/archives/a_growing_acceptance_of_social_networking_in_the_w.php (Retrieved March 2010).
- Wikimedia Foundation Inc. (March 10, 2010). *Wikipedia: The Free Encyclopedia*. "CAPTCHA." <http://en.wikipedia.org/wiki/CAPTCHA> (Retrieved March 2010).

ZEUS/ZBOT CRIMEWARE

Zeus Trojans are crimeware detected by Trend Micro as variants of the ZBOT family of malware. These Trojans typically arrive via spammed messages and steal information from infected systems. Once infected, systems become part of one of many networks of systems already compromised by Zeus Trojans. These botnets are controlled by cybercriminals for information theft for purposes of conducting wire fraud.

The Year That Was

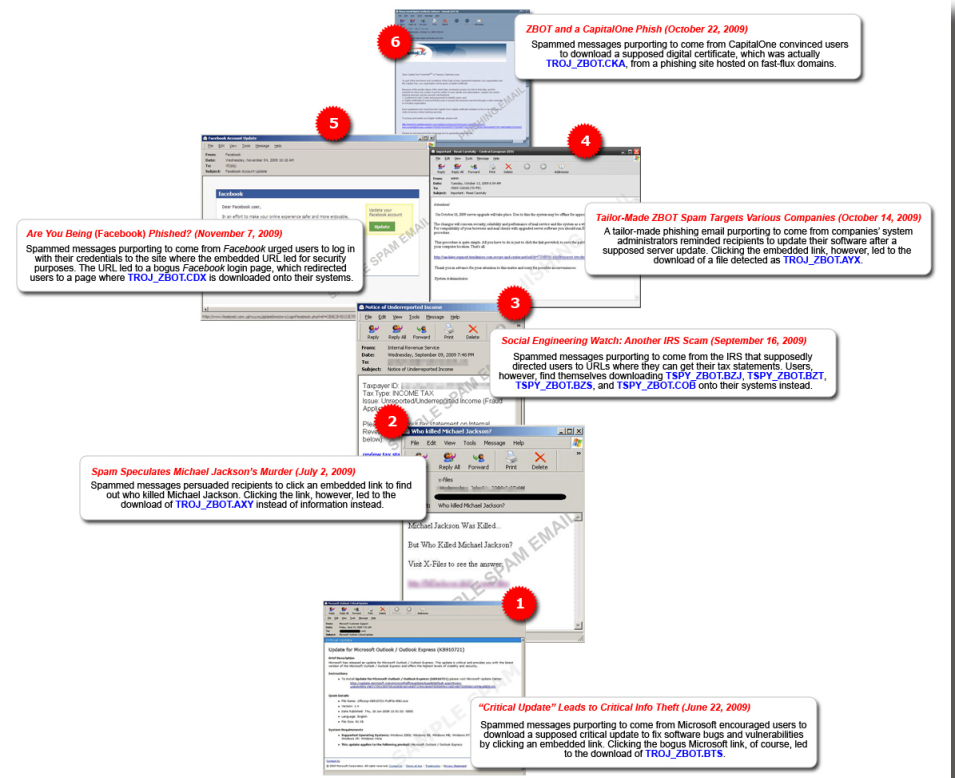


Figure 4. Six of the most notable ZBOT-related stories Trend Micro documented in 2009

By the third quarter of last year, Trend Micro already detected roughly 2,800 ZBOT variants and the number is still increasing.

By the third quarter of last year, Trend Micro already detected roughly 2,800 variants from this malware family and the number is still increasing! To date, we have recorded and distinguished eight ZBOT generations based on differences in their dropped copies, names of created folders, dropped file names, created mutexes, and URLs where a copy of itself and its components can be downloaded from.

ZeuS achieved notoriety due to the following reasons:

- File compression, which makes ZBOT variants difficult to analyze
- Rootkit capabilities, which allow ZBOT variants to hide themselves and their malicious routines from users
- Varying social engineering techniques that target a wide range of firms and organizations and use a variety of baits
- Effective business model that works
- Established network of money mules that act as the cyber-criminals' hands and feet above ground

Why Does the Threat Persist?

In the second half of 2009, Trend Micro prevented over 9 million infection attempts by ZBOT variants. However, these attacks continue to persist due to the following reasons:

- **File compression.** ZBOT variants are often compressed or packed usually with Ultimate Packer for eXecutables (UPX), a common type of compression software that is capable of encrypting actual .EXE application code. This, in effect, makes the application difficult to analyze. Earlier generations of ZBOT use UPX. However, variants from the new generation have been found to be compressed using other packers, if not unknown types, making the ordeal more difficult than it already is.
- **Rootkit capabilities.** ZBOT variants perform a number of stealth routines in order to hide themselves from users. They inject themselves into *SVCHOST.EXE* and *WINLOGON.EXE*, two of the many important Windows OS components that both run at startup and can have several instances running on a system at the same time. Since these are system files, they are not easily terminated using *Task Manager*. Another stealth tactic ZBOT variants employ is that they directly hook their functions to *NTOSKRNL.EXE*, another important Windows process. Hooking to this process allows them to hide all the files and folders they create from users' normal view.
- **Varying social engineering techniques.** It has been proven time and again that ZeuS has been using targeted, timely, and ever-changing social engineering ploys. From **banks** to **social networking sites** and **patch updates** to **news on pop stars**, ZeuS had it covered in 2009. Using diverse methods to bait users, the ZeuS botnet and the cybercriminals behind it only have three objectives in mind—to steal, to make money, and to steal some more.
- **Effective business model.** The organized cybercriminal group behind ZeuS uses a business model that ultimately works. Because of this, other groups of organized cybercriminals—professional and amateurs alike—use ZeuS to extort money from unknowing users.
- **Established network of money mules.** In line with organized cybercriminal activities, these underground groups have been found to have a network of money mules that act as their hands and feet above ground. Cybercriminals establish their mule networks by putting up bogus work-from home scams with innocent users having no way of knowing. What these mules do is move money from victims' accounts to the organized cybercriminals' accounts. Money mules basically shield cybercriminals from being identified, attributed, and eventually prosecuted for their malicious deeds. Most of the time, these mules take the fall for the real cybercriminals. Even worse, however, is the fact that these mules are not even aware that they are being used this way. Despite being dispensable, however, they are too important to cybercriminals that they would not be easily abandoned. We have reason to believe that these cybercriminals simply adjust their tactics and improve ZeuS to thwart off security companies and law enforcement agencies all together.

To protect systems from ZBOT infection via spam and phishing email messages, enterprises can:

- Keep their PCs and servers current with the latest software updates and patches
- Employ multilayered defense to secure PCs, servers, and networks
- Establish data protection policies and educate employees

What Can You Do?

To protect systems from the current and future ZeuS-related threats, Trend Micro advises users to remain vigilant and to regularly update applications. Downloading the *GeneriClean* tool ([TSC_GENCLEAN](#)), which rids systems of all TSPY_ZBOT variants, also helps. Enterprises can keep their networks safe by:

- **Keeping PCs and servers current with the latest software updates and patches.** Minimize exposure to vulnerabilities by applying the latest security updates and patches to software programs and OSs. Enable automatic updates, if possible.
- Employing multilayered defense to secure PCs, servers, and networks
 - Blocking threats at the gateway before they reach the network with a comprehensive security solution that includes URL filtering and cloud-based protection
 - Protecting endpoints—desktops, laptops, servers, and storage appliances—on and off the network
- Establishing data protection policies and educating employees
 - **Making sure employees are aware of spam and how they can help prevent these from spreading.** The following are some useful tips for employees:
 - **Always check who the email sender is.** If they know the people who sent the email message, check if they really did send the message. It will, however, be best to move suspicious-looking emails to spam inboxes.
 - **Carefully read through email messages.** Watch out for misspellings, grammatical lapses, and/or garbage characters in the message body. This is a good technique to practice, especially when a legitimate-looking email message from a company, regardless of popularity, ends up in their inboxes.
 - **Do not click embedded links.** Companies such as Microsoft will never send email messages that asks users to download digital certificates, to update their login credentials, or to install software into their systems. Make this a rule of thumb—go directly to the site's home page and log in or download from there.
 - **Check attachments' extension names.** Some email messages may contain compressed file attachments that appear harmless such as a *Microsoft Word* document file. Steer clear from attachments with double extension names and executable files in general.
 - Ensuring that employees never provide personal or confidential information in response to unsolicited email or IM requests

Non-Trend Micro product users can also stay protected from ZBOT infections with the aid of the following free tools:

- **Web Protection Add-On** is a lightweight add-on solution designed to proactively protect computers against Web threats and bot infiltration that can work alongside existing desktop protection solutions.
- **eMail ID** is a browser plug-in that helps identify legitimate email messages in users' inboxes. It helps users avoid opening and acting on phishing messages attempting to spoof real companies.

2009's Most Persistent Malware Threats

- *HouseCall* is Trend Micro's highly popular and capable on-demand scanner that identifies and removes viruses, Trojans, worms, unwanted browser plug-ins, and other malware.

References:

- Aljerro Gabon. (April 30, 2009). *TrendLabs Malware Blog*. "Invoice Spam Finds New Target: WorldPay." <http://blog.trendmicro.com/invoice-spam-finds-new-target-worldpay/> (Retrieved March 2010).
- Aljerro Gabon. (July 2, 2009). *TrendLabs Malware Blog*. "Spam Speculates Michael Jackson's Murder." <http://blog.trendmicro.com/spam-speculates-michael-jacksons-murder/> (Retrieved March 2010).
- Aljerro Gabon. (October 16, 2009). *TrendLabs Malware Blog*. "ZBOT Spam Campaign Continues." <http://blog.trendmicro.com/zbot-spam-campaign-continues/> (Retrieved March 2010).
- Argie Gallego. (June 22, 2009). *TrendLabs Malware Blog*. "'Critical Update' Leads to Critical Info Theft." <http://blog.trendmicro.com/critical-update-leads-to-critical-info-theft/> (Retrieved March 2010).
- Mary Bagtas. (May 12, 2009). *TrendLabs Malware Blog*. "Spoofed Western Union Mail Carries Info Stealer." <http://blog.trendmicro.com/spoofed-western-union-mail-carries-info-stealer/> (Retrieved March 2010).
- Roderick Ordoñez. (November 15, 2007). *TrendLabs Malware Blog*. "Storm Brews over Geocities." <http://blog.trendmicro.com/storm-brews-over-geocities/> (Retrieved March 2010).
- Trend Micro. (2010). *Threat Encyclopedia*. "TROJ_ZBOT.BJ." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_ZBOT.BJ (Retrieved March 2009).
- Verna Sagum. (November 7, 2009). *TrendLabs Malware Blog*. "Are You Being (Facebook) Phished?" <http://blog.trendmicro.com/are-you-being-facebook-phished/> (Retrieved March 2010).

▶ **FAKEAVs' prevalence has made them a familiar nuisance.**

ROGUE ANTIVIRUS APPLICATIONS

2009 saw the continued reign of FAKEAV with several new variants appearing every month. Their prevalence has made them a familiar nuisance, which may largely be due to their piggybacking on almost all known forms of malware delivery—from spam and fake codecs to poisoned search engine optimization (SEO) results and SQL injections.

Posting Date	Post Title	Infection Vector
January 5	Bogus <i>LinkedIn</i> Profiles Harbor Malicious Content	Malicious links in <i>LinkedIn</i>
February 6	Cybercrooks Handing Out Malware Flyers	Flyers and ads
March 2	Crack Sites Distribute VIRUX and FAKEAV	Accessing warez and crack sites
April 12	Rotten Eggs: An Easter Malware Campaign	SEO poisoning
April 14	The DOWNAD/Conficker Jigsaw Puzzle	Downloaded by other malware
May 11	Fake Antivirus Targets Brazil	Spam
June 4	Air France Flight 447 Search Results Lead to Rogue Antivirus	SEO poisoning
June 7	Reconfigure Your <i>Outlook</i> with Malware	Spam
June 24	Med Spam Litters <i>Silverlight</i> Forums	Malvertisements in <i>Silverlight</i> forums
June 25	Blackhat SEO Quick to Abuse Farrah Fawcett Death	SEO poisoning
July 23	"Solar Eclipse 2009 in America" Leads to FAKEAV	SEO poisoning
July 26	Rogue Antivirus Terminates .EXE Files	Ransomware
July 27	Malicious <i>Twitter</i> Posts Get More Personal	Malicious links in <i>Twitter</i>
August 3	Cory Aquino's Death Used to Spread Another FAKEAV	SEO poisoning
September 10	FAKEAV for 9/11	SEO poisoning
September 14	Bogus Profile in <i>LinkedIn</i> Leads to FAKEAV	Bogus <i>LinkedIn</i> profiles
September 15	Malvertisements in <i>NYTimes.com</i> Lead to FAKEAV	Malvertisements in <i>NYTimes.com</i>
September 17	Pick Your Poison: KOOBFACE or FAKEAV?	Malicious links in <i>Facebook</i>
September 22	Blackhat SEO and FAKEAV: A Dangerous Tandem	SEO poisoning
September 24	Bogus Sponsored Link Leads to FAKEAV	Sponsored links in <i>Bing</i> and <i>AltaVista</i>
September 28	Several Compromised Thai Sites Serve Malware	Compromised legitimate sites

2009's Most Persistent Malware Threats

Posting Date	Post Title	Infection Vector
September 29	Tropical Storm Leads to FAKEAV	SEO poisoning
October 21	FAKEAV Uses Conficker Worm as Bait	Spam
October 23	FAKEAV Goes Open Source... or Not?	Uses ClamAV components to appear legitimate
October 24	Spoofed Contract Carries Malware	Spam
October 28	Fake Facebook Password Notification Leads to Malware	Spam
November 16	Pacquiao Vs. Cotto Fight Live Stream Leads to FAKEAV	SEO poisoning
November 18	Meteor Shower and New Moon Lead to FAKEAV	SEO poisoning
November 19	Fake Blogs Lead to FAKEAV	SEO poisoning
December 21	News on Brittany Murphy's Death Lead to FAKEAV	SEO poisoning
December 24	PH: Mayon Volcano Eruption Spews Out SEO Attack	SEO poisoning
December 31	Malicious JavaScript Infects Websites	Injected code into PHP servers

Table 1. FAKEAV-related extortion scams documented in the TrendLabs Malware Blog in 2009



Figure 5. Behaviors FAKEAV variants normally exhibit

The most prominent FAKEAV attacks in 2008 made use of blue screens and misleading screensavers to incite fear among victims. However, this behavior has not been observed in 2009, as variants made more use of pop-up windows and balloon tray messages to urge users to buy bogus antivirus products. Such routines heavily relied on user panic to force users to shell out cash to rid their systems of supposed infections. FAKEAVs' legitimate look and feel add credibility to the malicious wares. Their behaviors varied per variant. Some acted as downloaders of more malware—other variants included—while some attempted to terminate security-related processes.

The main motive behind peddling FAKEAV basically remained the same though—for financial gain. A successful attack tricked users into purchasing rogue software but apart from losing money, perpetrators stole credit card credentials as well, which resulted in double gains for the FAKEAV creators.

▶ FAKEAVs' behaviors varied per variant but their main motive remained the same—to gain profit.

Why Does the Threat Persist?

FAKEAV variants usually exhibit similar routines, especially as they all lead to one thing—**profiting from user naivete**. However, cybercriminals used various and sometimes notable methods and social engineering techniques to lure users into installing the rogue software.

Whereas earlier generations of FAKEAV variants arrived via spam and drive-by downloads to trick users, the trend is now leaning toward poisoning search results. This can be considered a form of stealth attack, as the user is more likely to click a link returned by a trusted search engine. As such, appearing as a link in a search result makes the link appear harmless. The same logic applies to sites compromised to serve FAKEAV. There have been incidents where malvertisements on legitimate, even mainstream, high-traffic sites, led to FAKEAV.

FAKEAV variants in 2009 also rode on the popularity of social networking sites. Names of popular sites such as *Facebook*, *Twitter*, and *LinkedIn* were used in spammed messages to direct users to the download and installation of FAKEAV. The sites themselves were not excluded from becoming infection vectors. Spammed messages and fake profiles containing links that led to FAKEAV installations were also found circulating within the said social networking sites.

Arguably, FAKEAVs' greatest features include their ability to appear legitimate and to be the final payloads of spammed messages and links in social networking sites. Other routines observed in 2009 that added an authentic feel to notable FAKEAV attacks included the following:

- **Use of professional-looking interfaces.** Some variants even imitated the design of well-known legitimate antivirus software. They are also known for adopting professional-sounding names such as *Antivirus 2008*.
- **Use of standard Windows graphical user interface (GUI) elements.** These fool users into thinking that the messages they receive are official *Windows* error messages.
- **Use of professional-looking websites to accept payment.** FAKEAV variants likewise used professional-looking sites that contained ample information about the bogus products to accept payment. These used formal wording. Some even featured mock testimonials, displayed the “lock” symbol, and used the *https* prefix, essentially telling users they were “secure.”
- **Addition of actual files to users' systems.** Some variants added garbage files to supposed infected systems to further convince users of infections. Some even bundled legitimate antivirus software files with their FAKEAV applications.

Finally, as senior advanced threats researcher Feike Hacquebord says, “Selling FAKEAV is highly profitable for cybercriminal gangs. A lot of victims pay up to US\$100 for software that cannot detect real threats. FAKEAV affiliates and resellers receive extremely high provisions so this threat will not go away soon. Cybercriminal gangs that push FAKEAV are often also involved in other cybercrimes like large-scale click-fraud schemes and the spread of Trojans. They even have support departments that can be reached via phone and/or email though their main goal is not to serve FAKEAV customers but to create a façade for their business.”

▶ Senior advanced threats researcher Feike Hacquebord says, “Selling FAKEAV is highly profitable for cybercriminal gangs... so this threat will not go away soon.”

► Ultimately, enterprises are responsible for ensuring that their systems do not fall prey to FAKEAV attacks.

What Can You Do?

FAKEAV applications may look legitimate but none of their routines tell the actual truth about users' systems. They use fraudulent claims to scare users into believing their systems are infected. This is why some FAKEAV variants are classified as "scareware" or "ransomware" even though their routines are distinct enough to merit their own classification. FAKEAV variants constantly evolve to keep up with the latest trends, each time becoming more sophisticated.

Ultimately, enterprises are responsible for ensuring that their systems do not fall prey to FAKEAV attacks. They can do this by keeping the following best practices in mind:

- **Keep PCs and servers current with the latest software updates and patches.** Minimize exposure to vulnerabilities by applying the latest security updates and patches to software programs and OSs. Enable automatic updates, if possible.
- Employ multilayered defense to secure PCs, servers, and networks.
 - Block threats at the gateway before they reach the network with a comprehensive security solution that includes URL filtering and cloud-based protection.
 - Protect endpoints—desktops, laptops, servers, and storage appliances—on and off the network.

Do not panic when presented with warnings of system infection. Use an effective **security solution** to run a full system scan. In addition, it is not wise to purchase software that suddenly turn up in your machine. If in doubt, confirm the product's authenticity first. If your system does not have security software installed, you may use *HouseCall*, Trend Micro's highly popular and capable on-demand scanner for identifying and removing viruses, Trojans, worms, unwanted browser plug-ins, and other malware can also help. *eMail ID*, a browser plug-in, can also help protect systems by identifying legitimate email messages in users' inboxes. This helps users avoid opening and acting on phishing messages attempting to spoof real companies.

References:

- Ailene Dela Rosa. (June 7, 2009). *TrendLabs Malware Blog*. "Reconfigure Your Outlook with Malware." <http://blog.trendmicro.com/reconfigure-your-outlook-with-malware/> (Retrieved March 2010).
- Bernadette Irinco. (September 28, 2009). *TrendLabs Malware Blog*. "Several Compromised Thai Sites Serve Malware." <http://blog.trendmicro.com/several-compromised-thai-sites-serve-malware/> (Retrieved March 2010).
- Bernadette Irinco. (December 31, 2009). *TrendLabs Malware Blog*. "Malicious JavaScript Infects Websites." <http://blog.trendmicro.com/malicious-javascript-infects-websites/> (Retrieved March 2010).
- Brain Krebs. (March 24, 2010). *Krebs on Security: In-Depth Security News and Investigation*. "AV Profit: Rogue AV + Zeus = \$." <http://www.krebsonsecurity.com/2010/03/avprofit-rogue-av-zeus/> (Retrieved March 2010).
- David Sancho. (October 23, 2009). *TrendLabs Malware Blog*. "FAKEAV Goes Open Source... or Not?" <http://blog.trendmicro.com/fakeav-goes-open-source%E2%80%A6-or-not/> (Retrieved March 2010).

2009's Most Persistent Malware Threats

- Det Caraig. (August 3, 2009). *TrendLabs Malware Blog*. "Cory Aquino's Death Used to Spread Another FAKEAV." <http://blog.trendmicro.com/cory-aquino%E2%80%99s-death-used-to-spread-another-fakeav/> (Retrieved March 2010).
- Det Caraig. (December 21, 2009). *TrendLabs Malware Blog*. "News on Brittany Murphy's Death Lead to FAKEAV." <http://blog.trendmicro.com/news-on-brittany-murphy%E2%80%99s-death-lead-to-fakeav/> (Retrieved March 2010).
- Erika Mendoza. (July 26, 2009). *TrendLabs Malware Blog*. "Rogue Antivirus Terminates .EXE Files." <http://blog.trendmicro.com/rogue-antivirus-terminates-exe-files/> (Retrieved March 2010).
- Erika Mendoza. (September 24, 2009). *TrendLabs Malware Blog*. "Bogus Sponsored Link Leads to FAKEAV." <http://blog.trendmicro.com/bogus-sponsored-link-leads-to-fakeav/> (Retrieved March 2010).
- Erika Mendoza. (November 18, 2009). *TrendLabs Malware Blog*. "Meteor Shower and New Moon Lead to FAKEAV." <http://blog.trendmicro.com/meteor-shower-and-new-moon-lead-to-fakeav/> (Retrieved March 2010).
- Jake Soriano. (March 2, 2009). *TrendLabs Malware Blog*. "Crack Sites Distribute VIRUX and FAKEAV." <http://blog.trendmicro.com/crack-sites-distribute-virux-and-fakeav/> (Retrieved March 2010).
- Jake Soriano. (April 12, 2009). *TrendLabs Malware Blog*. "Rotten Eggs: An Easter Malware Campaign." <http://blog.trendmicro.com/rotten-eggs-an-easter-malware-campaign/> (Retrieved March 2010).
- Jessa De La Torre. (September 10, 2009). *TrendLabs Malware Blog*. "FAKEAV for 9/11." <http://blog.trendmicro.com/fakeav-for-september-11/> (Retrieved March 2010).
- Jessa De La Torre. (September 22, 2009). *TrendLabs Malware Blog*. "Blackhat SEO and FAKEAV: A Dangerous Tandem." <http://blog.trendmicro.com/blackhat-seo-and-fakeav-a-dangerous-tandem/> (Retrieved March 2010).
- Jessa De La Torre. (September 29, 2009). *TrendLabs Malware Blog*. "Tropical Storm Leads to FAKEAV." <http://blog.trendmicro.com/tropical-storm-leads-to-fakeav/> (Retrieved March 2010).
- Jessa De La Torre. (November 16, 2009). *TrendLabs Malware Blog*. "Pacquiao Vs. Cotto Fight Live Stream Leads to FAKEAV." <http://blog.trendmicro.com/pacquiao-cotto-fight-live-stream-leads-to-fakeav/> (Retrieved March 2010).
- JM Hipolito. (February 6, 2009). *TrendLabs Malware Blog*. "Cybercrooks Handing Out Malware Flyers." <http://blog.trendmicro.com/cybercrooks-handing-out-malware-flyers/> (Retrieved March 2010).
- JM Hipolito. (June 4, 2009). *TrendLabs Malware Blog*. "Air France Flight 447 Search Results Lead to Rogue Antivirus." <http://blog.trendmicro.com/search-results-for-air-france-flight-447-lead-to-rogue-antivirus/> (Retrieved March 2010).
- JM Hipolito. (July 27, 2009). *TrendLabs Malware Blog*. "Malicious Twitter Posts Get More Personal." <http://blog.trendmicro.com/malicious-twitter-posts-get-more-personal/> (Retrieved March 2010).
- JM Hipolito. (September 15, 2009). *TrendLabs Malware Blog*. "Malvertisements in NYTimes.com Lead to FAKEAV." <http://blog.trendmicro.com/malvertisements-in-nytimes-com-lead-to-fakeav/> (Retrieved March 2010).

2009's Most Persistent Malware Threats

- Jonathan Leopando. (November 19, 2009). *TrendLabs Malware Blog*. "Fake Blogs Lead to FAKEAV." <http://blog.trendmicro.com/fake-blogs-lead-to-fakeav/> (Retrieved March 2010).
- Jonell Baltazar. (September 17, 2009). *TrendLabs Malware Blog*. "Pick Your Poison: KOOFACE or FAKEAV?" <http://blog.trendmicro.com/pick-your-poison-koobface-or-fakeav/> (Retrieved March 2010).
- Joseph Pacamarra. (December 24, 2009). *TrendLabs Malware Blog*. "PH: Mayon Volcano Eruption Spews Out SEO Attack." <http://blog.trendmicro.com/ph-mayon-volcano-eruption-spews-out-seo-attack/> (Retrieved March 2010).
- Macky Cruz. (January 5, 2009). *TrendLabs Malware Blog*. "Bogus LinkedIn Profiles Harbor Malicious Content." <http://blog.trendmicro.com/bogus-linkedin-profiles-harbor-malicious-content/> (Retrieved March 2010).
- Macky Cruz. (June 25, 2009). *TrendLabs Malware Blog*. "Blackhat SEO Quick to Abuse Farrah Fawcett Death." <http://blog.trendmicro.com/blackhat-seo-quick-to-abuse-farah-fawcett-death/> (Retrieved March 2010).
- Macky Cruz. (September 14, 2009). *TrendLabs Malware Blog*. "Bogus Profile in LinkedIn Leads to FAKEAV." <http://blog.trendmicro.com/bogus-profile-in-linkedin-leads-to-fakeav/> (Retrieved March 2010).
- Maria Alarcon. (October 28, 2009). *TrendLabs Malware Blog*. "Fake Facebook Password Notification Leads to Malware." <http://blog.trendmicro.com/fake-facebook-password-notification-leads-to-malware/> (Retrieved March 2010).
- Maydalene Salvador. (October 24, 2009). *TrendLabs Malware Blog*. "Spoofed Contract Carries Malware." <http://blog.trendmicro.com/spoofed-contract-carries-malware/> (Retrieved March 2010).
- Paul Ferguson and Ivan Macalintal. (April 14, 2009). *TrendLabs Malware Blog*. "The DOWNAD/Conficker Jigsaw Puzzle." <http://blog.trendmicro.com/the-downadconficker-jigsaw-puzzle/> (Retrieved March 2010).
- Robby Dapiosen. (October 21, 2009). *TrendLabs Malware Blog*. "FAKEAV Uses Conficker Worm as Bait." <http://blog.trendmicro.com/fakeav-uses-conficker-worm-as-bait/> (Retrieved March 2010).
- Roderick Ordoñez. (May 11, 2009). *TrendLabs Malware Blog*. "Fake Antivirus Targets Brazil." <http://blog.trendmicro.com/fake-antivirus-targets-brazil/> (Retrieved March 2010).
- Roland Dela Paz. (July 23, 2009). *TrendLabs Malware Blog*. "'Solar Eclipse 2009 in America' Leads to FAKEAV." <http://blog.trendmicro.com/solar-eclipse-2009-in-america-leads-to-fakeav/> (Retrieved March 2010).
- Ryan Flores. (June 24, 2009). *TrendLabs Malware Blog*. "Med Spam Litters Silverlight Forums." <http://blog.trendmicro.com/med-spam-litters-silverlight-forums/> (Retrieved March 2010).
- Wikimedia Foundation Inc. (March 11, 2010). *Wikipedia*. "Sandbox." http://en.wikipedia.org/wiki/Sandbox_%28computer_security%29 (Retrieved March 2010).

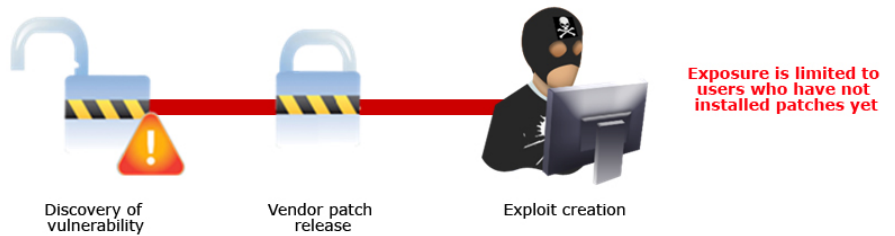
► All software has vulnerabilities, some are just more likely to be exploited than others.

ZERO-DAY EXPLOITS

All software has vulnerabilities though some are more likely to be exploited than others. Cybercriminals usually target unpatched or unreported vulnerabilities that can affect a larger number of systems. While there were several zero-day exploits in 2009, the most notable ones targeted *IE* and *Adobe Acrobat*.

IE Zero-Day Exploits

TYPICAL EXPLOIT SCENARIO



ZERO-DAY ATTACKS

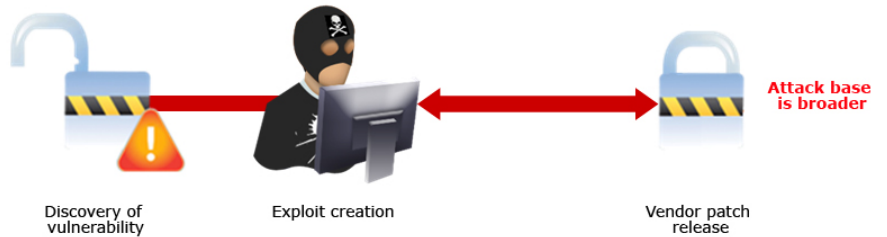


Figure 6. Typical exploit scenario and zero-day attacks

- In February, a **critical vulnerability in IE 7** arose from the browser's improper handling of errors, which allowed remote attackers to execute arbitrary code on affected systems. A spammed malicious .DOC file containing an ActiveX object automatically accessed a site rigged with a malicious .HTML file. This file exploited the **CVE-2009-0075** vulnerability, which downloaded a backdoor detected as **BKDR_AGENT.XZMS**, which then installed a .DLL file that had information-stealing capabilities.



Figure 7. Sample IE zero-day exploit infection chain

► Acrobat and Reader were two of cybercriminals' favorite Adobe software vulnerability targets in 2009.

- In July, Microsoft pushed several out-of-band patches for *IE* out in relation to a zero-day exploit revealed earlier in the month. It appeared that the underlying vulnerability was not fixed when independent security researchers discovered the flaw. Microsoft, however, preempted the exploitation of the possible issue by taking the highly unusual step of releasing an out-of-band patch.

Adobe Zero-Day Exploits

- In February, specially crafted .PDF files were found to cause system crashes that originated from *Adobe Reader 9.1* and *Acrobat 9.1* but not before they dropped malicious files onto affected systems. The exact malware dropped varied but could include backdoors and other software exploits. These spread the same way normal .PDF files were distributed, either as email attachments or downloaded from websites.
- In April, a *Adobe Acrobat* and *Reader getIcon()* vulnerability was exploited. *Adobe Reader* and *Acrobat 9.1* and *7.1.1* updates resolved this issue, which turned out to be an input validation issue in a JavaScript method that could potentially lead to remote code execution.
- In July, a vulnerability was discovered in *Adobe Reader 9.1.2* and *Flash Player 9* and *10*. The exploits used a technique known as heap spraying. Once a user opened a specially crafted .PDF file, two executable binaries were dropped and executed on their systems.
- In December, a vulnerability in *Adobe Reader* and *Acrobat 9.2* was exploited. This vulnerability (CVE-2009-4324) could cause a system to crash and potentially allow an attacker to take control of an affected system. A patch was subsequently released a month after.

Other Microsoft Zero-Day Vulnerabilities

- In May, a vulnerability in *Microsoft PowerPoint* was discovered, which could allow remote code execution if users opened a specially crafted .PPT file.
- In June, vulnerabilities were discovered in *Microsoft Internet Information Services (IIS)*, which could allow elevation of privilege. Notably, *Microsoft IIS* was again issued a patch for a separate vulnerability (MS09-053) in October.
- October also saw the release of a patch for a zero-day vulnerability in *Server Message Block Version 2 (SMBv2)*. The most severe of the vulnerabilities could allow remote code execution if an attacker sent a specially crafted Server Message Block packet to a computer running the *Server* service.
- One month after its release in October 2009, a zero-day vulnerability was also reported for Microsoft's latest OS, *Windows 7*. The said vulnerability could be used by an attacker to remotely crash infected computers.

▶ Given Adobe and Microsoft's popularity, exploiting zero-day vulnerabilities in their applications has the ability to affect a very large user base.

Why Does the Threat Persist?

Given Adobe and Microsoft's popularity, exploiting zero-day vulnerabilities in their applications has the potential to affect a very large user base, especially since some of their most popular applications are cross-platform. Exploiting a vulnerability in very popular applications required minimal user interaction (e.g., clicking a link). Systems can remain vulnerable years after a patch is released because it was never applied. Zero-day vulnerabilities also attracted cybercriminals because they could take advantage of these and exploit a large number of systems before vendors could release patches.

Trend Micro researcher, Rajiv Motwani, also outlined the following reasons why software vulnerabilities continue to persist:

- **Nonavailability of a centralized automatic update system for all applications installed on a computer.** Many applications are not patched given the fact that the main objective of each common user is to efficiently use his/her computer and not to protect it. Patching systems is ideally a full-time job in every organization and some people should be dedicated for that purpose.
- **Each vendor has its own patch release cycle.** The amount of time it takes to patch a vulnerability also varies from organization to organization. Hence, it is possible that vendors know that vulnerabilities exist in their software for months or years before they are actually patched. All the while, systems with these software remain vulnerable to threats.
- **Patches require a lot of testing in terms of performance, stability, and compatibility before they can be rolled out in a phased manner.** Hence, patching is likely to be delayed given the possible impact these may have. In addition, on critical servers, restarting a server once a patch is installed may also become an issue.
- **Use of legacy software even after their end of life.** Upgrading software is risky and requires a major investment. As such, enterprises just accept rather than mitigate or compensate for risks.
- **Lack of information about updates.** Several software do not issue update notifications. Unless customers go to vendors' websites, they will not know about newer versions, which could have fixes for several vulnerabilities.
- **Lack of user knowledge about the criticality of vulnerabilities or potential exploit outcomes.** Customers are usually unaware of the impact of not patching their systems. User machines become part of botnets without their knowledge. In this regard, user training is necessary.
- **Perception that traditional antivirus software protects against all kinds of threat.** This perception is pretty common but an antivirus solution is only part of a security solution.
- **Availability of malicious patches.** If users have been tricked into applying a malicious patch before, they may be hesitant to patch their systems again. It becomes a trust issue—who can users trust and who can they not?

To prevent system vulnerabilities from being exploited, users can:

- Use updated versions of installed security products
- Educate users to be careful of links, files, and data on social networking sites and IMs
- Educate users to be careful of specially crafted attachments to unsolicited email messages
- Verify the senders of suspicious-looking email messages
- Check the legitimacy of links

What Can You Do?

To prevent system vulnerabilities from being exploited, users can do the following:

- **Use updated versions of installed security products.** Ensure that all definitions are up-to-date at all times. As much as possible, keep software updated with the latest patches. Users should also stay up-to-date with the latest news regarding the applications installed in their systems.
- **Educate users to be careful with links, files, and data on social networking sites and instant messages (IMs).** A lot of exploits affect systems via malicious links that lurk in social networking sites and IMs.
- **Educate users to be careful of specially crafted attachments to unsolicited email messages.** Likewise, browser exploits may be activated through malicious links that lurk in the Web via blackhat SEO or embedded in spammed messages.
 - If an email messages seems suspicious, verify if the sender really did send an it with an attachment.
 - Links can also be checked by inspecting the browser's status bar. Note, however, that some links can be hidden. As a general rule, try to avoid links presented by suspicious-looking websites.

Business users can protect themselves from vulnerability exploits by using *Trend Micro Deep Security* and *OfficeScan* with the *Intrusion Defense Firewall (IDF)* plug-in. Home users who do not have security solutions installed can also avail of free tools like *Web Protection Add-On*, which can minimize the occurrence of exploits by blocking access to sites that host malicious exploits, and *eMail ID*, which helps users determine the trustworthiness of the messages they receive via email.

References:

- Ailene Dela Rosa. (May 14, 2009). *TrendLabs Malware Blog*. "CVE-2009-0556 Vulnerability Patched." <http://blog.trendmicro.com/cve-2009-0556-vulnerability-patched/> (Retrieved March 2010).
- CVE. "CVE-2009-0075." <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0075> (Retrieved March 2010).
- Det Caraig. (June 9, 2009). *TrendLabs Malware Blog*. "June 2009 Microsoft and Adobe Security Updates." <http://blog.trendmicro.com/june-2009-microsoft-and-adobe-security-updates/> (Retrieved March 2010).
- Jake Soriano. (February 17, 2009). *TrendLabs Malware Blog*. "Another Exploit Targets IE 7 Bug." <http://blog.trendmicro.com/another-exploit-targets-ie7-bug/> (Retrieved March 2010).
- Jessa De La Torre. (July 24, 2009). *TrendLabs Malware Blog*. "Another Day, a New Zero-Day Exploit for Adobe." <http://blog.trendmicro.com/another-day-a-new-zero-day-exploit-for-adobe/> (Retrieved March 2010).
- JJ Reyes. (April 9, 2009). *TrendLabs Malware Blog*. "Adobe Acrobat/Reader getIcon() Vuln Exploit in the Wild." <http://blog.trendmicro.com/adobe-acrobatreader-geticon-vuln-exploit-in-the-wild/> (Retrieved March 2010).

2009's Most Persistent Malware Threats

- JM Hipolito. (October 14, 2009). *TrendLabs Malware Blog*. "October Patch Tuesday: MS Releases 13 Security Updates." <http://blog.trendmicro.com/microsoft-releases-13-security-updates-for-october-patch-tuesday/> (Retrieved March 2010).
- Jonathan Leopando. (February 20, 2010). *TrendLabs Malware Blog*. "Portable Document Format or Portable Malware Format?" <http://blog.trendmicro.com/portable-document-format-or-portable-malware-format/> (Retrieved March 2010).
- Jonathan Leopando. (November 12, 2009). *TrendLabs Malware Blog*. "New SMB Zero-Day Exploit?" <http://blog.trendmicro.com/new-smb-zero-day-exploit/> (Retrieved March 2010).
- Roland Dela Paz. (December 16, 2009). *TrendLabs Malware Blog*. "New Adobe Zero-Day Vulnerability Again." <http://blog.trendmicro.com/new-adobe-zero-day-vulnerability-again/> (Retrieved March 2010).
- Trend Micro. (2010). *Threat Encyclopedia*. "BKDR_AGENT.XZMS." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?vname=BKDR_AGENT.XZMS (Retrieved March 2010).

POSTSCRIPT

Several other major attacks in 2009 deserve attention, including the yearlong and still ongoing infestation of compromised websites that redirect to malicious domains. Companies need to study all their external portals and to perform vulnerability testing for any interactive website to avoid SQL injections or cross-site scripting (XSS) attacks. In addition, given that the persistence of one of the more notable mass compromises dubbed as “Gumblar” was due to the use of stolen File Transfer Protocol (FTP) credentials to infiltrate a website’s back end, companies need to require and implement a strict password-creation and -renewal policy for all portals. In fact, companies should reconsider using FTP because network snooping and Domain Name System (DNS) and Address Resolution Protocol (ARP) exploits can easily capture FTP-related user credentials even when both the client and server are not compromised.

The persistent threats outlined in this report all arrive via different infection vectors—unpatched vulnerabilities, unsolicited email messages, and malicious URLs—wherein by the time a binary related to a cybercriminal attack is detected, it is often already too late. In the end, a single-pronged protection strategy is no longer reasonable. Large enterprises and SMBs should trace all possible entry points of malware attacks and data breaches and install equivalent safeguards, monitoring systems, and security software to cover as many bases as possible from the gateway down to the various endpoint devices and systems.

Trend Micro™ Smart Protection Network™ infrastructure delivers security that is smarter than conventional approaches. Leveraged across Trend Micro’s solutions and services, Smart Protection Network is a cloud-client content security infrastructure that automatically blocks threats before they reach you. A global network of threat intelligence sensors correlates with email, Web, and file reputation technologies 24 x 7 to provide comprehensive protection against threats. As the sophistication of threats, volume of attacks, and number of endpoints rapidly grow, the need for lightweight, comprehensive, and immediate threat intelligence in the cloud is critical to overall protection against data breaches, damage to business reputation, and loss of productivity. The following free tools also help protect computers from these threats:

- **eMail ID:** This browser plug-in helps users identify legitimate email messages in their inboxes. It uses a two-step check to verify the authenticity of messages from hundreds of major companies then displays results in the “from” area so that users will know what is real. This helps them avoid opening and acting on phishing messages attempting to spoof real companies.
- **HiJackThis:** This generates an in-depth report of registry and file settings from users’ computers. It does not separate safe from unsafe settings in its scan results, giving users the ability to selectively remove items from their machines. In addition to its scan-and-remove capability, it also comes with several useful tools to manually remove malware from infected computers.
- **HouseCall:** This is a capable on-demand scanner users can use to identify and remove viruses, Trojans, worms, unwanted browser plug-ins, and other malware from affected systems.
- **Web Protection Add-On:** This is a lightweight add-on solution that can work alongside users’ existing desktop protection. It was designed to proactively protect computers against Web threats and bot infiltration.

REFERENCES

- Elinor Mills. (January 25, 2010). *cnet news*. "Survey: Data Breaches from Malicious Attacks Doubled Last Year." http://news.cnet.com/8301-27080_3-10440220-245.html?part=rss&subj=news&tag=2547-1_3-0-20 (Retrieved March 2010).
- Frank Gens. (January 5, 2010). *IDC eXchange*. "IDC Survey: What IT Is Likely to Move to the Cloud?" <http://blogs.idc.com/ie/?p=843> (Retrieved March 2010).
- iPass Inc. (2010). "The iPass Mobile Workforce Report: Understanding Enterprise Mobility Trends and Mobile Usage." <http://www3.ipass.com/wp-content/uploads/2010/02/Mobile-Workforce-Report-22510.pdf> (Retrieved March 2010).
- Jon Brodtkin. (January 7, 2010). *NetworkWorld*. "Facebook, Twitter Becoming Business Tools, but CIOs Remain Wary." <http://www.networkworld.com/news/2010/010710-facebook-twitter-business-tools.html> (Retrieved March 2010).
- Tim Wilson. (September 11, 2007). *Security Dark Reading*. "Annual CSI Study: Cost of Cybercrime Is Skyrocketing." <http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208804727> (Retrieved March 2010).

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651

Phone: 1 +408.257.1500

Fax: 1 +408.257.2003

www.trendmicro.com

