

2010 THREATS: THE GOOD, THE BAD, AND THE UGLY

The past couple of years revealed a lot of technological advancements that significantly changed the way we live and do business today. Although most of them have already been out there for quite some time now, they are just becoming widely accepted and are fast becoming standards in today's world. As users and industries increasingly adopt new technologies, however, so do cybercriminals. While they continued to plague the Internet with malicious codes, they also found toolkits that enabled even the most novice of users to create malware and to profit off malicious schemes, earning 2010 the title, "The Year of the Toolkit."

2009 in Retrospect

In 2009, we saw cybercriminals make use of old and new online platforms to successfully spread malware to target users. Several high-profile malware threats were identified to have had recurrent themes, allowing them to be **considered the most persistent in 2009.**

True to this title, these threats were present all year long, proving to be a tough challenge for consumers and enterprises alike.

While these threats were not new, a number of new innovations were developed within them in an attempt to trump whatever security advances have been made to overcome them. For instance, KOOFACE upgraded its structure to become more resilient to command-and-control (C&C) domain takedowns after its C&C domains were taken down in July 2009. It also updated its components to make sure that the malicious URLs they spammed would not be blocked by *Facebook's* URL-filtering services.

Likewise, ZeuS/ZBOT continued to persist in 2009 due to a number of factors, the most notable of which was its effective business model and established network of money mules that other cybercriminal groups continued to rely on. And, of course, who could forget DOWNAD/Conficker and FAKEAV, which have been in the malware scene since 2008? While these threats seemed to have settled down quite a bit in 2009, they remained active in the sidelines and continued to have a fairly huge impact on users in 2010.

While cybercriminals continued to plague the Internet with malicious codes, they also found toolkits that enabled even the most novice of users to create malware and to profit off malicious schemes, earning 2010 the title, "The Year of the Toolkit."



The Good

Compared with the major attacks that took place in 2009, not many differences can be derived from 2010's attacks. However, 2009's threats proved to be key indicators of what came about in 2010.

Fortunately, Trend Micro experts anticipated and discussed these in "The Future of Threats and Threat Technologies: How the Landscape Is Changing," which was released to forewarn and arm users with knowledge of the threats that may be expected in 2010. The predictions that materialized in 2010, based on the predictions made, will be discussed in the following sections.

Global outbreaks will become extinct and localized, targeted attacks will grow.

As early as the first half of 2010, several targeted attacks were already reported by independent researchers. About 34 companies were suspected to have become victims of what were described as "highly sophisticated and targeted attacks."

Customized attacks also became widespread, as certain malware tried to target multiple but specific computing platforms. More and more, cybercriminals made browser and OS detection part of their standard attacks, allowing them to specify the payloads that would run on each target platform.



• About 34 companies were suspected to have become victims of what were described as "highly sophisticated and targeted attacks."

Undoubtedly, STUXNET was the most notable and talked-about highly targeted threat in 2010. This worm specifically targeted Siemens supervisory control and data acquisition (SCADA) WinCC systems, which were used to manage the industrial operation of power plants and energy refineries. Using multiple components with different functionality, efficient system vulnerability exploits, and a very effective propagation mechanism, this worm was without a doubt a complex malware worth the attention that it received from the media and the whole IT security industry. Although this threat was limited to critical systems, it should serve as a warning to all users and enterprises, big or small, to secure their systems at all times.

Drive-by infections will be the norm—one Web visit is enough to get infected.

Compromised websites were quite prolific in 2010. In June 2010, about 100,000 websites were compromised, including major news sites, *The Wall Street Journal* and *Jerusalem Post*. Users who visited the infected sites were affected by data stealers that targeted online games.

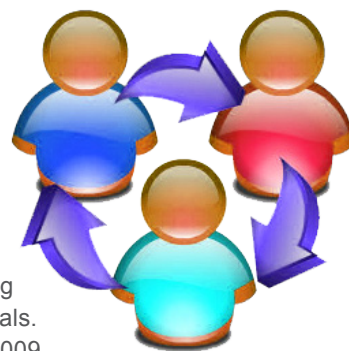


The other websites that were hacked to deliver malware to unsuspecting users were *The Nobel Peace Prize* and a number of *WordPress* blogs, among others. TrendLabsSM estimated that about 1,000 new websites were compromised every day, some of which have been repeatedly compromised in the past.

Zero-day vulnerabilities also posed serious problems in 2010. Most of the exploits were delivered via “drive-by” attacks wherein all that was necessary to become infected was to visit a website.

Company/Social networks will continue to be shaken by data breaches.

Social networking sites continued to be a source of threats throughout 2010. Vulnerabilities in social media platforms were also exploited by attackers in order to perform malicious activities. *Twitter* and *Facebook* were the main platforms cybercriminals targeted in 2010 due to their ever-growing popularity and number of users.



For *Facebook*, being the most popular social networking site also meant being the most targeted by cybercriminals. While various *Facebook*-related attacks were seen in 2009, targeting the site became a key trend in 2010, as several threats targeted its users month after month. In May 2010, *KOOBFACE*, the first social network worm to succeed in terms of operation, made a comeback with more tricks up its sleeves.

Cybercriminals also upped the ante for *Twitter*-related threats by ramping up their campaigns and getting more personal in their attacks. In June 2010, TrendLabs security researchers found backdoor programs proliferating through the site via Tweets written in Arabic. Riding on the popularity of *Twitter*, users of one of its most widely used applications, *TweetDeck*, became the target of a supposed update. A botnet targeting Latin American users also used *Twitter* for its C&C mechanism.

According to the Identity Theft Resource Center (ITRC), the number of data breaches in 2010 exceeded the previous year's with a reported 662 in December from 498 in 2009. The business sector accounted for the largest number of incidents at 279, followed by the medical/healthcare (160) and government and military (104) sectors.

Bots cannot be stopped anymore and will be around forever.

While certain old botnets refused to fade away and as efforts to take them down escalated, security experts continued to discover new botnets in 2010. One of them was the *Mehika Twitter* botnet that used *Twitter* to send out commands to zombies. It was one of the many Mexican botnets that plagued Latin American users throughout 2010.



According to the ITRC, the number of data breaches in 2010 exceeded the previous year's with a reported 662 in December from 498 in 2009.

The Azvhan bot family, which mostly **affected users in Asia**, also emerged. Discovered in April 2010, this botnet did not differ much from others in that it could execute various commands received from its C&C servers and steal information from affected users.

Similarly, the SpyEye botnet **was also revealed earlier in 2010**. Like ZeuS/ZBOT, this malware family consists of information stealers, the main difference being the fact that it prevents ZeuS malware from running on infected systems. Its server also **served two other botnets**—URLZone and Spencerlor. All three botnets were designed to steal user credentials for German banks.

Mobile threats will have more impact.

Throughout the years, mobile threats played a very minor role in unleashing malware badness from cybercriminals. This changed in 2010, as the emergence of more sophisticated threats targeting mobile devices were observed.

As the mobile OS landscape evolved and became more Web based and as the number of smartphone users **continued to rapidly increase**, mobile devices became a more common cybercrime target.



As the mobile OS landscape evolved and became more Web based and as the number of smartphone users continued to rapidly increase, mobile devices became a more common cybercrime target.

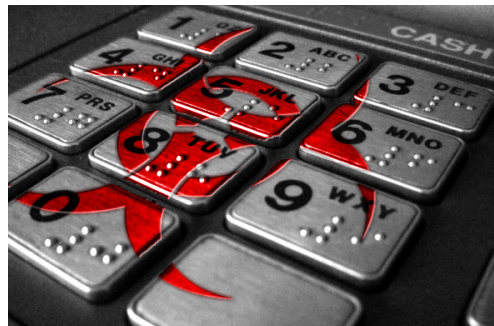
2010 marked the discovery of the first *Android OS* Trojan. Detected as **ANDROIDOS_DROIDSMS.A**, this malware affected *Android OS*-based smartphones. It came disguised as *Windows Media Player* and attempted to send text messages to premium mobile numbers. This was shortly followed by another mobile threat, which **came in the form of an *Android OS* app** known as *Tap Snake*. This malicious app had the ability to send a user's GPS location to a remote user. This allowed the remote user to monitor the whereabouts of an affected user through another application known as *GPS SPY*.

iPhone and *iPod* devices were, of course, not safe from threats as well. An app known as *JailbreakMe* **exploited specific vulnerabilities** in *Adobe Reader* and how the devices handled *IOSurface* properties that resulted in an integer overflow. Users who downloaded this app using *Mobile Safari* were actually tricked into downloading a malicious .PDF file detected as **TROJ_PIDIEF.HLA**.

Threats targeting new mobile OSs may have started to become rampant but let's not forget that older *Symbian OS* phones still dominated the worldwide smartphone sales and so **remained a favorite cybercrime target**. In July 2010, a new *Symbian* malware was discovered, which arbitrarily sent a text message to a premium number, causing affected users to incur charges for messages they never sent. The other common threats that only used to plague PC users such as text spam and text scams also **became mainstream for mobile devices**.

Cybercriminals will formulate more direct and brazen extortion tactics to obtain quicker access to cash.

Where else can one get easier and quicker access to cash than from an ATM? Cybercriminals know this and it is for this reason that ATMs **have become high-profile cybercrime targets** in 2010.

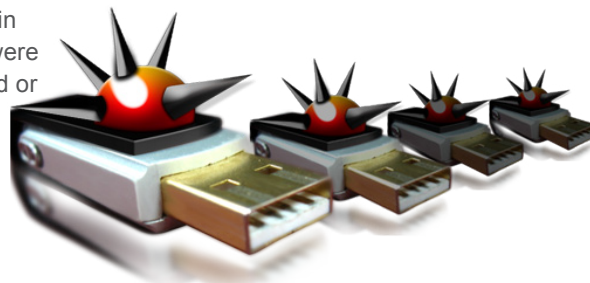


One way by which cybercriminals attacked ATMs was through devices known as skimmers. These devices stole the data encoded in the magnetic strips of ATM cards or debit or credit cards. An example of this device was the fake point-of-sale (POS) terminal that **was sold in underground forums**. This device came with a flash memory where it stored the data it stole off victims' debit or credit cards.

TrendLabs engineers also discovered a data-stealing malware family known as TSPY_SKIMMER, which specifically targeted ATMs. This malware was designed by someone who was familiar with ATM architecture and who had direct access to ATMs since it had to be manually installed into a terminal in order to work. It could also use an ATM's keypad and screen to send out commands such as checking for the installed malware version, printing out stolen information, and even dispensing cash.

Compromised products come straight from the factory.

In 2009, several incidents wherein devices coming off the shelves were found to have been compromised or tampered with were reported. 2010 was no different, as a couple of malware found their way to newly shipped mobile phones.



One of these threats was a *Windows*-based malware aka **WORM_AUTORUN.WAV**, which **came preinstalled into new Samsung S8500 Wave smartphones**. Another threat known as **WORM_SILLY.QT** came with Vodafone smartphones. This **infected computers** to which infected phones have been plugged in.

With the exception of a few new threats that specifically targeted mobile OSs and SCADA systems, there was really nothing new in terms of technique, behavior, or motivation that we haven't yet seen in the past.

The Bad

With the exception of a few new threats that specifically targeted mobile OSs and SCADA systems, there was really nothing new in terms of technique, behavior, or motivation that we haven't yet seen in the past. So far, most of the threats that made their appearance in 2010 were just upgrades of old malware variants, recycled techniques from old-school malware, or shared common behaviors with previously discovered malware.



Based on the TrendLabs half-year report, the number of malicious URLs increased from 1.5 billion in January 2010 to over 3.5 billion in just six months.

What was more significant was the fact that there seems to be no stopping cybercriminals from producing more and more threats each year. For instance, Web threats continued to severely affect users in 2010. Based on our half-year report, the number of malicious URLs increased from 1.5 billion in January 2010 to over 3.5 billion in just six months. By the end of 2010, TrendLabs engineers handled about 123,352 unique Web threats every day from an estimated total of almost 300,000 unique samples daily.

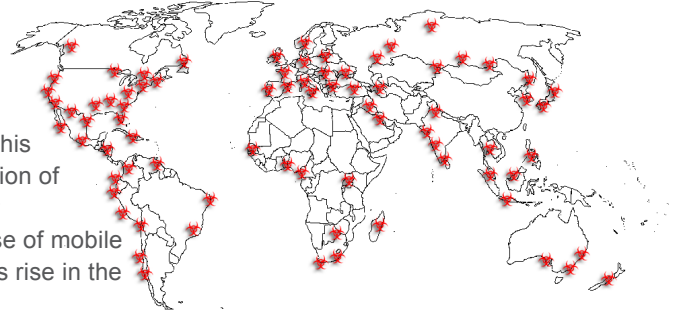
One highlight for Web threats was the fact that search engines became the primary means cybercriminals used to instigate attacks. Throughout 2010, cybercriminals continuously exploited holidays, newsworthy events, and popular themes to deliver malware via blackhat search engine optimization (SEO) poisoning. As expected, the majority of these threats led to data-stealing malware.

Also mainstays in the threat landscape were application vulnerabilities. TrendLabs threat researchers reported a total of about 2,552 common vulnerabilities and exposures published in just the first half of 2010. This number excluded vulnerabilities that were privately reported to vendors.

Perhaps the severity of malware growth was most evident in the United Arab Emirates (UAE) where a 33 percent growth in the number of infected systems was recorded in less than a year. This contributed to a 10,000 percent growth from 2004. In Saudi Arabia, more than 420,000 systems have been compromised, indicating a 65 percent rise in less than a year. Trend Micro also estimated more than 2 million infected systems in other parts of the Middle East in the last seven years.

The Ugly

In the “Trend Micro 2011 Threat Predictions” report, security experts are looking at a profitable year ahead for cybercriminals. This is due to the growing adoption of platforms beyond *Microsoft Windows*, the increasing use of mobile devices, and the continuous rise in the Internet penetration.



As discussed earlier, the Internet remained the most common threat vector that cybercriminals used to infiltrate users' systems. This is not about to change but will instead further escalate, as more and more digital devices are hooked to the Web. Security industry experts project that there **will be about 16 billion Internet-enabled devices worldwide by 2020**. We can, therefore, expect cybercriminals to exploit these devices for attacks as they are developed.

In addition, the Trend Micro predictions report also mentioned that cybercriminals will carry out more cunning malware campaigns in tandem with more devious social engineering techniques. Even as the technological landscape continues to change, the fact that users will always be the weakest link in the security chain will remain unchanged. As such, cybercriminals will continue to bank on vulnerabilities in human behavior to infiltrate systems and other devices.

Without proper awareness and knowledge of threats, all of the security measures and infrastructures an ordinary user or an enterprise puts up will be rendered useless.

** Please help us improve our reports by taking our quick survey.*

Resources:

- *Alertsec Xpress Data Security Blog*. (July 3, 2010). “Data Breach Report 2010 by ITRC.” <http://blog.alertsec.com/2010/07/data-breach-report-2010-by-itrc/> (Retrieved December 2010).
- Bernadette Irinco. (August 17, 2010). *TrendLabs Malware Blog*. “MaliciousAndroidApp Spies on User’s Location.” <http://blog.trendmicro.com/malicious-android-app-spies-on-users-location/> (Retrieved December 2010).
- Bernadette Irinco. (August 10, 2010). *TrendLabs Malware Blog*. “First Android Trojan in the Wild.” <http://blog.trendmicro.com/first-android-trojan-in-the-wild/> (Retrieved December 2010).
- Danielle Veluz. (June 5, 2010). *TrendLabs Malware Blog*. “Infected S8500 Wave Phones Make It to Germany.” <http://blog.trendmicro.com/infected-s8500-wave-phones-make-it-to-germany/> (Retrieved December 2010).

Even as the technological landscape continues to change, the fact that users will always be the weakest link in the security chain will remain unchanged.

- Danielle Veluz. (March 12, 2010). *TrendLabs Malware Blog*. "Malware Gets Smart with Vodafone Smartphone." <http://blog.trendmicro.com/malware-gets-smart-with-vodafone-smartphone/> (Retrieved December 2010).
- Florabel Baetiong. (March 2, 2010). *TrendLabs Malware Blog*. "Text Spam and Text Scams." <http://blog.trendmicro.com/text-spam-and-text-scams/> (Retrieved December 2010).
- Gartner, Inc. (November 10, 2010). *Gartner Newsroom*. "Gartner Says Worldwide Mobile Phone Sales Grew 35 Percent in Third Quarter 2010; Smartphone Sales Increased 96 Percent." <http://www.gartner.com/it/page.jsp?id=1466313> (Retrieved December 2010).
- Gelo Abendan. (March 1, 2010). *TrendLabs Malware Blog*. "KOOBFACE Makes a Comeback." <http://blog.trendmicro.com/koobface-makes-a-comeback/> (Retrieved December 2010).
- Georgina Enzer. (October 31, 2010). *ITP.net*. "Trend Micro Reveals Startling PC Bug Statistics: The Company Says Infected Computers in the UAE Have Increased by 10,000% Since 2004." <http://www.itp.net/582568-trend-micro-reveals-startling-pc-bug-statistics> (Retrieved December 2010).
- Ivan Macalintal. (December 12, 2010). *TrendLabs Malware Blog*. "2010 in Review: The Hype and Reality of STUXNET." <http://blog.trendmicro.com/2010-in-review-the-hype-and-reality-of-stuxnet/> (Retrieved December 2010).
- Jonathan Leopando. (October 26, 2010). *TrendLabs Malware Blog*. "Firefox Zero-Day Found in Compromised Nobel Peace Prize Website." <http://blog.trendmicro.com/firefox-zero-day-found-in-compromised-nobel-peace-prize-website/> (Retrieved December 2010).
- Jonathan Leopando. (August 31, 2010). *TrendLabs Malware Blog*. "TDSS Pretending to Be TweetDeck Update." <http://blog.trendmicro.com/tdss-pretending-to-be-tweetdeck-update/> (Retrieved December 2010).
- Jonathan Leopando. (August 4, 2010). *TrendLabs Malware Blog*. "Online iPhone Jailbreak Uses iOS Vulnerabilities." <http://blog.trendmicro.com/online-iphone-jailbreak-uses-ios-vulnerabilities/> (Retrieved December 2010).
- Jonathan Leopando. (June 30, 2010). *TrendLabs Malware Blog*. "New Symbian Malware on the Scene." <http://blog.trendmicro.com/new-symbian-malware-on-the-scene/> (Retrieved December 2010).
- Jonathan Leopando. (June 15, 2010). *TrendLabs Malware Blog*. "Passwords Matter—The Hidden Risks 'Minor' Info Stealers Pose." <http://blog.trendmicro.com/passwords-matter-the-hidden-risks-minor-info-stealers-pose/> (Retrieved December 2010).
- Jonathan Leopando. (April 11, 2010). *TrendLabs Malware Blog*. "WordPress Blogs Suffer from a Mass Compromise." <http://blog.trendmicro.com/wordpress-blogs-suffer-mass-compromise/> (Retrieved December 2010).

- Kevin Stevens. (September 15, 2010). *TrendLabs Malware Blog*. "One Server, Multiple Botnets." <http://blog.trendmicro.com/one-server-multiple-botnets/> (Retrieved December 2010).
- Loucif Kharouni. (September 2, 2010). *TrendLabs Malware Blog*. "PUSHDO Takedown Damages Botnet." <http://blog.trendmicro.com/pushdo-takedown-damages-botnet/> (Retrieved December 2010).
- Maxim Goncharov. (June 23, 2010). *TrendLabs Malware Blog*. "For Sale: Fake POS Devices." <http://blog.trendmicro.com/for-sale-fake-pos-devices/> (Retrieved December 2010).
- Norman Ingal. (November 3, 2010). *TrendLabs Malware Blog*. "Customized Malware Attacks Become Widespread." <http://blog.trendmicro.com/customized-malware-attacks-becoming-widespread/> (Retrieved December 2010).
- Patrick Estavillo. (September 24, 2010). *TrendLabs Malware Blog*. "New Azvhan Bot Family Revealed." <http://blog.trendmicro.com/new-azvhan-bot-family-revealed/> (Retrieved December 2010).
- Ranieri Romera. (September 13, 2010). *TrendLabs Malware Blog*. "Mehika Twitter Botnet Targets Twitter Users." <http://blog.trendmicro.com/mehika-twitter-botnet-targets-twitter-users/> (Retrieved December 2010).
- Ranieri Romera. (September 2010). *TrendWatch*. "Discerning Relationships: The Mexican Botnet Connection." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/discerning_relationships__september_2010_.pdf (Retrieved December 2010).
- Roland Dela Paz. (July 21, 2010). *TrendLabs Malware Blog*. "ATMs Now High-Profile Cybercrime Targets." <http://blog.trendmicro.com/atms-now-high-profile-cybercrime-targets/> (Retrieved December 2010).
- Roland Dela Paz. (February 16, 2010). *TrendLabs Malware Blog*. "Keeping an Eye on the EYEBOT and a Possible Bot War." <http://blog.trendmicro.com/keeping-an-eye-on-the-eyebot-and-a-possible-bot-war/> (Retrieved December 2010).
- Ryan Flores. (June 29, 2010). *TrendLabs Malware Blog*. "Backdoors in Twitter, Now in Arabic." <http://blog.trendmicro.com/backdoors-in-twitter-now-in-arabic/> (Retrieved December 2010).
- *The Telegraph*. (December 23, 2010). "16 Billion Devices Online by 2020, Says Report." <http://www.telegraph.co.uk/technology/internet/8097488/16bn-devices-online-by-2020-says-report.html> (Retrieved December 2010).
- TrendLabs. (August 2010). *Threat Encyclopedia*. "ANDROIDOS_DROIDSMS.A." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_DROIDSMS.A (Retrieved December 2010).

- TrendLabs. (July 2010). *TrendWatch*. "July2010ThreatRoundup." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/july_2010_threat_roundup.pdf (Retrieved December 2010).
- TrendLabs. (June 2010). *Threat Encyclopedia*. "WORM_AUTORUN.WAV." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=WORM_AUTORUN.WAV (Retrieved December 2010).
- TrendLabs. (June 2009). *Threat Encyclopedia*. "WORM_SILLY.QT." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=WORM_SILLY.QT (Retrieved December 2010).
- TrendLabs. (2009). *TrendWatch*. "2009's Most Persistent Malware Threats." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/2009s_most_persistent_malware_threats__march_2010_.pdf (Retrieved December 2010).
- TrendLabs. *Threat Encyclopedia*. "TROJ_PIDIEF.HLA." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=TROJ_PIDIEF.HLA (Retrieved December 2010).
- TrendLabs. *Threat Encyclopedia*. "ZeuS and Its Continuing Drive Toward Stealing Online Data." http://threatinfo.trendmicro.com/vinfo/web_attacks/ZeuS_and_its_Continuing_Drive_Towards_Stealing_Online_Data.html (Retrieved December 2010).
- TrendMicro. (1H2010). *TrendWatch*. "TrendLabsGlobalThreatTrends1H2010." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/tm101hthreat_report.pdf (Retrieved December 2010).
- TrendMicro. (December 9, 2010). *TrendWatch*. "TrendMicroThreatPredictionsfor2011." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/trend_micro_2011_threat_predictions.pdf (Retrieved December 2010).
- Trend Micro. (December 2009). *TrendWatch*. "The Future of Threats and Threat Technologies: How the Landscape Is Changing." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/trend_micro_2010_future_threat_report_final.pdf (Retrieved December 2010).