



Securing Your Journey
to the Cloud

Trend Micro

TrendLabs

Threat Trends 2010: The Year of the Toolkit



How Bad Was the Threat Landscape in 2010?

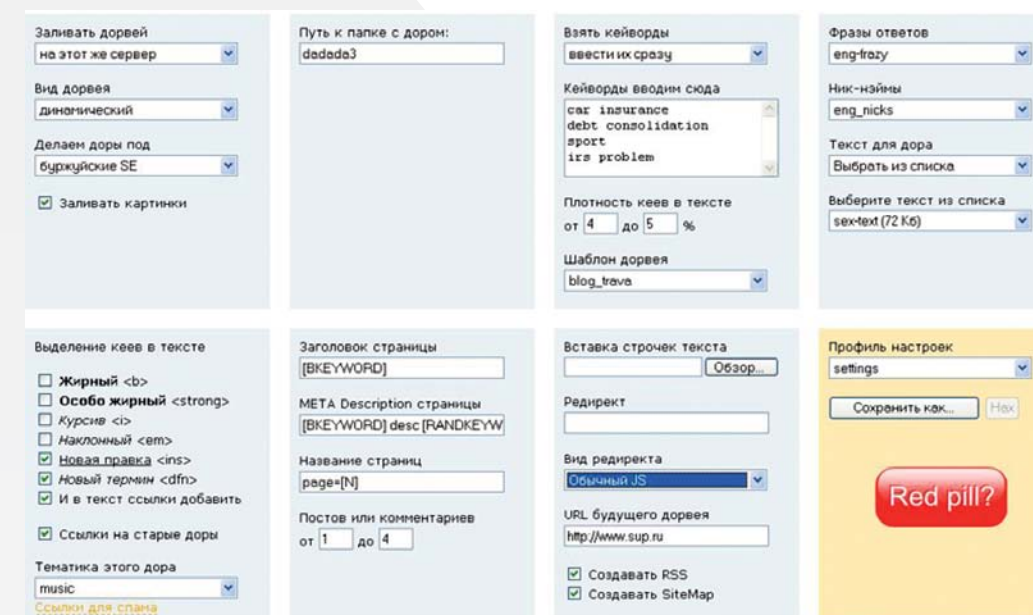
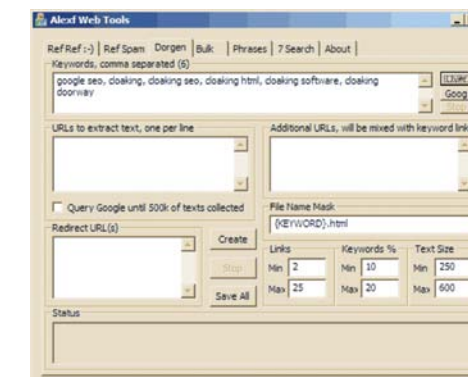
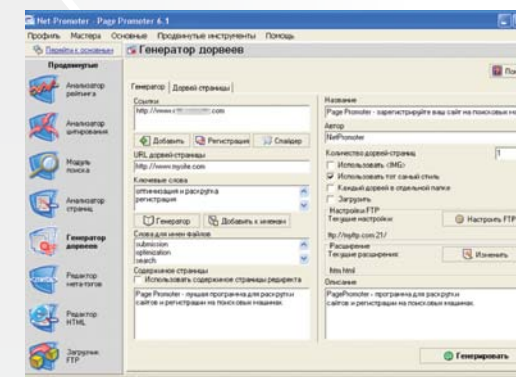
Era of Instant Crime

More than anything else, 2010 was distinguished by the full and proper emergence of toolkits as a means to perpetrate cybercrime. While these have always been a part of the cybercrime underground, in 2010 they flourished and became an even bigger part of the overall threat landscape.

Let us take, for example, a typical scenario for malware attacks. Many systems today are infected when users search for information utilizing search engines. Sometimes the infection is readily apparent—FAKEAV—at other times these are silent—banking Trojans. One would think that this is the work of a skilled hacker but that is not always the case.

Poisoning search engine results—a technique known as blackhat search engine optimization (SEO)—involves creating Web pages that will be highly ranked for certain search terms. Doing this manually is tedious but there are many point-and-click toolkits that automate the whole process. Tools like XRumer and uMaxSoft Doorway Generator can take target keywords and can automatically create thousands of the necessary sites.

Next, a cybercrime gang needs to upload the said pages to sites—either malicious or compromised. Again, compromising sites one by one is a tedious process. Toolkits also considerably automate this process, running the scripts needed to compromise sites en masse. Note that this process occurs within hours, if not less, after a topic becomes newsworthy.



The final stage of the attack is the payload itself—most commonly FAKEAV or a banking Trojan. Several toolkits exist to create FAKEAV interfaces. All major banking Trojans are distributed as toolkits, ranging from infamous threats like ZeuS and SpyEye to up-and-comers like ARES.

SpyEye Builder v1.2.00 [1 x 1] Injects in GPF



Spy Eye v1.2

Mained Pa.txt:

Collection.txt:

Encryption key (for config):

Commodor interval (sec):

Kill Zone:

Clear cookies when startup (IE, FF): ☐

Delete non-exportable certificates: ☐

Don't send http-ports: ☐


Compress build by UPK v3.07w: ☐

Make LTR config (without additional plugins & javascripts): ☐

☐ Webinjector ☐ DownloadData ☐ Plugin


• EIE name : • Mutex name :

Your system is clean

w hours. 

Данные товара: Twitter комплект	
Дата добавления:	2010-06-27
Стоимость:	0 руб.
Описание:	<p>Данная схема работы и пакет пил-скриптов - предполагает что:</p> <ol style="list-style-type: none"> 1. Вы уже знакомы с сервисом микро-блогов Twitter.com. 2. Вы знакомы с принципами и логикой Twitter.com. 3. Вы в курсе специфических глюков и подводных Twitter.com. 4. Вы знакомы с причинами блокировки и сущности аккаунтов в Twitter.com. 5. Вы имеете представление о Twitter API. 6. Вы не идюот. <p>Те кто занимался продвижением своих микроблогов в Twitter.com или продвижением своих продуктов (дворцев, сайтов, товаров) используя Twitter.com наверняка столкнулись с "нехорошими нововведениями" (которые нагде не прописаны, ни в API, ни в Термсах).</p> <p>Например: инфофальшивые себе на блогик 1х друзей за сутки. Вроде все нормально.</p> <p>А злодотский обмен сообщениями - сущность аккаунта. И бороться с администр.</p>

Xloder
Poison Ivy




Telnet Backdoor Trojan Builder

Telnet Backdoor Trojan Builder


Ну наверно все поняли для чего этот билдер
Принцип работы простой
Открываем **BUILDER.exe** и в настройках пишем :

- Login** - тут вводим логин
- Password** - тут вводим пароль
- Port** - тут вводим порт с помощью которого мы будем подключаться к компу чайника

Потом нажимаем **Build** и все наш трой готов
Прогу написал Бакинский хакер , что бы все было понятно сделал пару скриншов




Результат:
01.02.2010
Адреса:
Других нет
Подключений:
69
Репутация:
3384



Step 1 : Создать вирус

Step 2 : Наш вирус готов



Backdoor
Полный файл MS-DOS
1 KB

Malware is changing its shape - **every few hours.**



It's hard to underestimate the impact that toolkits have on online criminal activity. There used to be something of a barrier to entry, as technical knowledge and expertise were both necessary to enter the world of cybercrime. Today, with cybercrime toolkits in full production, very little, if any, technical knowhow is needed to profit. This allows cybercriminal

attacks to be conducted with far less effort and time, the effects of which can be seen in the explosive growth of threats in 2010. Because it's all about money like we predicted in "The Future of Threats and Threat Technologies: How the Landscape Is Changing" in 2010, we did not expect cybercrime to go away and it did not.



Figure 4. Other crimeware toolkits

2010 Prediction Proven:

It's all about money, so cybercrime will not go away.



ITEM	PRICE
Botnet source price (kit plus source code)	US\$150-350
Distributed denial of service (DDoS)	1 hour-US\$5 per day-US\$50
DDoS	1 hour-US\$7-10 per day-US\$20-70
Hidden Team Viewer (send information in Jabber)	50 wmz
Internet password-stealing software	US\$20
Jabber backdoor	100 wmz
Keylogger, logs for which are sent to email	Rub 500
Keylogger, logs for which are sent to email	Rub 300
Logs stealer	100kb/100 wmz
Multifunctional Trojan	Negotiable
Private radmin tool to control desktop	US\$5

ITEM	PRICE
Trojan generator	35 wmz
Trojan source for ibank2	Rub 3,000
Trojan that steals all passwords from non-IE browsers in .JPEG format	Rub 2,000

Spam Trends

Era of Instant Crime

The spam volume continued to rise when viewed on a year-over-year (YoY) basis. In 2010, however, TrendLabs observed a significant decline in the spam volume both in November and again in the days leading to the Christmas holidays. This appeared counterintuitive, considering the usual surge in spam taking advantage of the online holiday shopping spree.

Based on our collaboration with several Internet service providers (ISPs), we confirmed that the end of the Spamit operations at the start of October 2010 contributed to the significant decline in the spam volume.

We also observed a decrease in the volume of Rustock spam before Christmas, which continued on until the first week of January, after which the spam volume started going back to regular levels.

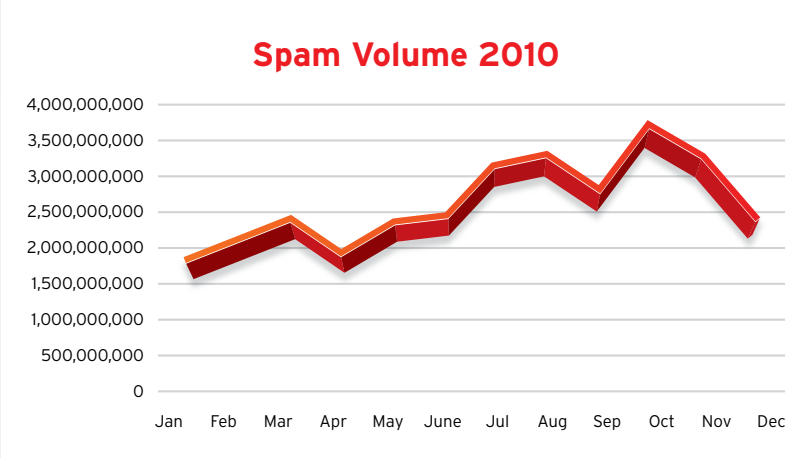


Figure 5. Spam volume in 2010

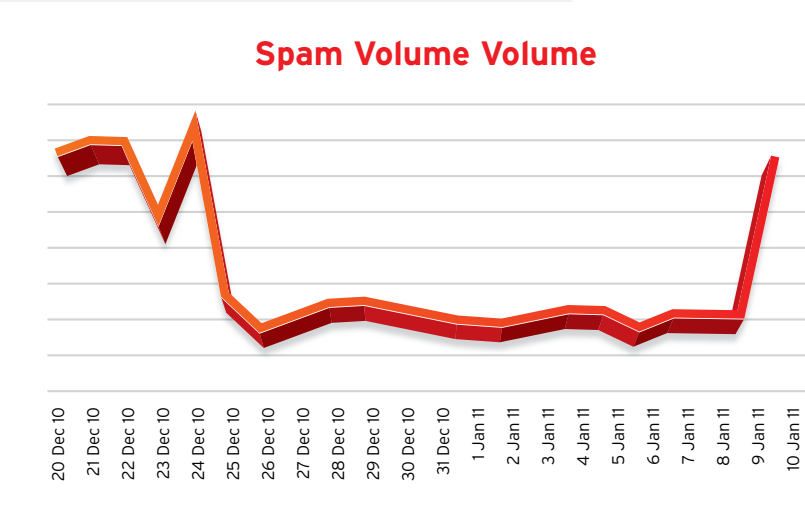


Figure 6. Spam volume from December 20, 2010-January 10, 2011

So far, our analysts believe that spamming is still too lucrative a business to completely abandon so any intervention that may affect the overall volume can only lead to a temporary slump.

In terms of spam distribution by country, the top spam recipient was still the United States. Overall, however, India turned out to be the second largest recipient, which indicated that it is an emerging significant Internet majority because of its growth in terms of Internet penetration and its use of English for formal/ official communications.

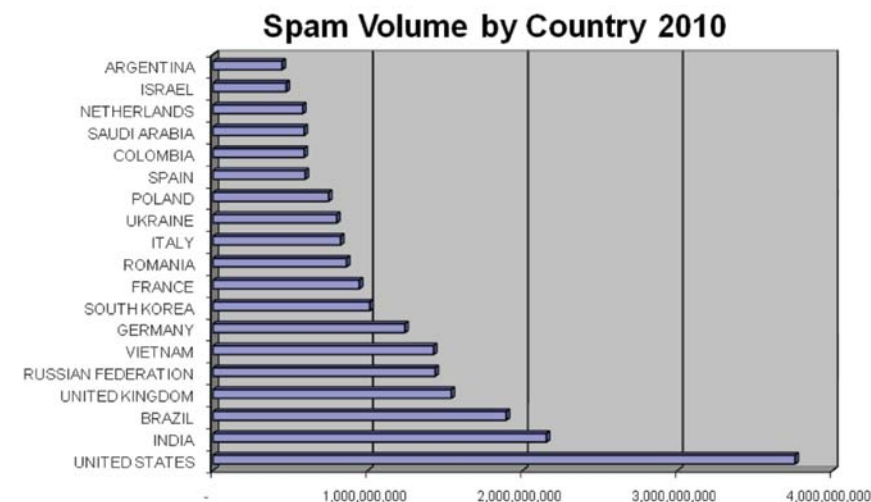


Figure 7. Spam volume by country in 2010

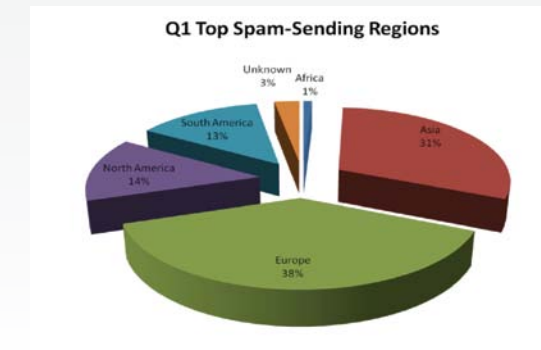


Figure 8. Top spam-sending regions in Q1 2010

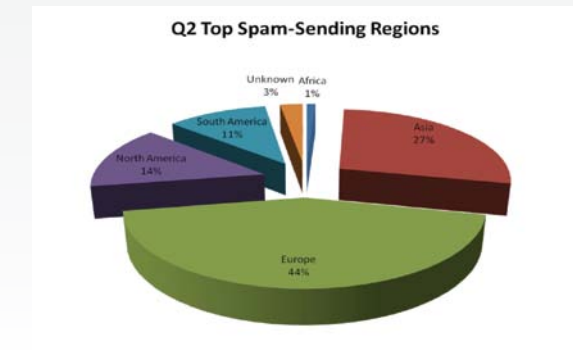


Figure 9. Top spam-sending regions in Q2 2010

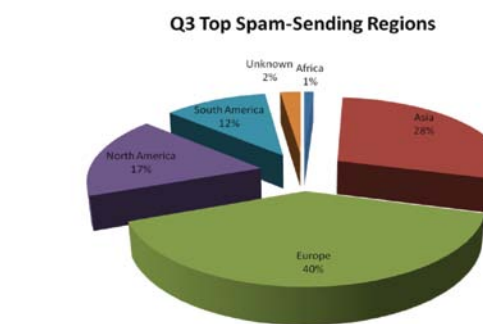


Figure 10. Top spam-sending regions in Q3 2010

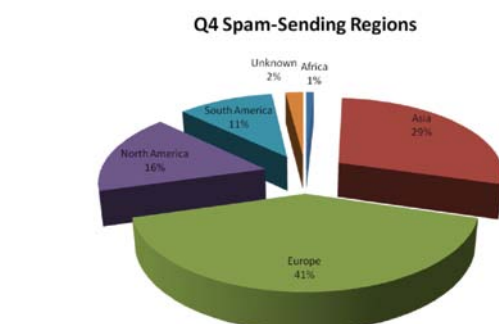


Figure 11. Top spam-sending regions in Q4 2010

In the “TrendLabs Global Threat Trends 1H 2010,” we noted an increase in the spam volume in Europe compared with other regions. Online gambling and casino-related spam were especially prevalent in the region, as such activities were less strictly regulated in them than in North America. This spam type was frequently seen written in Spanish. Meanwhile, German was used in many spam that sold replica items in the third quarter of 2010. Russia was the top spam-sending country in the fourth quarter, partly because sending spam was not a criminal offense in it.

TrendLabs classifies spam by type based on their content’s general characteristics. Pharmaceutical and other health-related spam made up the majority of the spam we tracked throughout the year. This spam type was not limited to selling pharmaceutical products online, however, as spammers also used these to disguise their phishing and malware attacks. Other non-English spam contained dating, adult, and commercial content.

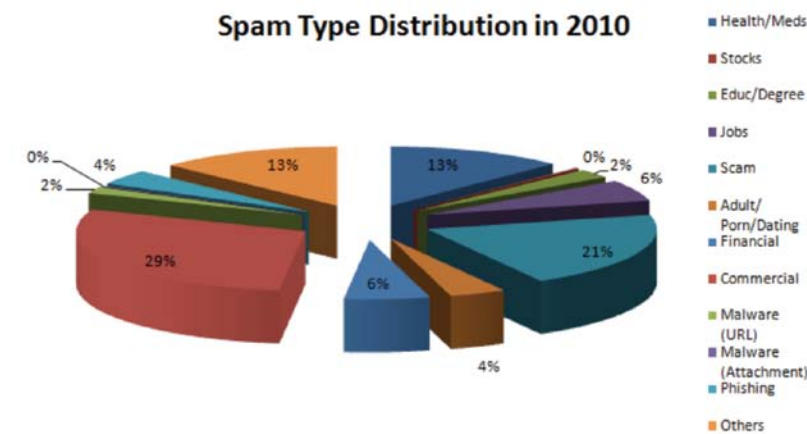


Figure 12. Top spam types in 2010

By technique, salad spam were frequently seen in 2010. The content of this spam type was noncommercial-, nonadvertising-, and nonbusiness-related in nature. This spam type can contain an article, an excerpt from a site, or a paragraph from someone’s biography. Some salad spam had no meaning while others were written with poor grammar. Some contained as few as 2-3 random characters. Research indicates that these messages were sent more to gather “live” email addresses rather than to actually conduct attacks.

Different kinds of spam-related toolkits and services have been on sale for a long time now in underground forums, including bulk stolen email addresses. Together, these enabled cybercriminals to automate and simplify email abuse as an entry point for spam, scams, and malware.

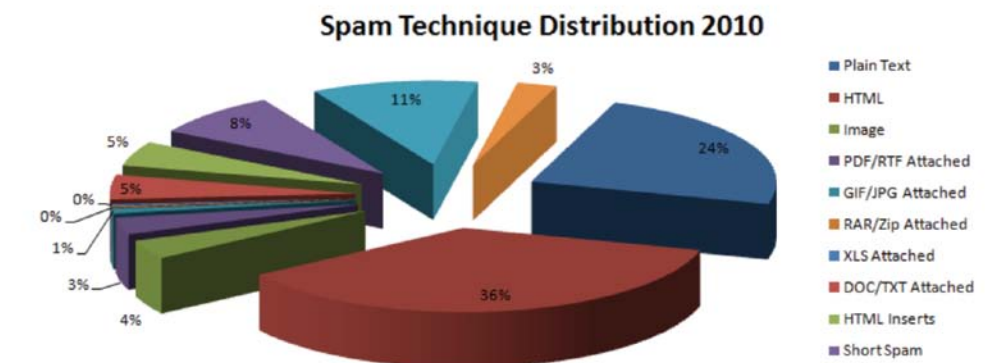


Figure 13. Top spamming techniques in 2010

Other Notable Spam Trends/Attacks

Phishing email gradually started to target not only banks but also popular social networking sites like Facebook, Twitter, MySpace, and the like, just as we predicted in 2010.

Social engineering was on the rise all year long with the use of various noteworthy events and topics like the tax season and WikiLeaks as well as social networking sites to spread malware.

Nigerian scams and fake lottery notifications also continued to proliferate in 2010. We saw multiple variants presented in different styles and with varying techniques.

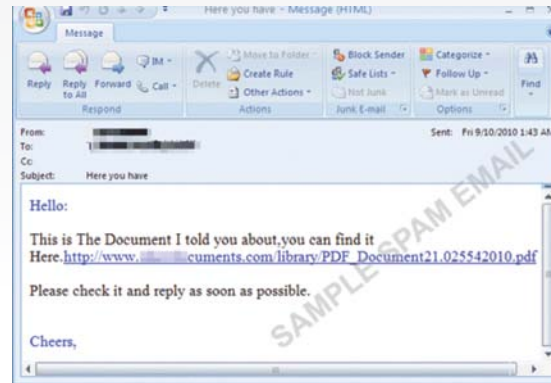


Figure 14. Sample “Here you have” spam

2010 Prediction Proven:

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



2010 Prediction Proven:

No global outbreaks, but localized and targeted attacks



At the start of 2010, we predicted that there will be fewer global outbreaks. We believed that cybercriminals will instead go for localized and targeted attacks, and we were right. Spam that carried malicious files or links to malware were also seen in 2010 with the proliferation of malware-related spam outbreaks. The most

notable malware-carrying spam was the “Here you have” spam, an email that contained links that led to WORM_MEYLM.E.B, a password-stealing worm that also installed a powerful backdoor program. This spam run was believed to have started out as a targeted attack that may have gone out of the spammers’ control.

Web-Based Threats

The Web has become the preferred choice by which cybercriminals reach their victims. Cybercriminals are willing to invest time and money to develop software, tools, and services that perform different cybercriminal activities—from poisoning search results to setting up exploit-ridden sites.

TrendLabs sampled the malware arrival vectors to determine what the most common means of infection is today. More than 80 percent of the top malware responsible for the most infections in 2010 arrived via the Web, most commonly via unknowingly downloading malicious binaries, proving our 2010 prediction that one Web visit is enough to get infected. Non-Web arrival methods include infections from network shares, removable drives, and the like. Note, however, that as most malware arrive through multiple infection vectors, the count in the chart below amounts to more than 100 percent.

2010 Prediction Proven:
Drive-by infections are the norm—one Web visit is enough to get infected. 

TrendLabs monitors the growth of malicious URLs and domains and found that in 2010 their volume continued to rise. We observed that certain top-level domains were heavily abused and used to host hundreds of thousands of malicious domains. Some domain registrars failed to enforce stricter policies to avoid widespread abuse by cybercriminals.

TrendLabs also monitors where malicious URLs are located (bad actors) and which countries these targeted (victims).

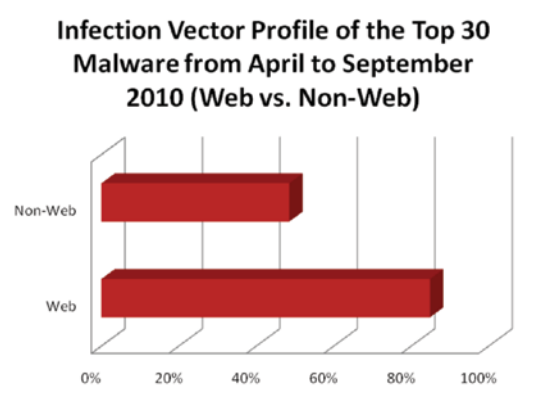


Figure 15. Infection vector profile of the top 30 malware from April-September 2010

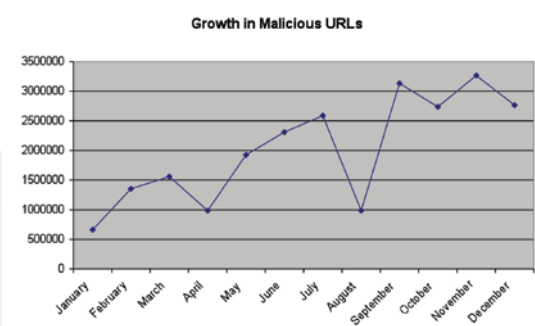


Figure 16. Growth in the malicious URL volume in 2010

Top Bad Actors per Quarter

The United States and China were almost always either the top 1 or 2 bad actor in each quarter in 2010. This means the majority of the malicious URLs each quarter were hosted (either knowingly or as a result).

Q1	Q2	Q3	Q4
United States	United States	China	United States
China	China	United States	Russian Federation
Netherlands	Ireland	Germany	China
Germany	Romania	Japan	Germany
Russian Federation	Germany	Ireland	Netherlands
Romania	Japan	Russian Federation	Japan
Japan	Netherlands	Romania	Canada
France	United Kingdom	Netherlands	Romania
United Kingdom	Russian Federation	Ukraine	United Kingdom
Canada	Ukraine	Italy	Unknown
Ukraine	Unknown	United Kingdom	Ukraine
South Korea	France	France	France
Sweden	Canada	Canada	Switzerland
Italy	South Korea	South Korea	South Korea
Unknown	Australia	Australia	Australia
Poland	Sweden	Sweden	Moldova
Bosnia and Herzegovina	Belgium	Switzerland	Hungary
Turkey	Italy	Belgium	Italy
Australia	Bahamas	Latvia	Belgium
Portugal	Latvia	Unknown	Sweden

Table 2. Top bad actors in 2010 by quarter

Top Victims per Quarter

Consequently, most of the victims were also from China and the United States. In addition, several of the users who accessed malicious content were from Japan.

Q1	Q2	Q3	Q4
Japan	Japan	Japan	United States
United States	United States	China	Japan
China	China	United States	Russian Federation
Taiwan	Australia	Taiwan	China
Australia	Taiwan	Australia	Australia
France	France	Russian Federation	Taiwan
Germany	Canada	France	France
Canada	Germany	Canada	Ukraine
Russian Federation	Italy	Germany	Germany
Italy	Spain	India	Canada
India	United Kingdom	Hong Kong	India
Spain	Russian Federation	Italy	Italy
United Kingdom	India	United Kingdom	United Kingdom
Norway	Norway	Singapore	Spain
Turkey	Turkey	Spain	Turkey
New Zealand	New Zealand	Malaysia	Malaysia
Brazil	Netherlands	Ukraine	Poland
Singapore	Sweden	Macao	Netherlands
Netherlands	Singapore	Turkey	Saudi Arabia
Hong Kong	Brazil	New Zealand	Brazil

Table 3. Top victims in 2010 by quarter

Top 10 Domains

One of the riskiest domains we blocked is related to a blackhat SEO attack wherein certain search results were poisoned to redirect to other malware-carrying sites, typically FAKEAV variants.

Malicious Domain	Country	Description
delivery.adyea.com	DEU	Related to blackhat SEO attacks that led to malicious banners or ads
dt.tongji.linezing.com	CHN	Related to CVE-2010-0806—a vulnerability in the Peer Objects component aka iepeers.dll
95.211.1.176	ROU	Related to a Trojan
hot1.xgazo.info	USA	Related to Proxy Avoidance
linux106.mysite4now.net	USA	A malicious file detected as TROJ_BREDLAB.SMP
ad.globe7.com	USA	Related to ads and a cross-site scripting (XSS) vulnerability
trafficconverter.biz	USA	Distributes malware, particularly DOWNAD variants
bid.openx.net	USA	Malicious advertising page
gchp.sagac.info	USA	Related to Proxy Avoidance
zOg7yai0.com	ROU	Malware distribution page

Table 4. Top malicious domains blocked in 2010

Top 10 Malicious URLs Blocked

Malicious Domain	Country	Description
delivery.adyea.com:80/lg.php	DEU	Reportedly related to blackhat SEO attacks that led to malicious banners or ads
dt.tongji.linezing.com:80/tongji.do	CHN	Related to CVE-2010-0806—a vulnerability in the Peer Objects component aka iepeers.dll
hot1.xgazo.info:80/pic.php	USA	Related to Proxy Avoidance
ad.proxad.net:80/delivery/lg.php	FRA	Known for malicious activities
ad.globe7.com:80/iframe3	USA	Related to ads and an XSS vulnerability
gchp.sagac.info:80/pic.php	USA	Related to Proxy Avoidance
newt1.adultadworld.com:80/jsc/z5/ff2.html	USA	Related to ZBOT variants
www.lzjl.com:80/popup.php	USA	A browser exploit
www.trafficholder.com:80/in/in.php	USA	Adult site traffic promoter known for distributing malware
trafficconverter.biz:80/	USA	Distributes malware, particularly DOWNAD variants

Table 5. Top malicious URLs blocked in 2010

Blackhat SEO attacks, which plagued users throughout 2009, continued throughout 2010. As in the past, search results for various news and human interest items were poisoned with links leading to FAKEAV malware. The most notable news or events cybercriminals leveraged include the Haiti earthquake, Apple’s iPad announcement, the rumored death of Johnny Depp, the “Super Bowl,” and the “Winter Olympics.” In some instances, searches for even phrases like “free printable” were also poisoned to lead to compromised sites.

Notable Site Compromises

Mass compromises continued to be a prevalent risk that Web users had to contend with. For instance, in the early part of the June, some 100,000 sites were compromised. Users who visited infected sites ended up with systems infected by data stealers that targeted online games.

The support page of Chinese PC maker Lenovo was compromised with the addition of a malicious iframe that led to the download of a BREDOLAB variant.

Redirectors in compromised sites also raised a flag in July because of the significant number of HTML redirectors that eventually led to the infamous Canadian Pharmacy or Pharmacy Express. Based on available data, there was a daily average of 1,000 new compromised sites, some of which have repeatedly been hit before.

Several Blog*Spot (now Blogger) pages were compromised in late August 2010, which pushed these to display spam supposedly from Newegg, UPS, Amazon, and/or LinkedIn. Run-of-the-mill resume and e-card spam were also posted in compromised blogs.

Several WordPress blogs became victims of a mass compromise attack. The blogs' settings were modified by cybercriminals, which led affected users to a malicious site that ended with a TROJ_FAKEAV.ZZY infection.

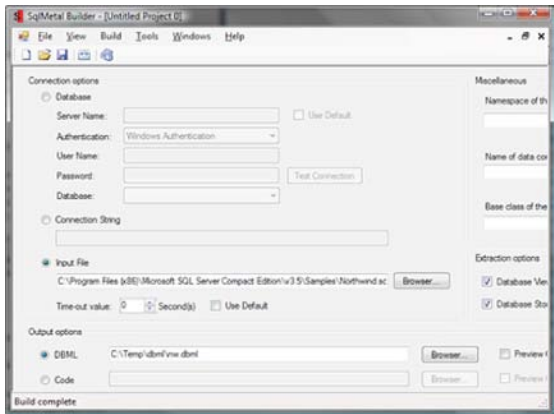


Figure 17. Sample SQL injection tool

Social Networking Sites

Cybercriminals are training their eyes on social networking sites as a major platform on which to launch spam, scams, and malware attacks. One of the most dangerous malware-related attacks include that which used Twitter to send out malware in relation to the "World Cup." Regional attacks also used Twitter, as Tweets in Arabic that led to various backdoor programs were also spotted.

Twitter has long been used to spread malware both via publicly viewable and private Tweets and direct messages (DMs). A recent botnet was found to use the site for its command-and-control (C&C) mechanism, again supporting our claim in 2010 that bots cannot be stopped and will be around forever. Like ZBOT variants, this malware was distributed via a builder application.

Two attacks specifically targeted Facebook users via DMs sent by the relentless KOOFACE botnet and shortened URLs padded with a Facebook-related query string. Twitter likewise continued to be a favorite target, as evidenced by the underground release of a Twitter kit, which can become an effective spamming tool in the long run.

Meanwhile, different types of spam and some voucher scams proliferated in social networking sites. Compromised or hacked Twitter accounts were used to deliver links that led to Acai Berry diet pill-selling sites. Facebook was also used to spread malware. In one particular attack, cybercriminals used social engineering to get users to directly paste an obfuscated JavaScript code into their browser address bars. While the code did little more than spam other users' walls, this made it possible to use the same technique to proliferate more malicious wares.

2010 Prediction Proven:

Bots cannot be stopped anymore, and will be **around forever**.



File-Based Threats

TrendLabs monitors instances of malware trending worldwide, by region, and by industry. Based on available data, DOWNAD (aka Conficker) continued to be the most prevalent malware. This network-based worm infiltrated several corporate and business networks beginning 2008 and continues to do so today. It arrives by exploiting the Microsoft Server Service vulnerability MS08-067.

Pesky adware like ADW_MYWEBSEARCH and ADW_ZANGO.BK were likewise prevalent, most notably in the North American region.

2010 Top 5 Malware per Quarter based on Malware Activity Detected Globally

Top Malware in Q1		Top Malware in Q2	Top Malware in Q3	Top Malware in Q4
1	WORM_DOWNAD.AD	WORM_DOWNAD.AD	WORM_DOWNAD.AD	WORM_DOWNAD.AD
2	CRCK_KEYGEN	ADW_MYWEBSEARCH	CRCK_KEYGEN	CRCK_KEYGEN
3	TROJ_FAKEAL.SMDP	CRCK_KEYGEN	TROJ_BURNIX.SMEP	TROJ_FLYSTUD.SMZ
4	WORM_FLYSTUD.SMC	ADW_TCENT	TROJ_FAKEAV.SMES	TROJ_HILOTI.SMEO
5	ADW_ZANGO.BK	WORM_FLYSTUD.SMC	HKTL_BLKRAIN	TROJ_FAKEAL.SMEP

Table 6. Top 5 malware by quarter based on globally detected malware activity in 2010

Almost all of the regions still had problems with malware such as certain worms and file infectors due to the use of technically advanced antivirus evasion techniques. PE_MABEZAT.B-O, for instance, had a built-in polymorphic engine that changes its file size every time it infects files.

2010 Top 5 Malware per Quarter based on Malware Activity Detected per Region

Top Malware in APAC		Top Malware in China	Top Malware in EMEA
1	WORM_DOWNAD.AD	WORM_ECODE.E-CN	WORM_DOWNAD.AD
2	CRCK_KEYGEN	WORM_DOWNAD.AD	CRCK_KEYGEN
3	PE_SALITY.EK	CRCK_KEYGEN	PE_MABEZAT.B-O
4	PE_SALITY.EN-1	ADW_TCENT	HKTL_DECRYPT
5	BKDR_HUPIGO.SMX	TROJ_SWIZZOR.KCC	PE_MABEZAT.B-1

Top Malware in Japan		Top Malware in Latin America	Top Malware in North America
1	CRCK_KEYGEN	WORM_DOWNAD.AD	ADW_MYWEBSEARCH
2	WORM_DOWNAD.AD	CRCK_KEYGEN	WORM_DOWNAD.AD
3	PE_PARITE.A	WORM_FLYSTUDI.F	CRCK_KEYGEN
4	WORM_ANTINNY.AI	WORM_VB.SMP	TROJ_FAKEAV.SMES
5	WORM_ANTINNY.JB	TROJ_FLYSTUD.SMZ	ADW_ZANGO.BK

Table 7. Top 5 malware by quarter by region based on detected malware activity in 2010

The education and government sectors were most affected in 2010. Schools were often considered opportune targets for multiple reasons, including outmoded infrastructure, lack of resource and budget, and lack of user awareness and accountability. The government

sector includes local governments, which do not often have the same budget or resource for their IT needs, unlike central government. In addition, local governments do not generally face the same level of scrutiny that push them to reinforce their security policies.

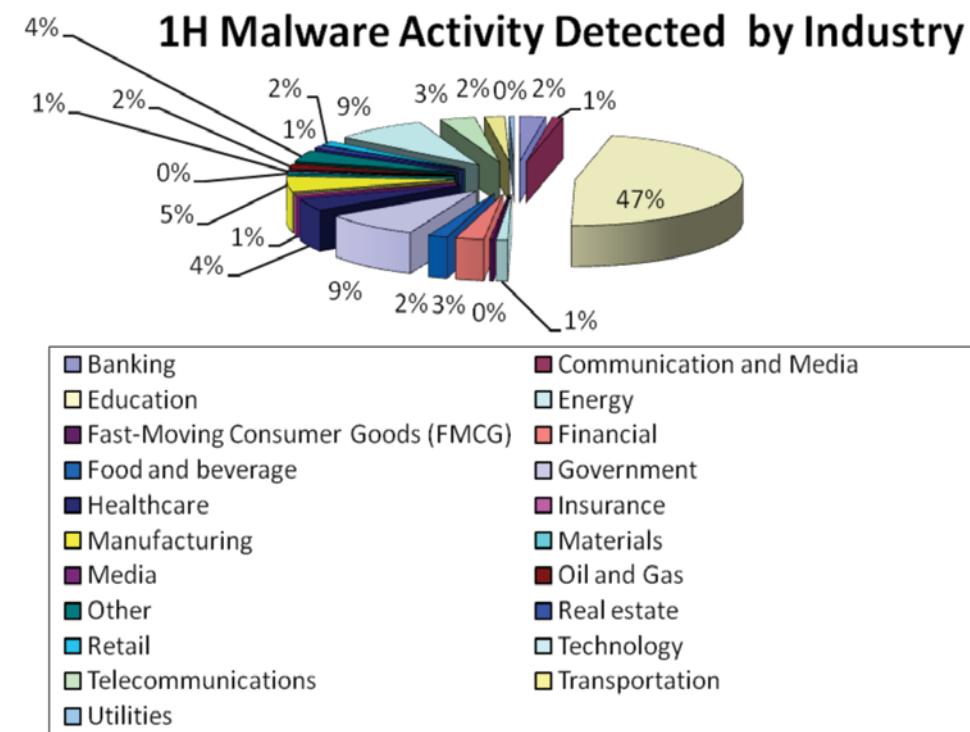


Figure 18. Malware activities by industry in H1 2010

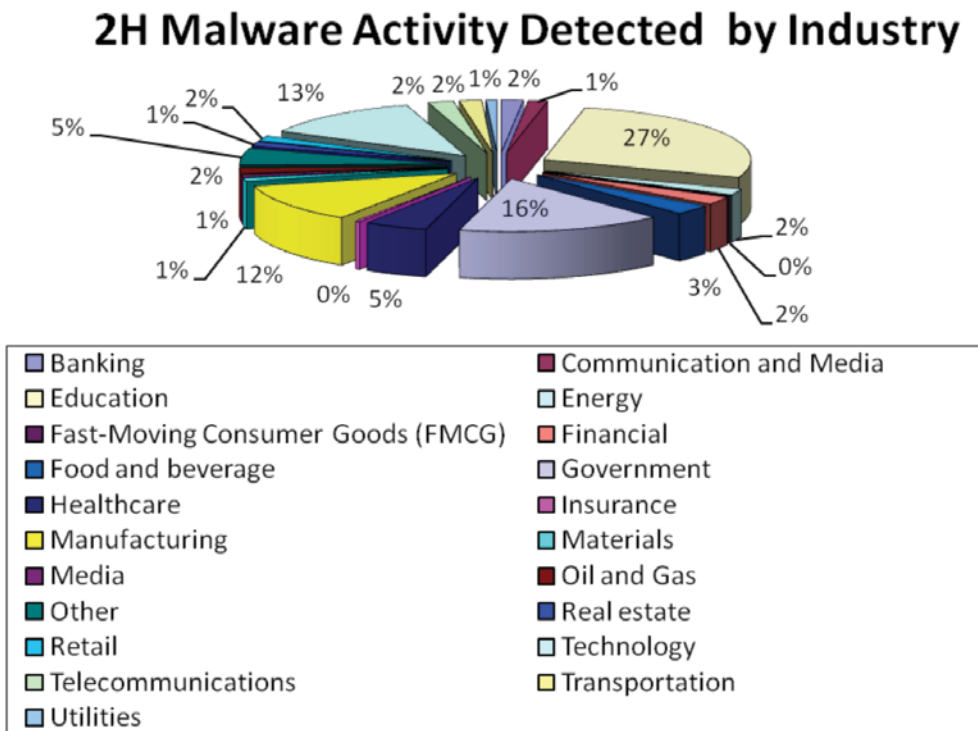


Figure 19. Malware activities by industry in H2 2010

STUXNET Attacks SCADA Systems

One of the most noteworthy malware attacks to date involved STUXNET—a sophisticated malware that targeted a specific vendor’s supervisory control and data acquisition (SCADA) platform—raised awareness of the impact of failing to secure industrial control systems. It first surfaced in July 2010, during which most of the vulnerabilities that it exploited were still unpatched.

STUXNET has three components—a worm, an .LNK file, and a rootkit. The worm executes all of the attack’s major routines. The LNK component primarily ensures the execution of the propagated worms because the vulnerability it exploits—the Windows shortcut vulnerability—makes it especially effective. The rootkit component is responsible for hiding related files and processes.

The worm component—WORM_STUXNET.A—looks for legitimate .DLL files used by Siemens WinCC systems in the Windows system folder and replaces these with almost the same files with additional codes to call the functions that access, read, write, and delete code blocks on the programmable logic controller (PLC). It can thus intercept and modify received and sent data.

Furthermore, STUXNET exploits a password security bypass vulnerability that allowed it to view project database information on, to alter settings on, or to delete some data from the WinCC server.

ZeuS Developments in 2010

ZeuS is a botnet toolkit that became very popular in the cybercriminal underground. It spawned different botnets that have stolen millions of dollars from home users and companies alike. In the first half of 2010, ZeuS 2.0 was released. ZeuS 2.0 carried several improvements with regard to its ability to hide its existence and activities, specifically the use of random instead of fixed file names and mutexes and strengthened encryption.

Meanwhile, ZeuS’ competitors benefitted from the going-rate of the toolkit, which at one point reached US\$8,000 for just the basic package. ZeuS’ most successful competitor was SpyEye, a toolkit that sold for up to US\$2,500 with additional features. We documented our findings on SpyEye in the following blog entries:

- Uncovered SpyEye C&C Server Targets Polish Users
- One Server, Multiple Botnets
- The SpyEye Interface, Part 1: CN 1
- The SpyEye Interface, Part 2: SYN 1

In October 2010, shortly after an international operation that shut down one of the cybercriminal gangs using ZeuS and resulted in charges being brought against several individuals, ZeuS’ creator handed over the ZeuS code to the SpyEye creator. Trend Micro first found samples of the new ZeuS variant—TSPY_ZBOT.BYZ—that, in addition to performing information-stealing routines, also infected executable files on infected systems. The infected files generated domains that the variants then accessed to download more malware. The in-depth analysis on TSPY_ZBOT.BYZ revealed a well-engineered threat, the results of which was documented in our white paper, “File-Patching ZBOT Variants: ZeuS 2.0 Levels Up.”

The toolkits that enabled automated information theft were definitely driving forces of cybercrime throughout the year. We expect to see mergers and improvements in the cybercriminal underground that will learn from past mistakes and make detection harder for the security industry.

FAKEAV Updates

The threats FAKEAV malware pose continued to cause trouble for users in 2010. Preexisting behaviors in 2009 were reinforced in 2010—news and other events that caught the public eye were routinely poisoned with malicious search results.

There were two major developments to FAKEAV. First, we found that the cybercriminals that sold FAKEAV malware used increasingly sophisticated ways to deliver their wares. Networks of doorway pages—pages on individual sites or compromised ISPs that hosted redirections to other doorway pages and/or

exploits for various vulnerabilities—were found and extensively documented by our researchers in 2010, as in the blog post “Doorway Pages and Other FAKEAV Stealth Tactics.”

The vulnerabilities used to deliver FAKEAV malware also changed somewhat. In addition to the usual well-known targets such as Windows; IE; and Adobe Flash Player, Acrobat, and Reader, Oracle’s Java was also increasingly used by increasingly used by FAKEAV purveyors. According to our own researchers, these were used in tandem with so-called customized attacks.

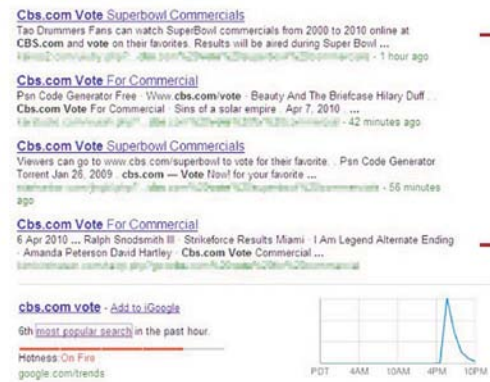


Figure 20. Sample doorway pages

These customized attacks were one of the biggest developments in FAKEAV malware in 2010. The creators of FAKEAV malware now use various techniques to determine what software run on users' systems to send them to pages that more closely resembled their working environments. For example, users of Firefox browsers get pages that more closely resembled real pages from Mozilla while IE users received a different page altogether. This made the attacks more convincing.

A final development in FAKEAV malware in the latter half of the year was the rise of fake utility malware. This “cousin” of FAKEAV malware is distributed in the same way. However, instead of finding these on infected systems, users are told that there are problems with their hardware that they needed to fix.

Similarly, whatever problems that needed to be fixed required payment.

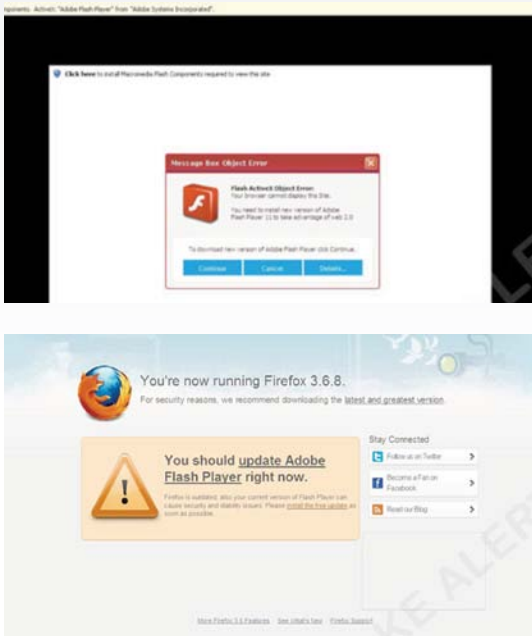


Figure 21. Customized malicious graphical user interfaces (GUIs)



Figure 22. Sample fake utility tool

Mobile Threats

Mobile phone usage will continue increasing well into 2011. Gartner reported in November 2010 that the global mobile phone sales grew 35 percent in the third quarter compared with the same period the previous year. Smartphone sales accounted for a 19.3 percent share, after posting a 96 percent growth compared with the same period the previous year.

The numbers, however, differed per research agency in 2010. Apple's iOS and Google's Android OS are both poised to conquer the overall smartphone OS market. Of these two, however, Android OS is more widely available, as iOS is basically exclusive to the iPhone.

Phishing attacks present the same threat to mobile device as to PC users. In November 2010, an independent researcher found that in certain cases, the Safari browser hides the address bar after a website finishes loading. Phishers can abuse this to add an added layer of believability to their attacks. They can place the legitimate URL in a fake address bar while the phished one loads in the real but hidden address bar.

The important thing to always remember is that these days, mobile devices act as mini-computers. They offer most, if not all, of the functionality of a normal PC, delivered in a smaller and more portable format.

Threats such as data and personal information theft are very real considerations, as device loss and theft occur daily. Some reports even suggest that as many as 12,000 laptops are lost every week in U.S. airports alone. Given the exponential growth of mobile devices combined with increasing consumerization, as companies allow or encourage employees to purchase their own hardware, including e-readers, tablet PCs, smartphones, and laptops, we can expect security to be a growing issue.

In August, we saw malware target the Android OS, the first of which was ANDROIDOS_DROIDSMS.A, a malicious text message-sending application disguised as Windows Media Player. A week after, another application, ANDROIDOS_DROISNAKE.A, which can send a user's Global Positioning System (GPS) location via HTTP POST, surfaced. Other Android OS malware were discovered thereafter.

Some smartphones that came preinstalled with malware were also documented in 2010 like the 3,000 Android OS smartphones that came with WORM_SILLY.QT, a worm with denial-of-service (DoS) capabilities.

We also found other malware target smartphone OSs like Symbian. Cybercriminals are always on the lookout for any form of monoculture, which can be a large base of possible targets for scams or malware attacks. The increase in the use of Android OS in smartphones, along with the OS' open source code, may contribute to an increase in attempts that target the OS.

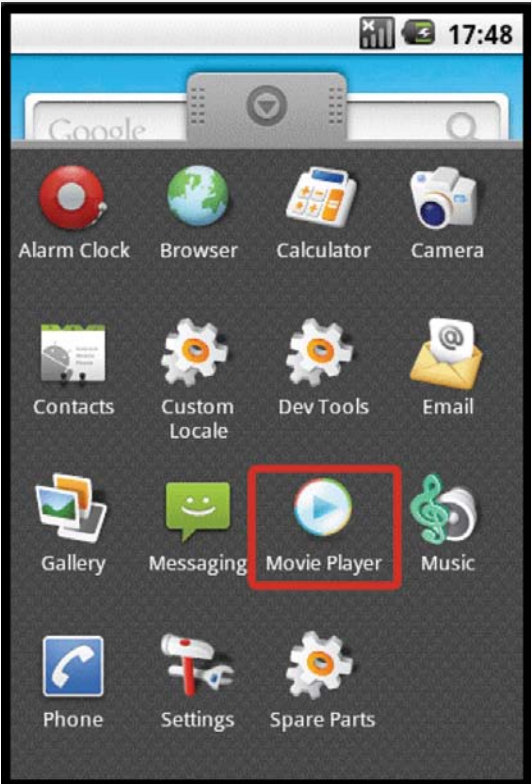


Figure 23. Sample Android OS malware

Vulnerability Landscape

Overall, the number of vulnerabilities went down but popular applications and OSs were still affected. As such, our 2010 prediction that risk mitigation is not as viable an option anymore even with alternative browsers/OSs came true. Windows, IE, Java, Adobe Acrobat, Adobe Reader, and Adobe Flash Player were all hit by new vulnerabilities throughout 2010.

In 2010, a total of 4,651 vulnerabilities were assigned designations in the Common Vulnerabilities and Exposures (CVE) database. This slightly decreased from 2009 although this particular data does not reflect the number of vulnerabilities that resulted in malicious exploitation.

2010 Prediction Proven:

Risk mitigation is not as viable an option anymore—even with alternative browsers/OSs



Number of Vulnerabilities

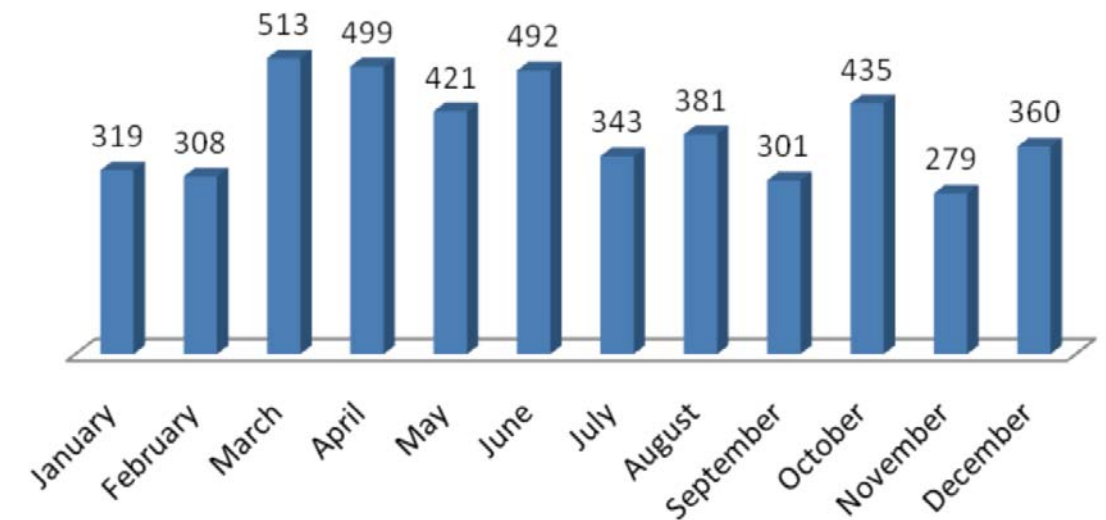


Figure 24. Number of vulnerabilities each month in 2010

Among the vendors, Microsoft had the most CVEs issued at 317. Apple came in second with 302 CVEs

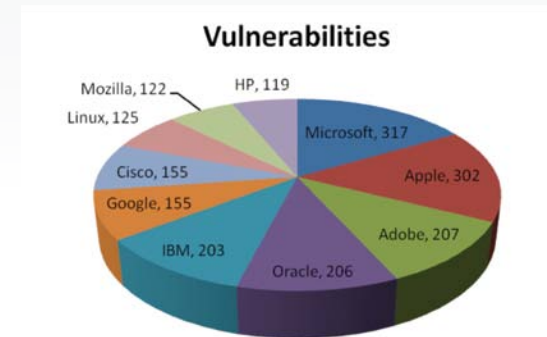


Figure 25. Top 10 vendors in terms of CVEs issued

Attacks on third-party applications have become more popular and Adobe's appearance in the top 10 vendors with the most vulnerabilities found list is a good indication of the focus vulnerability researchers now have on popular applications. Both the OSs themselves as well as common server applications were hardened against vulnerabilities in recent

Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) to measure their severity and potential user impact.

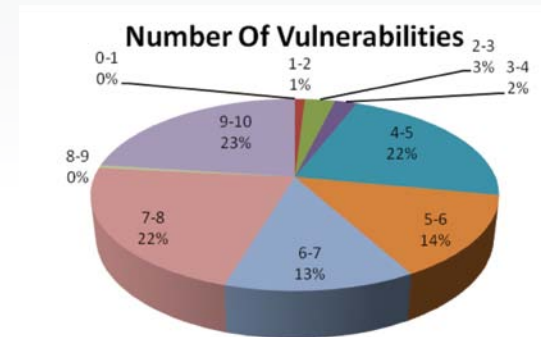


Figure 26. Vulnerability shares in terms of CVSS

years, as awareness of vulnerabilities as a security problem grew. This focus on third-party applications increases the risk for typical end users, as they tend to ignore third-party programs as posers of security risks. In addition, no common patching platform like Windows Update is provided, raising the risk of having vulnerable versions on user systems.

Trend Micro Technology and Protection

The Trend Micro™ Smart Protection Network™ infrastructure delivers advanced protection from the cloud, blocking threats in real-time before they reach users. By continuously processing the threat intelligence gathered through its extensive global network of honeypots, customers, and partners, Trend Micro delivers automatic protection against the latest threats and provides "better together"

security, much like an automated neighborhood watch that involves the community in protecting others. Because the threat information gathered is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer's personal or business information is always protected.

Trend Micro Smart Protection Network

By the end of 2010 the Smart Protection Network:

- **Processed 45 billion queries every 24 hours**
- **Blocked 5 billion threats daily**
- **Processed 3.2 terabytes of data daily**
- **Saw an average 102 million users connected to the network each day**

Trend Micro Smart Protection Network uses patent-pending “in-the-cloud correlation technology” with behavior analysis to correlate combinations of Web, email, and file threat activities to determine if these are malicious. By correlating the different components of a threat and continuously updating its threat databases, Trend Micro has the distinct advantage of being able to respond in real time, providing immediate and automatic protection from email, file, and Web threats.

Another key component of the Trend Micro Smart Protection Network is integrated smart feedback that provides continuous communication between Trend Micro products as well as the company’s 24/ 7

threat research centers and technologies in a two-way update stream. Each new threat identified via a single customer’s routine reputation check, for example, automatically updates all of Trend Micro’s threat databases around the world, blocking any subsequent customer encounters of a given threat.

Differentiating Trend Micro from other security organizations, and in demonstration of the Company’s data protection expertise, by the end of 2010, the Smart Protection Network was seeing 45 billion queries every 24 hours, blocking 5 billion threats and processing 3.2 terabytes of data on a daily basis. On average, 102 million users were connected to the network each day.

Trend Micro Solutions and Services

Trend Micro Enterprise Security Solutions

Trend Micro Enterprise Security Solutions refer to a tightly integrated offering of content security products, services, and solutions that take full advantage of the Trend Micro Smart Protection Network. Optimized to deliver immediate protection, Trend Micro Enterprise Security also dramatically reduce the cost and complexity of security management.

Trend Micro SecureCloud™

Now available for early adopters of cloud computing, Trend Micro SecureCloud is a hosted key management and data- encryption solution designed to protect and control confidential information that users deploy in public and private cloud-computing environments.

Trend Micro™ Worry-Free™ Business Security

Designed specifically to fit the needs of small businesses, Trend Micro Worry-Free Business Security protects user systems wherever they’re connected in the office, at home, or on the road. Powered by the Trend Micro Smart Protection Network, threats are detected faster to keep users’ data safe and security constantly updated.

Trend Micro™ Titanium™

Combining easy-to-use security with cloud-client technologies, Trend Micro Titanium blocks threats such as infected websites, phishing attacks, viruses and spyware before they can reach a users’ computer. State-of-the-art protection for user data is delivered while ensuring that computer performance is not impacted.

Advice for Businesses Adopting Cloud Computing Strategies

In March 2010, the Cloud Security Alliance (CSA) published “Top Threats to Cloud Computing V1.0” to help organizations better understand the risks related to cloud computing and to consequently make more informed risk management decisions when adopting cloud computing strategies. With the right approach and security solutions, public clouds can be just as secure as a typical traditional corporate data center. We recommend that organizations provide their own layers of protection in addition to that afforded by cloud service providers.

- **Encrypt all sensitive data.** The information that is exclusive to and owned by your organization should always be protected. The OS and applications are less important here, as in the cloud, these are typically just standard images that are simply recycled to form a master image upon shutdown. The information that is proprietary to you or that you have collected from customers and business partners are those that you have a legal obligation to protect.
- **Ensure that your firewall, intrusion prevention system (IPS), and intrusion detection system (IDS) protect each VM (virtual machine) separately.** Particularly in a public cloud environment, the other VMs running on the same physical hardware as yours should be considered hostile. The firewall at the cloud service provider’s perimeter cannot help you here.
- **Only decrypt data within the secure container you established for your VMs.** Ensure that you check for tampering and data-stealing malware before decrypting your data.
- **Make sure that you are in control of your encryption keys.** Trend Micro offers two products—Deep Security™ and SecureCloud—which when layered together can achieve the four recommendations above and counter the threats identified.

Advice for Small and Medium-Sized Businesses Adopting Cloud Computing Strategies

Just like enterprises, small and medium-sized businesses (SMBs) also need protection from all kinds of threats. To make sure your data stays safe from abuse and misuse, keep the following best practices in mind:

- Use effective solutions to protect your business.
 - o To protect your company network, deploy solutions that use cloud-based protection. Technologies like the Trend Micro Smart Protection Network combines Internet-based or in-the-cloud technologies with lighter-weight clients to help businesses close the infection window and to respond in real time before threats can even reach a user’s PC or can compromise an entire network. By checking URLs, email messages, and files against continuously updated and correlated threat databases in the cloud, you always have immediate access to the latest protection wherever you connect.
 - o Phishing poses a significant threat for organizations. Phishing sites can compromise your brand and/or your company’s image as well as your ability to keep your customers’ confidence while conducting business over the Internet. Protect your employees and customers by procuring all brand-related and look-alike domain names.

o Stay ahead of threats by reading security-related blogs like the TrendLabs Malware Blog and related information pages like the Threat Encyclopedia and social networks such as Trend Micro's Twitter account to be warned about and to educate users who may otherwise be drawn to sites under false pretenses.

o Educate your employees about how cybercriminals lure victims to their schemes. Make use of threat information provided on security vendor sites like TrendWatch.

o Try downloading tools such as the Trend Micro Threat Widget from this page to help raise awareness.

• Safeguard your customers' interests.

o Standardize company communications and let your customers know about your email and website policies. This way, you can help your customers better identify legitimate messages. Avoid sending phishy-looking email messages by following these guidelines:

- Do not request personal information through email.
- Personalize email messages when possible.
- Do not redirect to another domain from the URL provided to customers.
- Do not rely on pop-up windows for data collection, especially those with no address bars or navigational elements.

• Do not use instant messaging or chat applications when talking to customers unless they initiate the communication.

• Be explicit in the detail of communications that require the immediate action or attention of recipients.

• Establish and implement effective IT usage guidelines.

o Just as you would never leave your front door unlocked when you are not home, you must take the same precautions with your system to make sure your business stays protected. Protecting your business requires you to educate yourself and your employees about safe cybersecurity practices. A comprehensive set of IT usage guidelines should focus on the following:

• **Prevention.** Identify solutions, policies, and procedures to reduce the risks brought about by attacks.

• **Resolution.** In the event of a computer security breach, you should have plans and procedures in place to determine what resources you will use to remedy a threat.

• **Restitution.** Be prepared to address the repercussions of a security threat with your employees and customers to ensure that any loss of trust or business is minimal and short-lived.

Advice for End Users

No system is safe from cybercriminals. Enterprises and SMBs are not the only ones at risk, so are end users. To stay safe in the current threat landscape, keep these top end-user computing tips in mind:

- **Keep your PC current with the latest software updates and patches.** Apply the latest security updates and patches to your software and OS and enable automatic updates when possible. Since cybercriminals typically take advantage of flaws in software to plant malware on your PC, keeping your software current will minimize your exposure to vulnerability exploits.
- **Protect yourself and your PC.** If you receive an email requesting personal or confidential information, do not respond or provide the information by clicking links to potential phishing pages or by calling given phone numbers. Legitimate organizations such as credit card companies and banks will never request this information via email.
- **Beware of unexpected or strange-looking email and instant messages (IMs) regardless of sender.** Never open attachments or click links in dubious-looking email and IMs. If you trust the sender, scan attachments before opening them. Never provide personal information in your email or IM responses.
- Regularly check your bank, credit, and debit card statements to ensure that all transactions are legitimate.

- **Beware of Web pages requiring software installation.** Scan programs before executing them. Always read the end-user license agreement (EULA) and cancel if you notice other programs being downloaded in conjunction with your desired program.
- **If the content of an email message sounds too good to be true, it probably is.** If you suspect an email is spam, delete it immediately.
- Reject all IMs from people you do not know.
- When shopping, banking, or making other transactions online, make sure the website address contains an s as in <https://www.bank.com>. You should also see a lock icon in the lower right area of your Web browser.
- Choose secure passwords.
 - o Use a combination of letters, numbers, and symbols and avoid using your first and last names as login name.
 - o **Avoid using the same password for all your login needs.** Do not use the password you use for social networking sites as your online banking password.
 - o Change your password every few months.

About Trend Micro

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com

Copyright© 2011 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and the Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated, TrendLabs is a service mark of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.