Report

McAfee Threats Report: Third Quarter 2010

By McAfee® Labs™

Looking at computer threats from quarter to quarter remains a busy experience for us at McAfee Labs. Through the first three quarters of the year we have analyzed and catalogued more threats than in all other years combined, and the growth in both volume and sophistication of malware and attacks shows no signs of slowing.

This quarter we have seen quite a bit of activity from old nemeses such as Koobface, fake anti-virus software, password-stealing Trojans, and AutoRun (a.k.a. USB-based) malware. In this report we will look at the top malware threats around the globe. We observed significant development in one of the most dangerous threats we face: the Zeus robot network. Threats to mobile devices are attracting more attention, and we now see the Zeus bot is also riding the mobile wave. In many ways these new threats will mirror many of the established threats as they make their way to new platforms—because the human element, with its constant susceptibility to social engineering, remains the same.

Spam volumes are still quite high, and the geographical and subject breakdown by region is as fascinating as always this quarter. We will also look globally at botnets.

We saw growth in the number of malicious websites and continued abuse of search-engine results. SQL-injection attacks allowed China to reclaim the dubious honor of Number 1 source. Search engine and term abuse continues to mirror the news of the day, and we saw many developments in the areas of cybercrime and hactivism—specifically in stolen identities and cybercrime toolkits.

However, all these attack vectors take a backseat to the quarter's most significant threat: Stuxnet. This advanced worm took center stage amid rumors of government conspiracies and cyberwarfare.

When we look back, this year might well become known as the Year of the Targeted Attack, due to narrowly aimed malware such as Stuxnet and Operation Aurora. In the mean time, let's see what the threat landscape in the third quarter held for us.

Table of Contents

Botnets	4
Spam	6
Stuxnet: a Targeted Attack Runs Rampant	8
Malware	10
Zeus	14
Web Threats	16
Search Engine, Term, and Twitter Abuse	19
SQL Attacks and Vulnerabilities	20
Cybercrime	22
Hacktivism	23
Actions Against Cybercriminals	24
About the Authors	25
About McAfee Labs™	25
About McAfee, Inc.	25

Botnets

Botnet distributions change from quarter to quarter. This period the clear leaders were Rustock and Cutwail. Historically the latter has been responsible for more spam runs than any other, and it also holds the record for the most infected hosts. Earlier this year Cutwail bots engaged in distributed denial-of-service attacks against more than 300 websites, including the United States government departments of the Central Intelligence Agency and Federal Bureau of Investigation as well as Twitter and PayPal. In spite of these attacks, there has been much debate that they may have not been intentional. On purpose or not, Cutwail's reach illustrates the multifaceted nature of botnets in the arsenal of today's cybercriminals.

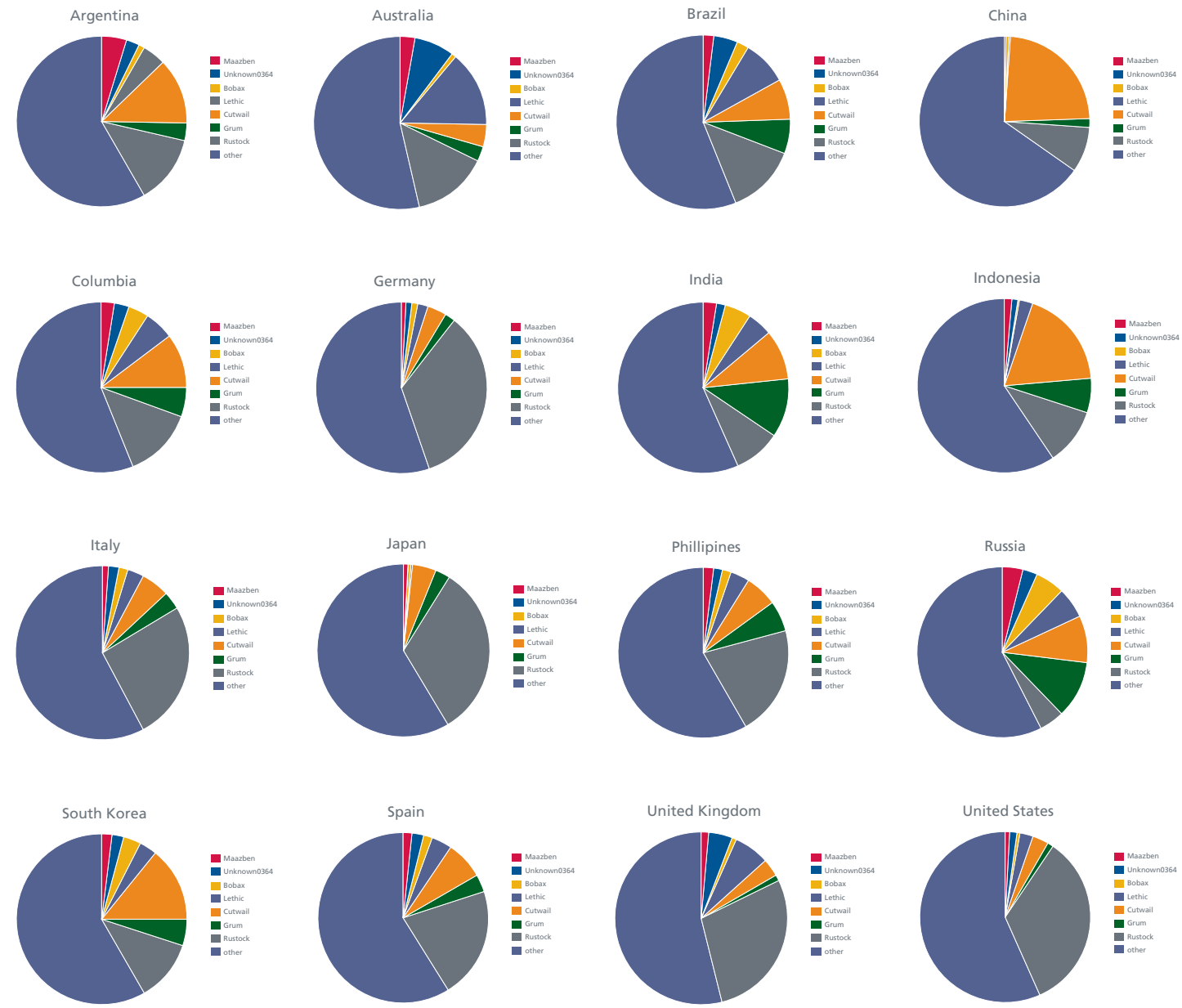
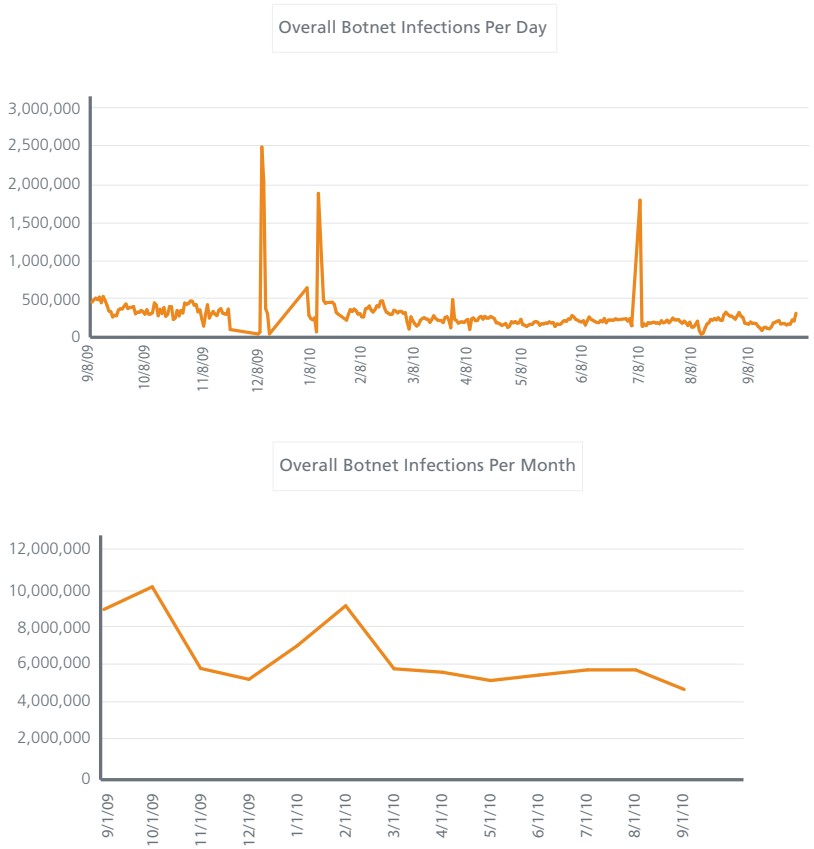


Figure 1: Botnets vary in impact among countries. Nonetheless, Rustock and Cutwail demonstrate their worldwide reach.

Although several days show spikes in activity, McAfee Labs finds that new bot infections have been consistent at below 500,000 per day. The monthly chart shows that we see on average about 6,000,000 new botnet infections per month.



Figures 2a and 2b: Daily new botnet infections have remained generally consistent during the past year, with a slight downward trend. Monthly averages, on the other hand, have dropped almost by half.

Spam

Although continuing as one of the most persistent threats we face, spam has continued its overall decrease in volume this quarter, both globally and in local geographies. With the exceptions of Belarus, Greece, Indonesia, and Russia, all the countries that McAfee Labs currently tracks have shown drops in spam volumes:

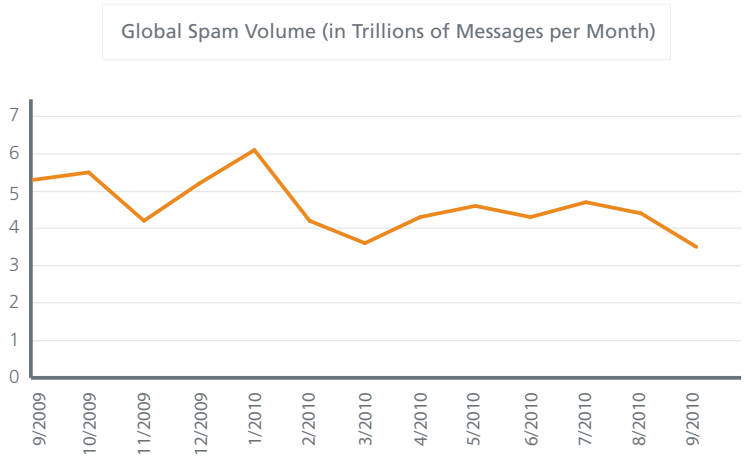


Figure 3: Spam, though remaining high, continues its overall decline this quarter.

Although spam volumes as a whole are declining, the threats of identity theft, phishing attacks, and malicious links from spam remain as serious as ever. Stay updated and informed!

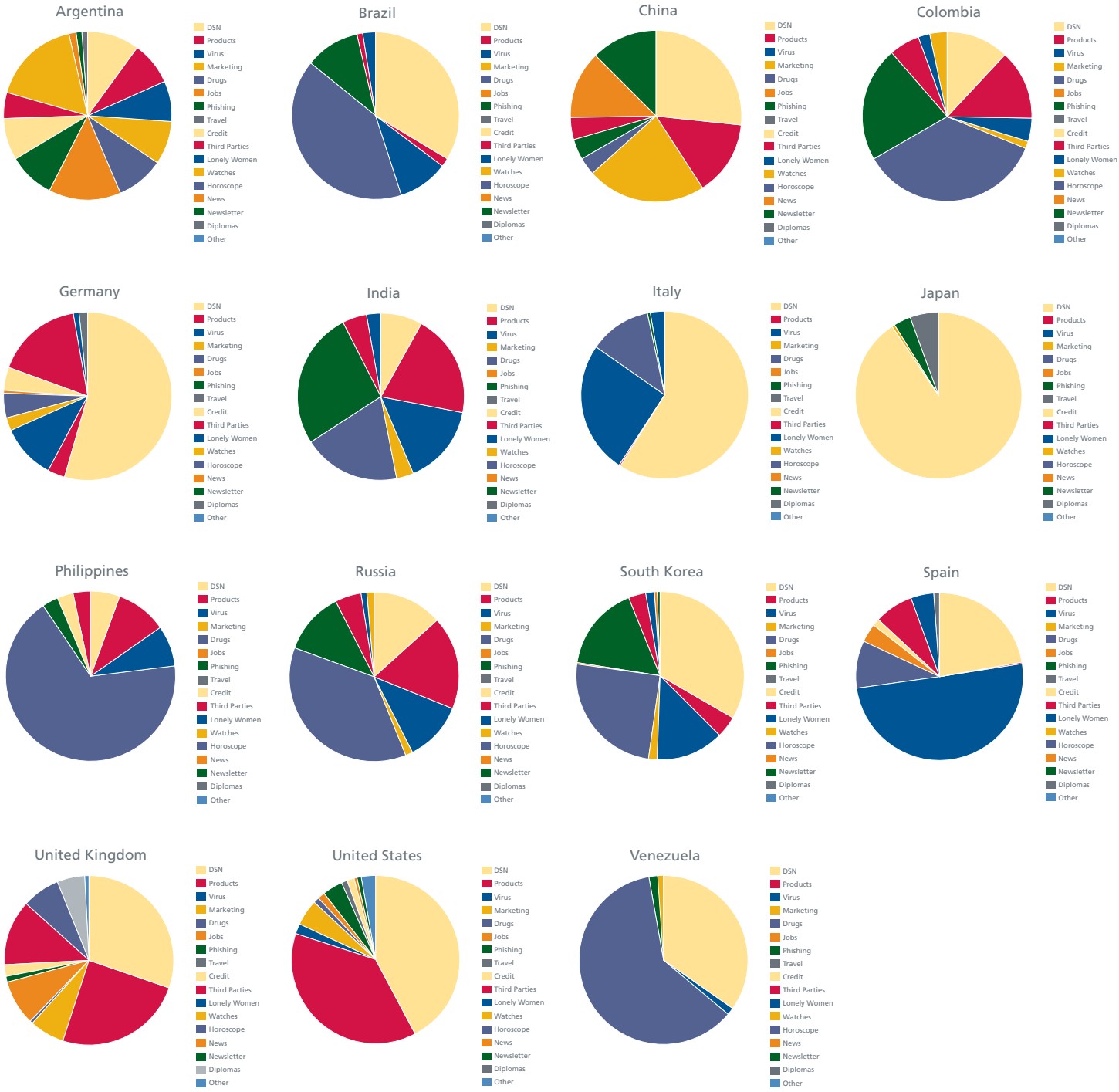


Figure 4: Spam subjects vary considerably among countries. These charts show the relative frequency of the leading topics originating within each nation. These subjects do not represent all spam traffic, only the most popular. DSN stands for Delivery Status Notification, bogus messages that claim your email has failed to reach its destination.

Stuxnet: a Targeted Attack Runs Rampant

The discovery of the Stuxnet worm in July marked the beginning of a new era. When Stuxnet was first detected, we quickly realized that it checked for the presence of a particular process control system (PCS), a PC-based routine for operating, monitoring, and controlling industrial machines. We initially assumed Stuxnet was written for industrial espionage. This view was strengthened by Stuxnet's exploitation of multiple zero-day vulnerabilities across all versions of Windows; these actions alone could be worth hundreds of thousands of U.S. dollars on the black market.

Stuxnet was the first malware that was publicly reported to specifically attack industrial control systems, which can also be interpreted as an attack against critical infrastructure. PCS software can run anything from a pizza oven to an oil rig. This attack caused many companies to finally evaluate application control solutions as a possible way to secure these vital systems, in which running traditional anti-virus (AV) software is out of question. In spite of the anxiety, the turmoil around Stuxnet soon stopped.

In September, however, more detailed analyses found that Stuxnet is more than just a spy worm, it is a weapon written to sabotage a specific industrial installation. What was the target? Considering how Stuxnet was written, in particular its manipulation of the programmable logic device it targets after making absolutely sure the device is the one installation it is meant to hit to avoid collateral damage, and using four zero-day exploits to spread and escalate privileges to administrator rights, it is clear that the attackers had a lot of resources at their disposal. Researchers also determined that Stuxnet was released at least as far back as June 2009, and probably before that. As many of the first infected systems were reported in Iran, some named the gas centrifuges at the uranium enrichment plant in Natanz as the target. Others named the nuclear reactor at Bushehr. The actual target is impossible to verify, but in early October the Iranian intelligence minister Heidar Moslehi said "The enemy had sent electronic worms through the Internet to undermine Iran's nuclear activities."[1]

Speculation still runs wild regarding who is behind the attack. A registry key set as an infection marker with a value of 19790509 could be interpreted as a date, and on that date a Jewish-Iranian businessman was executed, prompting a mass exodus of Jews from Iran.[2] But this can be highly misleading or even a false path. With the help of Google, you can find a significant event for any given date.

In one major goal of the attack the attackers failed miserably: preventing collateral damage. The self-replicating functionality—propagating via USB devices, network shares, and exploiting vulnerabilities—works well. Too well, actually, Stuxnet is completely out of control, having infected thousands, if not millions, of computers of unintended victims. Today infections are reported from all over the globe, from companies and home users. The damages Stuxnet causes will certainly dwarf those intended by its authors.

And let's not get too thrilled by the cyber–James Bond theme surrounding Stuxnet. The incident points to some very serious problems:

- A lot of critical systems are open to attack, even if they are on separate networks and not connected to the Internet
- Attacks against industrial control systems are a reality
- Security researchers have warned that such high-profile targeted attacks will make use of zero-day vulnerabilities, which someone is buying on the black market. Now we have proof of this.

Securing critical systems against future targeted attacks must be a priority for enterprises and governments alike. Application control solutions may be the key technology to achieve this.

1. "Iran says several held for spying on nuclear sites," Reuters. http://www.reuters.com/article/idUSTRE6911XH20101002
2. "Stuxnet code hints at possible Israeli origin, researchers say," Computerworld. http://www.computerworld.com/s/article/9188982/Stuxnet_code_hints_at_possible_Israeli_origin_researchers_say

Maps created by McAfee Global Threat Intelligence technology illustrate the breadth and concentration of the Stuxnet infections.

Figures 5a, 5b, 5c: Stuxnet infections were first found in Iran, but today India suffers from the greatest concentration of attacks. Source: McAfee Global Threat Intelligence.

Malware

In spite of advances in other threat vectors, malware continues to be the biggest threat facing corporate and consumer users and the object of most of McAfee Labs research and analysis. So far this year we have identified more than 14 million unique pieces of malware. That's well over one million more malware than at the same time last year; thus, even though the increase has slowed this quarter, the growth continues.

When we look at daily malware growth during the last several years, the trend becomes even more pronounced: In 2007 we identified on average more than 16,000 new pieces of malware per day; in 2008 the figure jumped to more than 29,000 per day. Last year our daily detections rose to 46,000 per day, and in 2010 we have reached a frightening 60,000 new identifications per day.

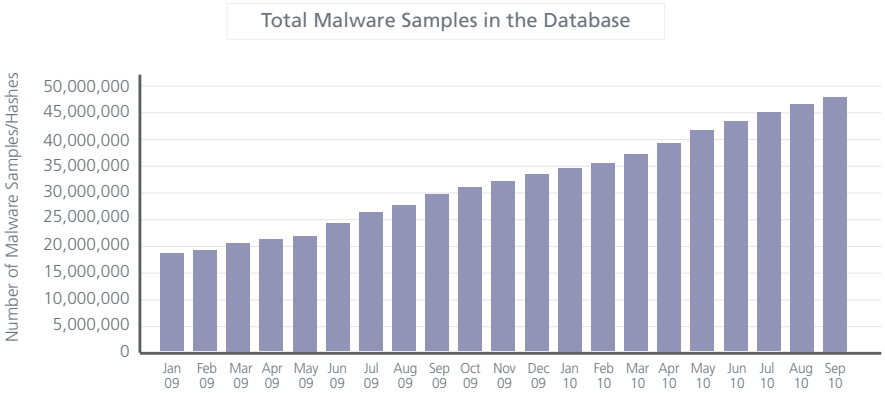


Figure 6: Total count of unique malware (including variants) in the McAfee Labs database.

The implications are clear: Cybercriminals are here to stay and they are working hard to steal our money and data, both corporate and consumer.

This quarter's Top 10 malware around the world has a mix of many established standards, mainly in the form of password-stealing Trojans, AutoRun malware, and fake AV software. Quite a bit of adware and potentially unwanted programs have also joined the leaders. Two notables are Exploit-CVE2008-5353 and Exploit-ByteVerify. Both relate to Java vulnerabilities (though in very different ways) and are commonly encountered via malicious websites.

Rank	Top 10 Global Malware
1	Generic!atr
2	Generic.dx
3	W32/Conficker.worm!inf
4	FakeAlert-FakeSpy!env.a
5	Exploit-CVE2008-5353
6	GameVance
7	Generic PUP.x
8	Adware-HotBar.b
9	Exploit-ByteVerify
10	Adware-Url.gen

Most of the malware in the Global Top 10 supports cybercrime, which gives us a largely profit-driven threat landscape. Users must continue to be vigilant and informed in their surfing and downloading habits!

Looking a bit closer into each major region reminds us of the local variety of malware:

Rank	Africa
1	Generic!atr
2	Generic.dx
3	W32/YahLover.worm.gen
4	New Win32
5	W32/Sality.gen

Rank	Asia
1	Generic.dx
2	Generic!atr
3	W32/Conficker.worm!inf
4	New Poly Win32
5	Adware-BDSearch

Rank	Australia
1	Generic!atr
2	Exploit-CVE2008-5353
3	Generic.dx
4	W32/Conficker.worm!inf
5	Adware-Url.gen

Rank	Europe
1	Generic!atr
2	Generic.dx
3	Exploit-CVE2008-5353
4	W32/Conficker.worm!inf
5	Adware-Url.gen

Rank	North America
1	Exploit-ByteVerify
2	Generic!atr
3	Exploit-CVE2008-5353
4	GameVance
5	Generic.dx

Rank	South America
1	Generic!atr
2	W32/Conficker.worm!inf
3	Generic.dx
4	W32/Autorun.worm.zf.gen
5	W32/Sality.gen

Delving a bit deeper into some of the specific malware threats that we deal with, we continue to see a dynamic landscape. Depending upon the day and the quarter, we might find Koobface, fake AV, or password-stealing Trojans in the lead. Parasitic malware continues to grow in prevalence due to the continued proliferation of USB-based devices. This last class of malware is unique in that it can be quite destructive to data as well as to the environment it replicates in.

The clear leader this quarter has been password-stealing Trojans (commonly called PWS). Many types of malware fall into this category. (Even Zeus, which we shall discuss soon, is often detected as a PWS.) This area of malware makes cybercriminals a tidy sum of money as they collect a variety of confidential information, such as usernames, banking credentials, and gaming accounts, which are then sold on the criminal underground.

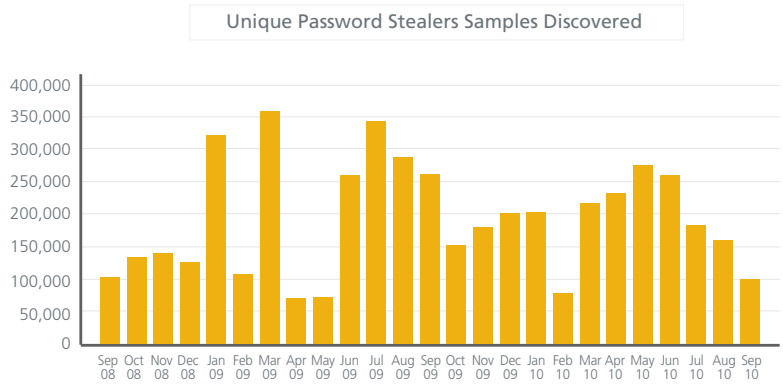


Figure 7: Password-stealing Trojans primarily target data in victims' bank accounts.

It should come as no surprise that fake anti-virus software continues to have a strong quarterly presence. This is a popular area for today's cyberscammers, as these "products" are designed to scare unsuspecting users into buying bogus technology through fake detections and removals.

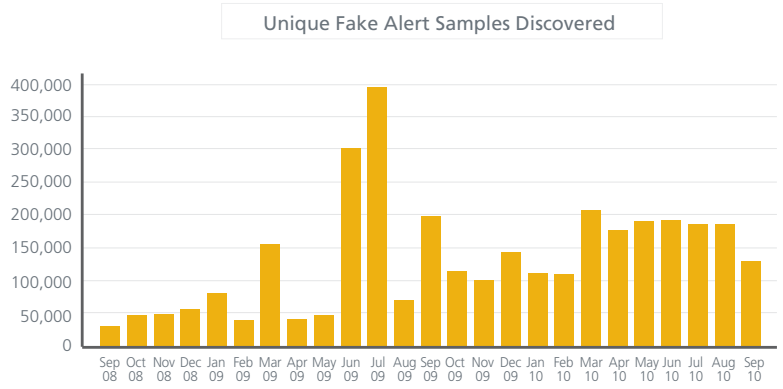


Figure 8: Fake security software samples peaked in the third quarter of 2009, but the overall numbers remain high for this lucrative form of cybercrime.

Although both AutoRun malware and Koobface have leveled off a bit, users must remain vigilant. Koobface, with its focus on Facebook users, will be with us for a long time as social media and social networking sites continue to grow in use and business applications.

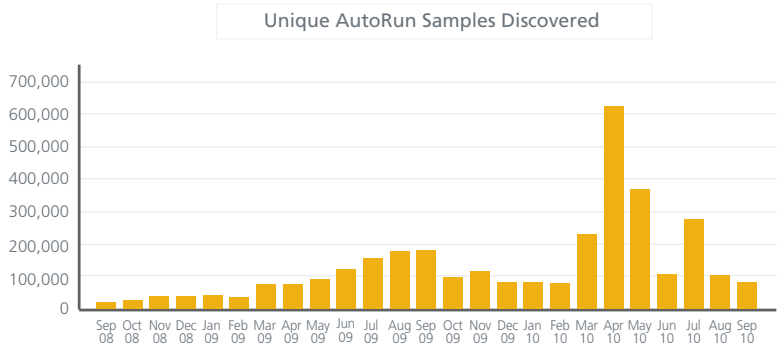


Figure 9: AutoRun worms took a leap in July, but then returned to typical levels.

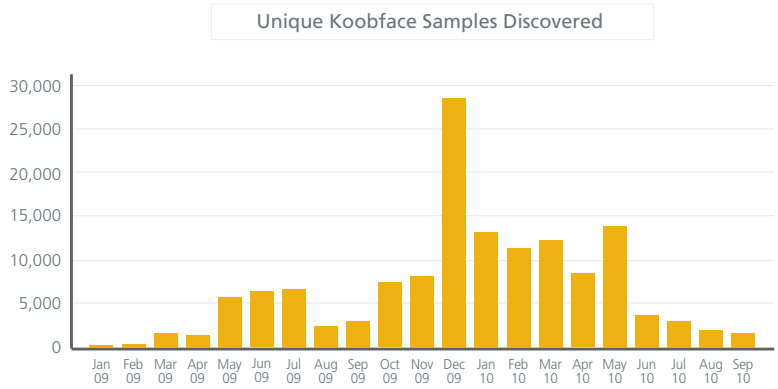


Figure 10: New Koobface variants dropped off sharply since peaking in December, but the malware continues to plague Facebook users.

Zeus

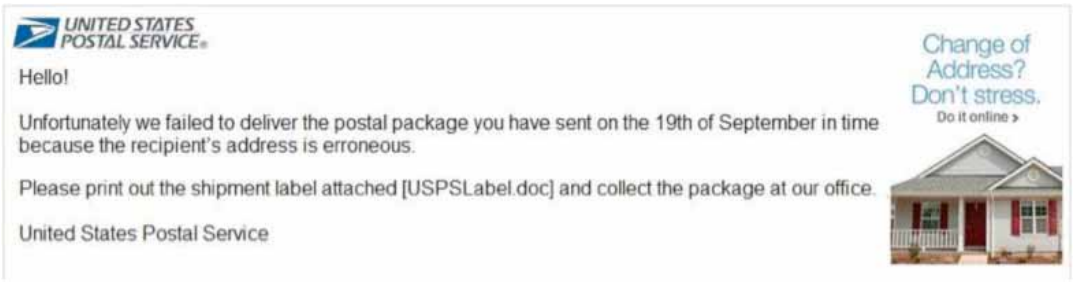
As sophisticated malware goes, Zeus might just be in a class by itself. Also called Zbot or PWS-Zbot, Zeus is usually spread via download or phishing attacks and sites. Although technically a Trojan, Zeus has many bot features and functions. McAfee Labs has seen some recent changes to Zeus, a well-developed and maintained threat, that bear discussion.

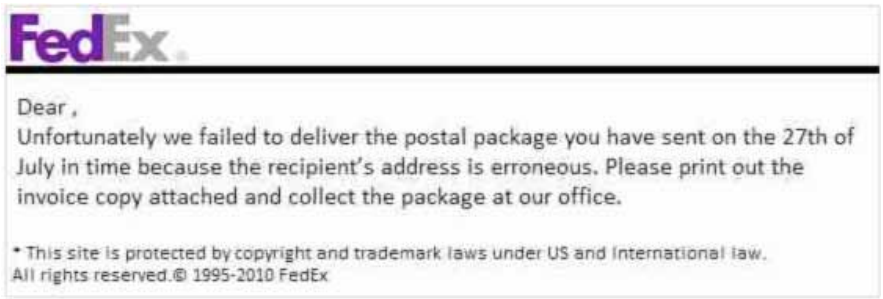
During this quarter, McAfee Labs noticed that the Zeus crew has been quite active. We saw several email campaigns that tried to deliver either Zeus itself or the Bredolab Trojan, which will download several kinds of malware.

Some of the lures for these spam campaigns exploited the following brands:

- eFAX
- FedEx
- Internal Revenue Service
- Social Security Administration
- United States Postal Service
- Western Union

We observed cybercriminals using an interesting tactic to bypass antispam technologies by using graphics instead of text in an email. Although some spam campaigns such as the ones targeting the SSA or IRS still use text in emails, the following examples employ the graphical touch:





Figures 11a, 11b, 11c: Zeus campaigns switched from text to graphics in emails to avoid antispam measures.

We looked at several Zeus campaigns this quarter to learn which countries sent the most spam:

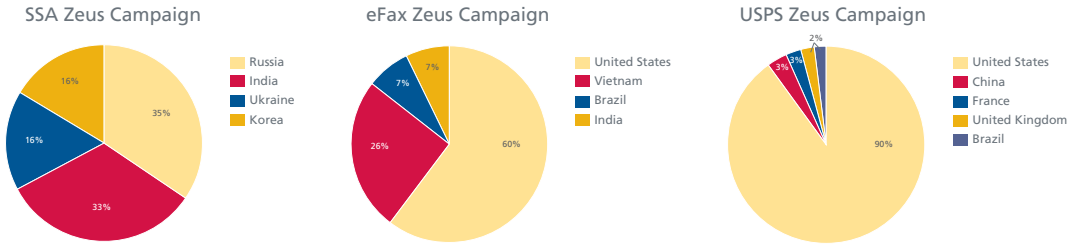
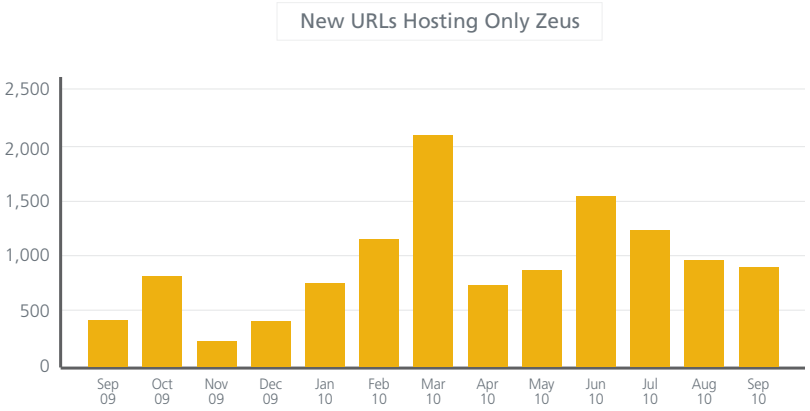


Figure 12: Several leading Zeus attacks this quarter originated in just a few countries.

McAfee Labs has also encountered many new URLs that specifically host Zeus binaries.



Figures 13: Sites hosting exclusively Zeus malware show cyclical increases.

Going mobile

Zeus recently increased its reach by taking the mobile approach. Cybercriminals know that many financial institutions use a two-factor authentication method. A common and cheap one is to use SMS for the second authentication.

Here's one way it can work:

- User logs on the online banking website
- User tries to make a money transfer
- Bank asks for additional code
- Code is sent to user's phone via text message (SMS)
- User enters the code to validate the transaction

Because Zeus has access to the computer, it can do just about anything it wants. One of Zeus' achievements was to create a way to intercept SMS messages so it can validate *its own* transactions. To achieve this, it had to create a way to get onto the mobile device that received the SMS code.

Next the Zeus crew needed to identify the online banking user's cell phone model. This is actually easy: Because Zeus controls the computer, in the same way it can inject additional fields into an online banking webpage to gather passwords, it can request additional data such as phone number and phone model. After gathering this information, the Zeus controller can send a text message to the

victim, with a URL that the user would have to access to download a security add-on to the mobile phone. The download is a malicious file that will intercept the SMS message received and send it to the Zeus controller. Thus when a user receives a text message from the bank with the additional code, the criminal can perform the full bank operation.

The malicious file will currently work only on BlackBerrys and Symbian-based phones, and originally had the names *cert.jad*, *cert.sis*, and *sertificate.jad*.

All mobile phone users should investigate security technologies for their devices in the same way they consider their security for their computers. Cybercriminals will look for victims in all types of financial transactions.

Web Threats

Many users do not realize the risks that the growth in Internet sites yields. Thousands of new sites come online every day. Many of these are very useful. Many others, however, are suspicious or downright malicious. This dichotomy leaves most users with a serious knowledge gap: How do we know which are safe and which are malicious? Using our Global Threat Intelligence capabilities, McAfee Labs can identify and classify sites, and inform and protect users in real time against the onslaught of daily web threats.

We continue to see many new malicious websites spring up every day. The rapid changes are often tied to popular news and daily events around the world. Cybercriminals follow global trends, and prepare their websites in anticipation of user activity.

This quarter we have seen some interesting malicious website activity. These sites exist for malicious purposes: browser exploits, malware downloads, botnet control, malware "phone home" and drop zones, etc. The pronounced spike in July is a reflection of Stuxnet phoning home. The spike in the middle of September had to do with a series of URLs attacking some very specific targets. We also noted significant Koobface activity at this time, as well as other malicious URLs being served by legitimate sites.

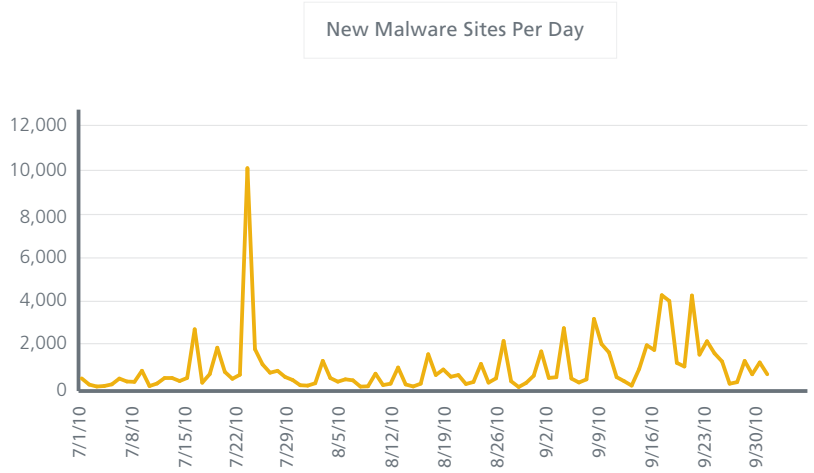
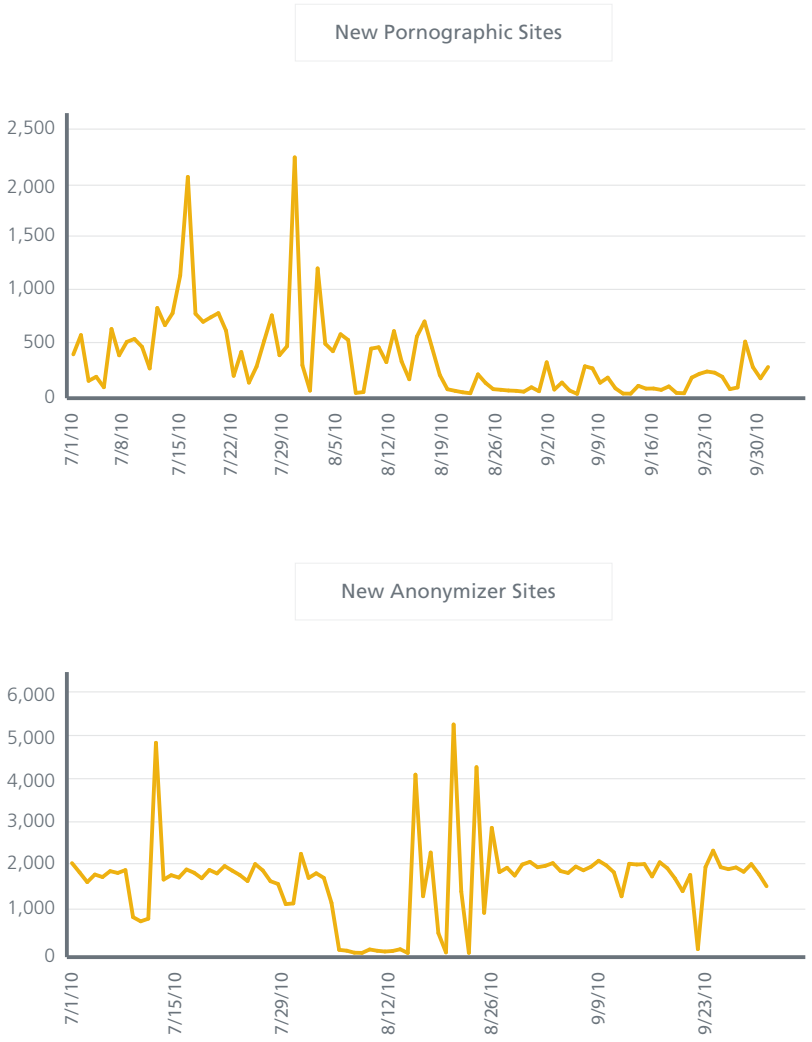


Figure 14: McAfee Labs sensors discover daily hundreds to thousands of new sites that host malware. Stuxnet was responsible for the leap in July.

New pornographic sites and anonomizer sites have remained steady throughout the quarter.



Figures 15a, 15b: The emergence of new sites hosting pornographic materials held steady in the second part of the quarter. Sites that allow anonymous browsing also showed a relatively flat line with some dramatic exceptions. Anonymizers can offer useful legitimate services, but they are often misused by cybercriminals.

We have seen a marked increase in new phishing sites this year overall and during this past quarter. These attacks have been much more targeted than in previous years and thus more successful.

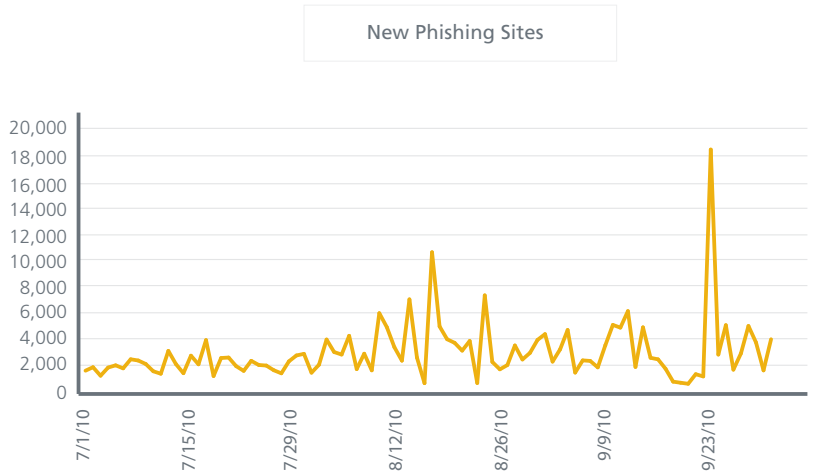


Figure 16: Until April this year new phishing sites discovered daily averaged fewer than 1,000. Since then the average has more than doubled.

What are all those websites doing? Let's take a look at our Top 15 categories, courtesy of McAfee Labs. We see that Instant Messaging has moved up to Number 13 in our analysis—IM has never previously been in the top 20. This position shows the growing expansion of this type of communications technology as well as the overall trend toward more social media.

Top 15 Website Categories	Number of Sites
Malicious Sites	14,475,580
Residential IP Addresses	6,040,787
Spam URLs	4,085,439
Pornography	2,815,319
Content Servers	2,511,339
Business	2,510,899
Phishing	1,474,321
Parked Domains	1,215,048
Travel	1,140,018
Anonymizers	997,863
Online Shopping	979,092
Real Estate	873,159
Instant Messaging	842,263
Government/Military	829,381
Marketing/Merchandizing	826,286

Search Engine, Term, and Twitter Abuse

Cybercriminals and scammers are in many ways just as clever and insightful into human behavior as good marketers are. One of the reasons they are so successful at scams and malware distribution is the way they conduct "market research." One of the genuine powers of social networking and Web 2.0 technologies is the ability to engage in global, dynamic conversations. Twitter in particular makes following terms, events, celebrities, and trends particularly easy. The flip side of these technologies is that they are also simple to abuse and mine for intelligence on potential victims.

Figure 17: Turkish hacktivists defaced websites and Facebook accounts to protest Israel's action against the Gaza Flotilla.

Data like this tells the wily social engineer or scammer many things, but most important it tells them what users are tweeting about right now. This information is truly powerful as it allows an attacker to poison the most popular Twitter terms and trends as they are being discussed. Combined with a URL-shortening service such as bit.ly, which hides website destinations, this data becomes even more effective:

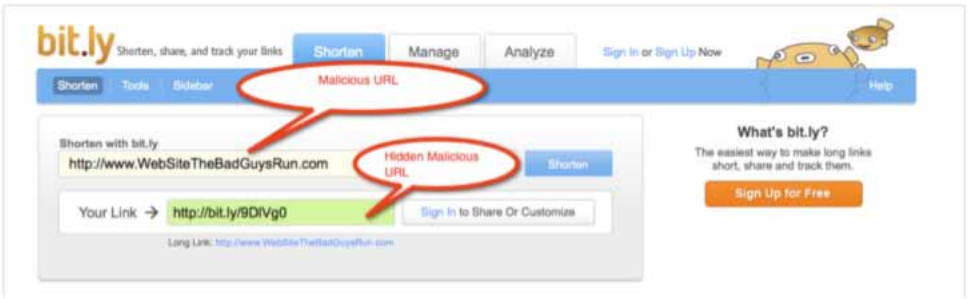


Figure 18: Clever cyberscammers can take current topics and use them to lure victims via hidden URLs.

McAfee Labs tracks this vector of abuse closely, and we expect to see it continue to grow in use and sophistication. This vector was also a major driver in the development and recent release of our own Secure URL Shortening Service, at http://mcaf.ee, which allows users to create and distribute safe, shortened URLs that are backed by McAfee Global Threat Intelligence.

Looking at the Top 250 Google Trends search terms abused this quarter reveals that cybercriminals latch on to many celebrities, weather events, disasters, TV shows, and music:

Figure 19: During this quarter 60 percent of top Google search terms returned malicious sites within the first 100 results.

Due to its success, ease of use, and implementation, we expect search engine and term abuse to continue for years to come. Users must consider how they surf, how they search, and how they look for news online.

SQL Attacks and Vulnerabilities

This quarter saw a significant change in the source of SQL-injection attacks we track. Last quarter the Number 1 source of SQL attacks was the United States, with China running a fairly close second. This quarter China has taken the top spot, with 54 percent of tracked SQL-injection attacks originating in that country. The United States is a distant second, at 24 percent.

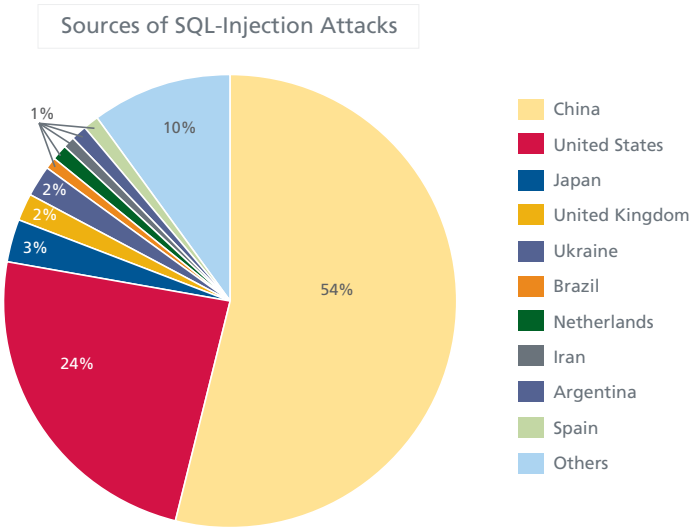


Figure 20: China and the United States are the usual leaders as origins of website attacks based on SQL injection. Other countries lag far behind.

In this quarter we also saw more than a few zero-day vulnerabilities exploited in the wild, some in very targeted attacks while others were much broader:

CVE-2010-2883—Adobe SING tag buffer overflow vulnerability: This zero-day attack was discovered in the wild by McAfee Labs researchers on September 7. This issue is unpatched at the time of writing this report and is being actively exploited. Adobe Reader Versions 9.3.4 and earlier are affected. Adobe is expected to release a patch in early October. The vulnerability was found using some new exploitation techniques to bypass data execution prevention and address space layout randomization.

CVE-2010-2884—Adobe Reader, Flash Player code execution vulnerability: Another critical zero-day vulnerability affected Adobe products. This one was discovered in the wild exploiting Adobe Flash Player Versions 10.1.82.76 and earlier on Windows, Mac, Linux, and Solaris. A patch fixing this issue was released on September 20. Flash users should upgrade to the latest player. The patch for Reader is expected in early October.

CVE-2010-2568—Windows Shortcut Icon Loading Vulnerability: This critical Windows vulnerability was discovered in the wild in July and was used to launch attacks on SCADA infrastructure. Attackers exploited a design flaw in the way shortcut (LNK) files are parsed. The vulnerability was patched by Microsoft as MS10-046. This threat later became a part of the well-organized attack Stuxnet. McAfee Labs is actively tracking this threat.

CVE-2010-2729—Print Spooler Service Impersonation Vulnerability: This zero-day vulnerability was found in the wild and was used by Stuxnet. This flaw was rated critical for Windows XP platforms. Microsoft quickly released a patch with security bulletin MS10-061.

CVE-2010-3332—ASP.NET Padding Oracle Vulnerability: We saw limited targeted attacks exploiting an information disclosure vulnerability in Microsoft ASP .NET. This flaw allowed attackers to tamper with encrypted data. Microsoft patched this vulnerability in MS10-070.

This short list shows that both Adobe and Microsoft products were popular victims of the top vulnerabilities exploited this quarter. Adobe products have been heavily targeted this past year. We expect these attacks to continue and eventually make their way to mobile platforms as well. There are many reasons for this: Chief among them is Adobe's huge popularity as a web-based application and the wide adoption of PDF and Flash technologies. Cybercriminals go where users go.

Cybercrime

Every day, information related to stolen, misappropriated, and sometimes even fake credit cards falls into the hands of cybercriminals. If they have no immediate use for the data, it ends up on the Internet where it is sold to other crooks. Various packages are typically offered: credit card "dumps," cards with card verification values, and bank logins.

Dumps are information electronically copied from the magnetic stripe on the back of credit and debit cards. Prices for this data vary, depending on the inclusion of the card's PIN.

Credit and Debit Card Dumps	Estimate of Prices (without PIN, with PIN) in U.S. Dollars							
	United States		European Union		Canada, Australia		Asia	
Visa Classic	15	80	50	150	30	150	50	150
MasterCard Standard		90		140		150	60	140
Visa Gold/Premier	30	100	70	160	35	160	120	150
Visa Platinum		110		170		170	150	170
Purchasing/Signature	35	120	100		40		100	
Business/Corporate	45	130		170		175	150	170
Infinite			130	190	45	200		190
MasterCard World		140						
AMEX Green	20							
AMEX Red			40					
AMEX Gold	40		70					
AMEX Platinum	50							

This quarter, five exploit kits, "crimeware" if you like, made the headlines. They can be used to create botnets via sets of precompiled exploits that take advantage of software vulnerabilities.

Exploit Kits (Release)	Prices in U.S. Dollars	Description
Zombie Infection Kit (July)	1,000	New Russian kit contains at least 10 package exploits, including: • Windows Help Center (HCP) CVE-2010-1885 • Java Web Start Argument Injection CVE-2010-0886
Phoenix v2.3r (August)	2,200	The Phoenix Exploits Kit first appeared in 2007 and receives regular updates. Today it includes 15 exploits, with 5 from 2010: • Adobe Reader LibTiff CVE-2010-0188 • Java SMB CVE-2010-0746 • IE iepeers CVE-2010-0806 • Adobe PDF SWF CVE-2010-1297 • Windows Help Center (HCP) CVE-2010-1885
CrimePack v3.1.3 (July)	400	CrimePack appeared in 2009. Among 14 exploits, 4 are from 2010: • IE iepeers CVE-2010-0806 • Java getValue CVE-2010-0840 • JRE toolkit cmd exe CVE-2010-1423 • Windows Help Center (HCP) CVE-2010-1885
SpyEye v1.2 (April)	Kit for 500–1,000	Created by Gribodemon, v1.0 came to market in December 2009. Version 1.2 is a serious Zeus competitor.
Zeus	Kit for 3,000–4,000. Must include add-ons and plug-ins from 500–10,000	The most important news this quarter is the appearance of Zitmo (Zeus in the Mobile). We also saw the first samples of v2.1.

Hacktivism

When cybercrime moves into the political realm, we call it hacktivism.

Country/Target	Date	Description
Philippines	August 27	On the same day that the Philippine Information Agency homepage was defaced, the official website of the provincial government of Bulacan was breached by another hacker with a more pointed political message. The attacker requested an apology and investigation into the August 23 hostage-taking incident that killed several residents of China's Hong Kong Special Administrative Region.[3]
France	July 14	Taking advantage of Bastille Day, hacktivists cloned the French Foreign Ministry website. The bogus site stole the logo and style and many of the video contents of the official site. The lead video on the hoax site was a film of a young, pompous woman in glasses, sitting in front of French and E.U. flags.
Worldwide	September 9	An unsophisticated mass-mailer, W32/VBMania@MM, spread a link to a malicious SCR file that was disguised as a PDF. Much of the worm's code was identical to a piece of malware that was released last month, and both worms refer to a Libyan hacker who uses the name Iraq Resistance and who has been trying to form a hacking group called Brigades of Tariq ibn Ziyad. According to a Google translation of a 2008 post announcing the group, its goal is "to penetrate U.S. agencies belonging to the U.S. Army," Iraq Resistance said.
Japan	September 15	Japan suspected Chinese hackers of launching distributed denial-of-service (DDoS) attacks against its Defense Ministry and National Police Agency websites in protest over Tokyo's handling of the collisions between a Chinese fishing boat and Japan Coast Guard patrol boats near disputed East China Sea islands.[4]
United States, India	September 17/18	A coordinated and massive DDoS attack took down the websites of both the Motion Picture Association of America and the Indian AiPlex Software firm. This protest was coordinated by antipiracy activists in revenge for the shutting down of Pirate Bay. (AiPlex told the Sydney Morning Herald that it used cyberattacks on sites hosting pirated movies on behalf of the film industry.[5]) Calling their offensive Operation Payback, the Internet collective Anonymous asked sympathizers to use Low Orbit Ion Cannon DDoS tools to initiate the attacks.
Burma	September 27	Websites belonging to exiled Burmese media organizations have been hit with DDoS attacks on the anniversary of Burma's 2007 monk-led uprising.[6]

3. http://asiancorrespondent.com/tonyo-cruz-blog/hacker-leaves-angry-message-in-local-philippine-govt-website
4. http://mdn.mainichi.jp/mdnnews/news/20100918p2g00m0dm012000c.html
5. http://www.smh.com.au/technology/technology-news/film-industry-hires-cyber-hitmen-to-take-down-internet-pirates-20100907-14ypv.html
6. http://www.dvb.no/elections/mass-cyber-attack-paralyses-burmese-media/11932

Actions Against Cybercriminals

Law enforcement around the world continues to make strides in fighting cybercrime.

Country/Target	Date	Description
United States, Slovenia, Spain	July 28	Slovenian police identified and arrested the Mariposa botnet's suspected creator, a 23-year-old Slovenian citizen known as Iserdo.[7] The botnet surfaced in December 2008 and spanned an estimated 12 million computers across the globe. It grew to infect more than half of the Fortune 1,000 companies, as well as at least 40 major banks.
France	August 7	French police, acting on information from U.S. authorities arrested the notorious cybercriminal "BadB" at the Nice airport as he was boarding a plane to Moscow. BadB (Vladislav Anatolieviech Horohorin) was the founder of carder websites such as CarterPlanet, BadB.biz, and Dump.name. He allegedly became one of the world's biggest traffickers in stolen credit card and social security numbers. Horohorin has been added to a long list of defendants charged with participating in the coordinated US$9.5 million global heist against card processing company RBS WorldPay, in a revised federal indictment issued in Atlanta, Georgia, on August 28.[8]
Russia	August	Officers of the Moscow economic crime service along with colleagues from the K section with support from specialists of the information security group arrested the Winlock ransomware gang. Their malware disabled certain Windows components, rendering a PC unusable, and then displayed pornographic images. To unlock the code, victims had to send SMS messages that cost between 300 and 1,000 rubles (US$33.40).[9]
Romania	September	The Romanian Directorate of Investigations of Organized Crime and Terrorism arrested cybercriminal Liviu Mihail Concioiu. After he launched, in 2009, two phishing attacks against eBay employees and reached the client database, he targeted a thousand high-value eBay users with dedicated phishing emails. Concioiu has also been charged with creating fake ATM cards for Italian banks and withdrawing more than €300,000 from these accounts. These and other crimes created a total loss of US$3 million.[10]
United Kingdom, United States, Netherlands, Ukraine	September 27–30	This month saw the execution of numerous arrests and search warrants in multiple countries in one of the largest cybercriminal cases ever investigated: • Total FBI cases: 390 • Attempted theft: US$220 million • Actual loss: US$70 million • United States: 92 charged and 39 arrested • United Kingdom: 20 arrested and 8 search warrants • Ukraine: 5 arrested and 8 search warrants Using the Zeus Trojan, hackers in Eastern Europe infected computers around the world to secretly capture passwords, account numbers, and other data used to log into online banking accounts. With this information, the hackers, earning commissions, made unauthorized transfers of thousands of dollars at a time, often routing the funds to other accounts controlled by a network of "money mules."[11]

7. http://www.fbi.gov/pressrel/pressrel10/mariposa072810.htm
8. http://www.wired.com/threatlevel/2010/09/viktor-pleshchuk/#more-19031
9. http://www.itar-tass.com/eng/level2.html?NewsID=15445927&PageNum=1
10. eBay Spear Phisher Liviu Mihail Concioiu Arrested in Romania: http://garwarner.blogspot.com/2010/09/ebay-spear-phisher-liviu-mihail.html
11. http://www.fbi.gov/page2/oct10/cyber_100110.html

About the Authors

This report was prepared and written by Pedro Bueno, Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget, Craig Schmugar, and Adam Wosotowsky of McAfee Labs.

About McAfee Labs™

McAfee Labs is the global research team of McAfee, Inc. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based service McAfee Global Threat Intelligence. The McAfee Labs team of 350 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

15901rpt_quarterly-threat-q3_1010_fnl_ETMG