Report

McAfee Threats Report: Third Quarter 2011

By McAfee® Labs™

There is a concept in science and engineering referred to as the signal-to-noise ratio. Without getting too geeky, it is defined as the ratio of signal power to noise power, essentially comparing the level of desired signal to the level of background noise. Informally, it often refers to the ratio of useful information to false, useless, or irrelevant information. Did we say irrelevant and often useless information? Welcome to the world of information security. We have tons of noise that obfuscates the desired signals we need to hear.

The third quarter of 2011 offered its fair share of noise and signal: Malware continues to be produced daily at high levels, but we often miss its sophistication—which lies buried beneath the big numbers. McAfee Labs saw some significant increases this quarter in stealth malware techniques, often referred to as rootkits, especially from the TDSS family. We also observed the continued emphasis on mobile malware, specifically targeting the Android operating system. In fact, this quarter Android was the sole target of mobile malware writers. A true portent indeed!

Spam and messaging threats continue to evolve. The volume numbers are still at or near their lowest in years, but that does not tell the full story. Although numerically spam is low around the world, the targeted spam, sometimes called spearphishing, is actually more sophisticated than ever. Simply look at any high-profile attack in the news and you will see that the initial vector of compromise is almost always a spearphishing email. Spearphishing is in many ways the stealth malware or rootkit of spam—designed to bypass our mental filter using evasion and well-crafted lures.

Other interesting news this quarter includes changes to Fake AV, while AutoRun and password-stealing Trojan malware remain at steady levels. Botnets made some strong advances globally and continue to be dispersed differently in almost every region and country. Likewise, the lures McAfee Labs sees in spam also demonstrate global variety. Attackers continue to show great agility in these areas: lures and malware that are specific to both regions and languages.

Our Top Threats breakdown shows this variety as well. Threats in North America were quite different from those in Asia, Australia, and the rest of the world. We found more variety in Top Threats this quarter than in the past.

Finally, we gathered reports of significant activity in the areas of cybercrime, cyberwarfare, and hacktivism. Law enforcement made strides with several arrests. Prices continue to be very fluid on the cybercrime underground. Multiple high-profile attacks as well as shifting tactics from hacktivist groups such as Anonymous have provided more than enough excitement.

One thing is certain: 2011 continues to be a year of change, challenge, and chaos in information security.

Table of Contents

Mobile Threats

Last quarter the Android mobile operating system (OS) became the most "popular" platform for new malware. This quarter Android became the exclusive platform for all new mobile malware. The Symbian OS (for Nokia handsets) remains the platform with the all-time greatest number of malware, but Android is clearly today's target.

Premium-rate SMS-sending Trojans continue to be attractive to malware authors. The Android/Wapaxy, Android/LoveTrp, and Android/HippoSMS families are new versions of premium-rate SMS Trojans that sign up victims to subscription services. The malware also cleverly deletes all subscription confirmation messages received so that the victim remains unaware of the activity, and the attacker makes more money.

Maliciously modified apps made up a good portion of mobile malware this quarter. The Android/PJApp family sends SMS messages, too, but also collects sensitive information (IMEI, IMSI, SIM data) from the phone. This type of theft has been a continuing trend for malware written for any platform: Steal as much data as possible once the device has been compromised.

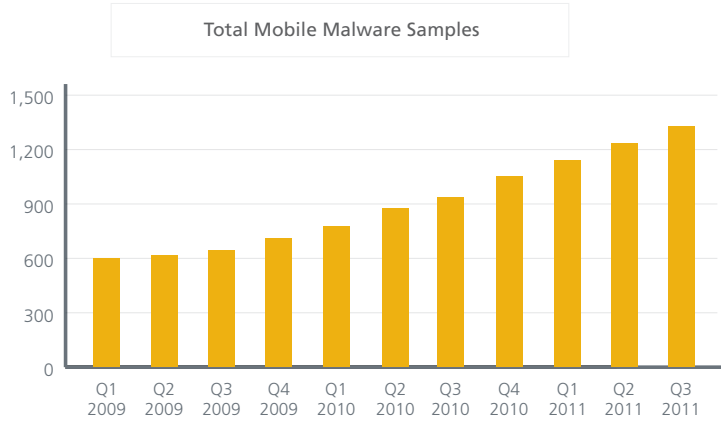
In an interesting turn, Android malware has begun a new method of stealing information from users: by recording their phone calls. Two examples are Android/NickiSpy.A and Android/GoldenEagle.A, both of which record user conversations and forward them to the attacker. Attackers can't be sure that the first one or two calls have the information they seek, so these malware remain on the devices for extended periods without being detected; that's a very persistent threat indeed!

Another technique for stealing information is to use root exploits to gain access to system databases. This allows attackers to break free of the application sandbox that Android would normally make them sit in, and allows attackers access to all of the phone's data and operations. The Android/DroidDeluxe and Android.ApkMon families try to gain root access (via different exploits) to read system files (such as SMS database, emails, and contacts). We expect this trend to continue as it has proved useful for years on other platforms.

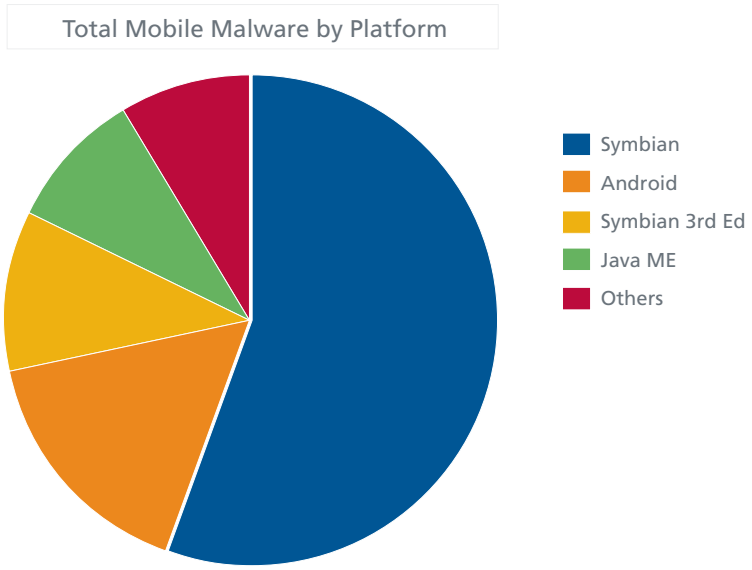
Now that the SpyEye family of crimeware has started to take over from Zeus, the former's authors apparently see the need to develop their own SMS-forwarding functionality. As this feature is necessary only to enable the malware to complete fraudulent banking transactions, these Trojans are very simple in their design. Android/Spitmo.A is an SMS-forwarding Trojan that operates very similarly in this regard to the Zitmo family. Why write a complex routine when a simple one will do the job?

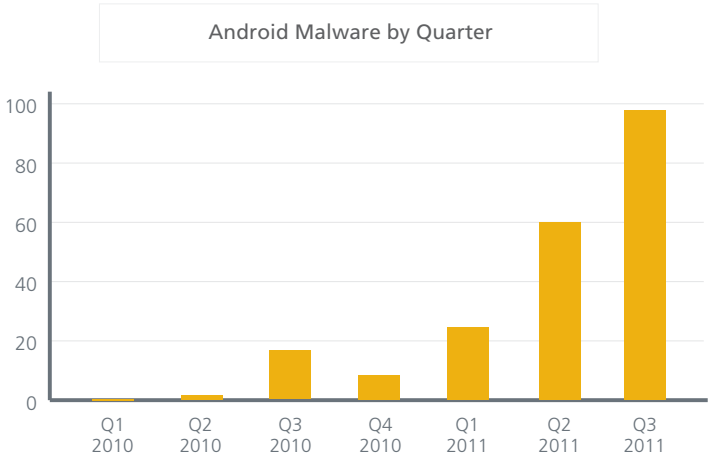
Mobile Malware Statistics

As you can see in the next chart, mobile malware growth in 2011 is firmly on target to exceed last year's and become the busiest year in mobile malware's short, but interesting, history.



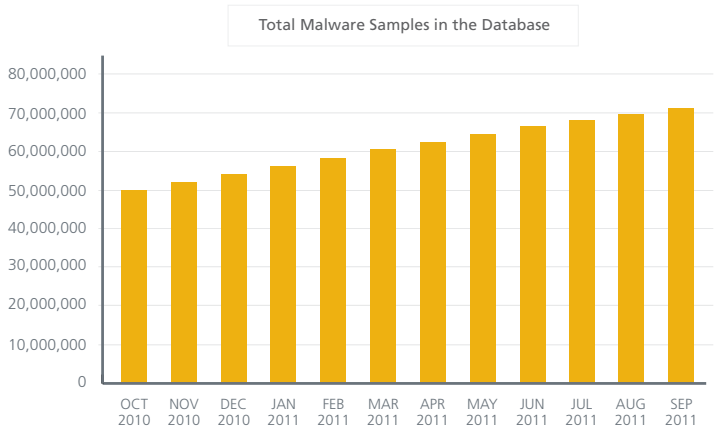
And Android is the top target of today's mobile malware authors.

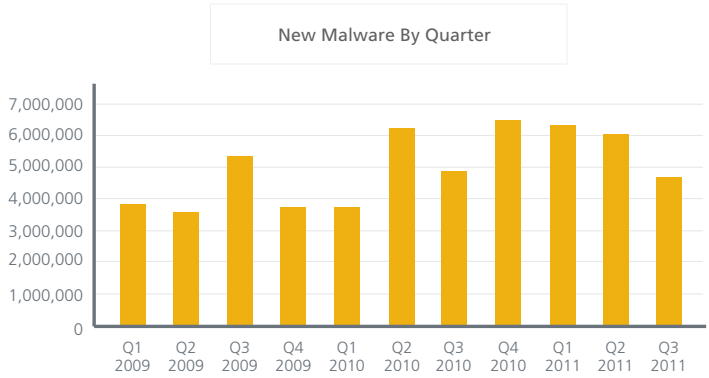




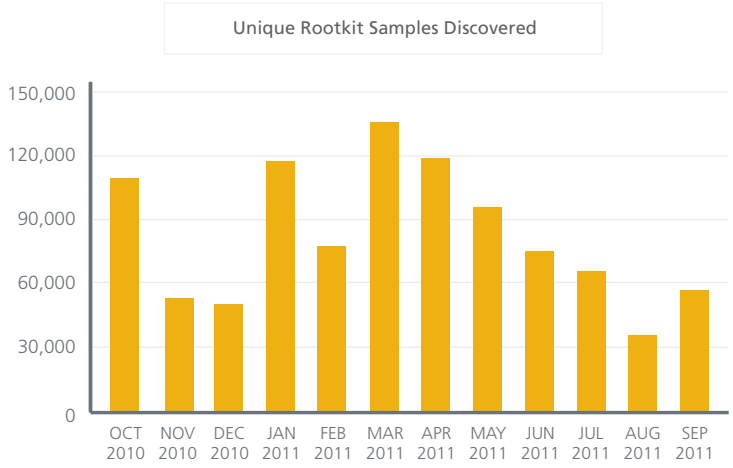
Malware Threats

The overall growth of malware declined slightly during this quarter compared with last quarter but remains about equal with last year's pace at the same time of year. Third-quarter growth has been slower than the second quarter's for the last two years; maybe malware writers take vacations like the rest of us. But we warn you not to get complacent—because the cumulative malware number has exceeded the 70 million mark. We predicted this figure last year. We expect to count around 75 million unique malware samples by year's end.

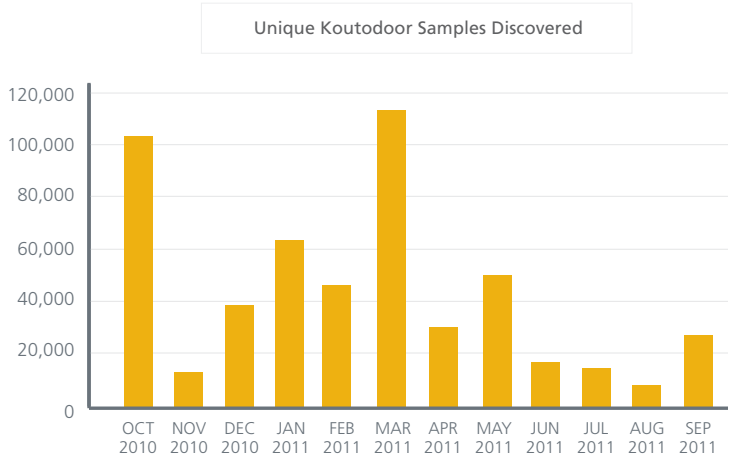


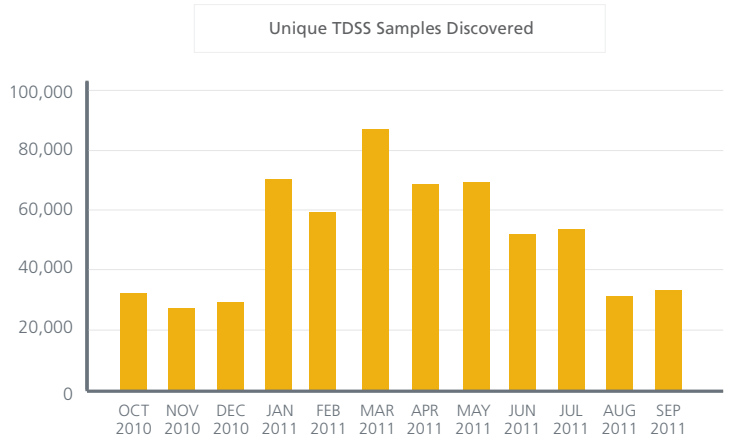


Despite the fact that their overall numbers are slightly down, we saw interesting development in rootkits in general. Rootkits, or stealth malware, are one of the nastiest threats we face. They are designed to evade detection and thus "live" on a system for prolonged periods. The next graph shows that the overall numbers are again on a growth curve:

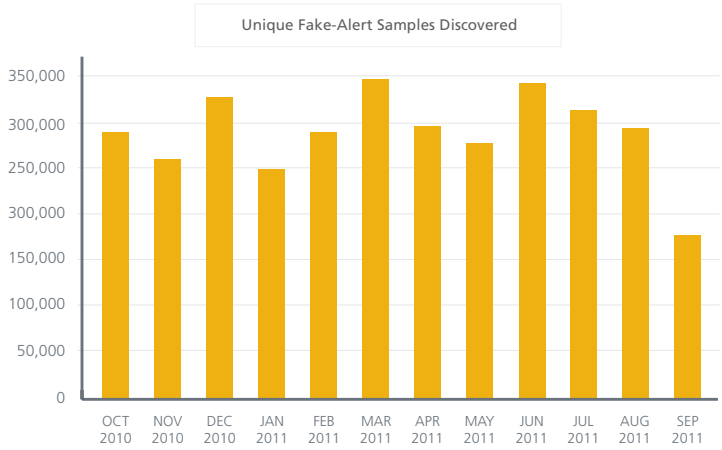


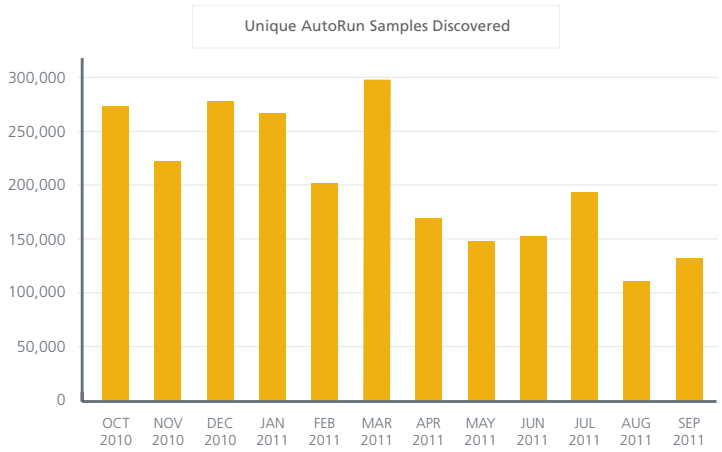
The story becomes more interesting when we look at two of the most developed and widespread rootkits: Koutadoor and TDSS. Both of these families are popular, but we have seen a bit more development focused on TDSS. Comparing the next two charts bears out this view.

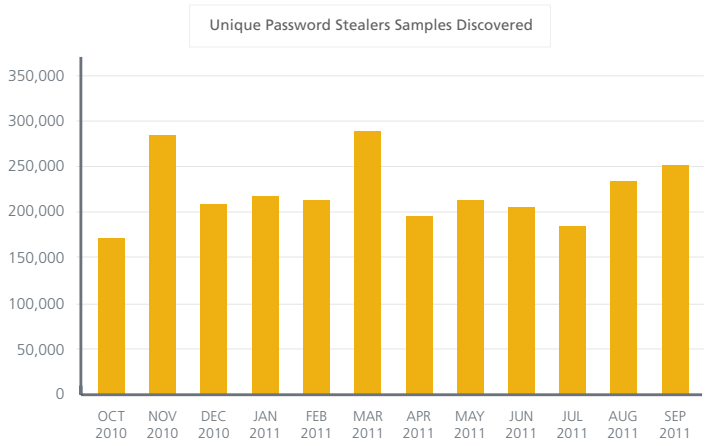




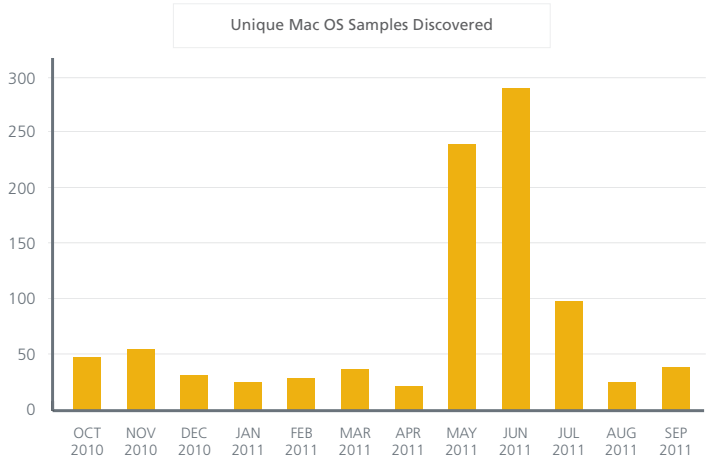
Let's catch up on some of our other "favorite" malware: Fake AV, AutoRun, and password-stealing Trojans. Fake AV, also known as fake alert or rogue security software, has bounced back strongly from previous quarters, while AutoRun and password stealers remain at relatively constant levels.



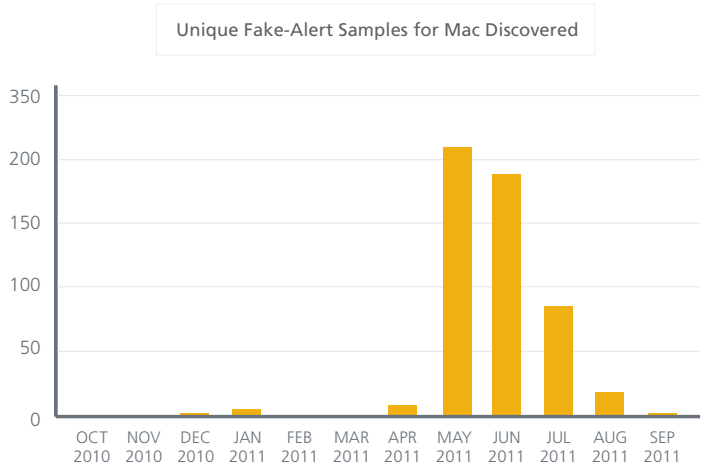




Previously considered almost a misnomer, Mac malware continues to show a bit of growth—although this can be deceptive. When we look at a chart of overall malware growth for the Mac, the trend appears unremarkable:



The story is a bit different when we examine the chart specific to Fake AV for the Mac:



Fake AV software for Mac boomed in the second quarter this year. Although the current period was not as strong, any OS can be a target. Stay prepared regardless.

Global Infected Computers

The top threats around the world continue to change from quarter to quarter. Last quarter, downloaders and certain potentially unwanted programs (PUPs) were prevalent. This quarter, parasitic malware and exploits are a bit more popular, with exploit scripts at the forefront of global detections. This data is representative of real-world detections from detection technologies worldwide. Thus malware will show up in the same list as PUPs and other threats. As you can see from our global breakdown, some regions see variations on a theme while other regions face completely different threats. Web-based exploitation leading to parasitic malware infections is prevalent overall, and those password-stealing Trojans just will not go away.

Rank	Top 5 Global Threats
1	Malicious Iframes
2	Malicious Windows Shortcut Files
3	Parasitic File Infector
4	USB-Based AutoRun Parasitic Malware
5	Web-Based File Infectors

Rank	North America
1	Malicious Iframes
2	Malicious Windows Shortcut Files
3	Parasitic File Infector
4	Web-Based File Infectors
5	USB-Based AutoRun Parasitic Malware

Rank	South America
1	Banker Trojan Variant
2	Password-Stealing Trojan Variant
3	Password-Stealing Trojan Variant
4	Password-Stealing Trojan Variant
5	USB-Based AutoRun Parasitic Malware

Rank	Europe
1	Web-Based File Infectors
2	Parasitic File Infector
3	USB-Based AutoRun Parasitic Malware
4	Generic Downloader Trojan
5	Adware-HotBar

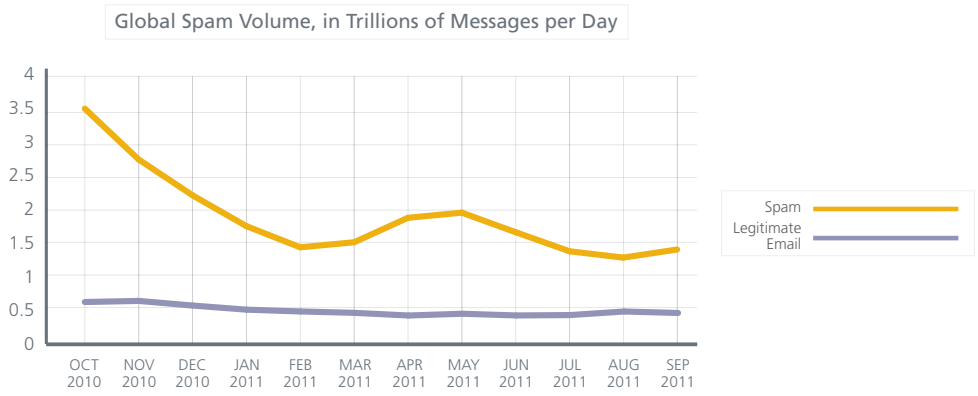
Rank	Asia
1	Parasitic File Infector
2	Password-Stealing Trojan Variant
3	USB-Based AutoRun Parasitic Malware
4	Generic Downloader Trojan
5	Password-Stealing Trojan Variant

Rank	Africa
1	Password-Stealing Trojan Variant
2	USB-Based AutoRun Parasitic Malware
3	Adware-HotBar
4	Malicious Windows Shortcut Files
5	Mabezat Worm Variant

Rank	Australia
1	Password-Stealing Trojan Variant
2	Malicious Windows Shortcut Files
3	Malicious Windows Shortcut Files Variant
4	Parasitic File Infector
5	Zeus/SpyEye Trojan Variant

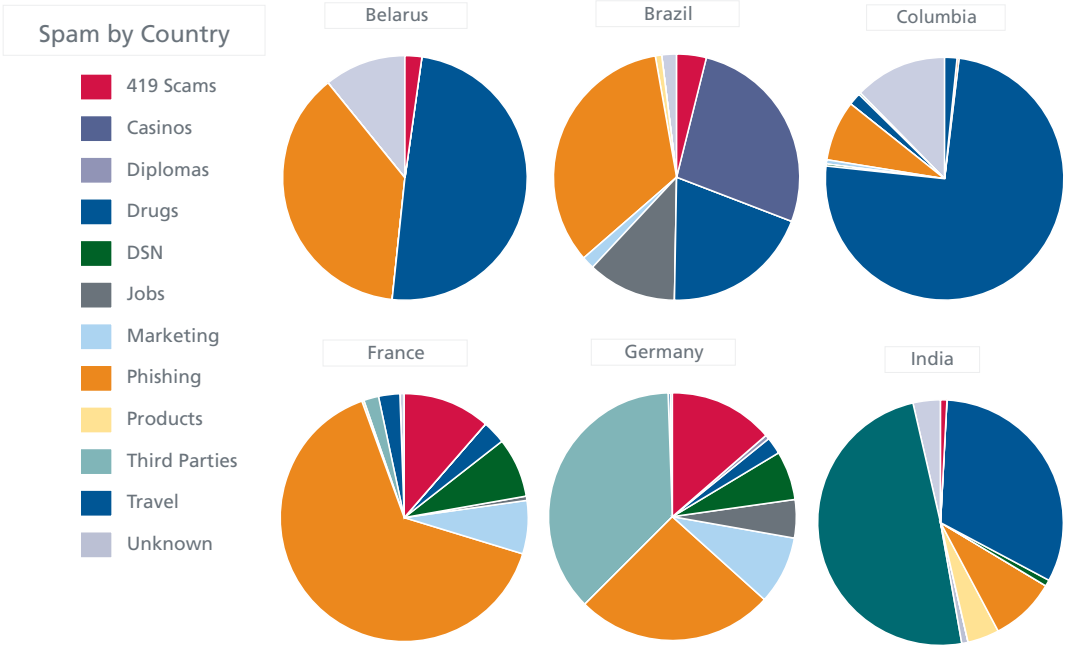
Messaging Threats

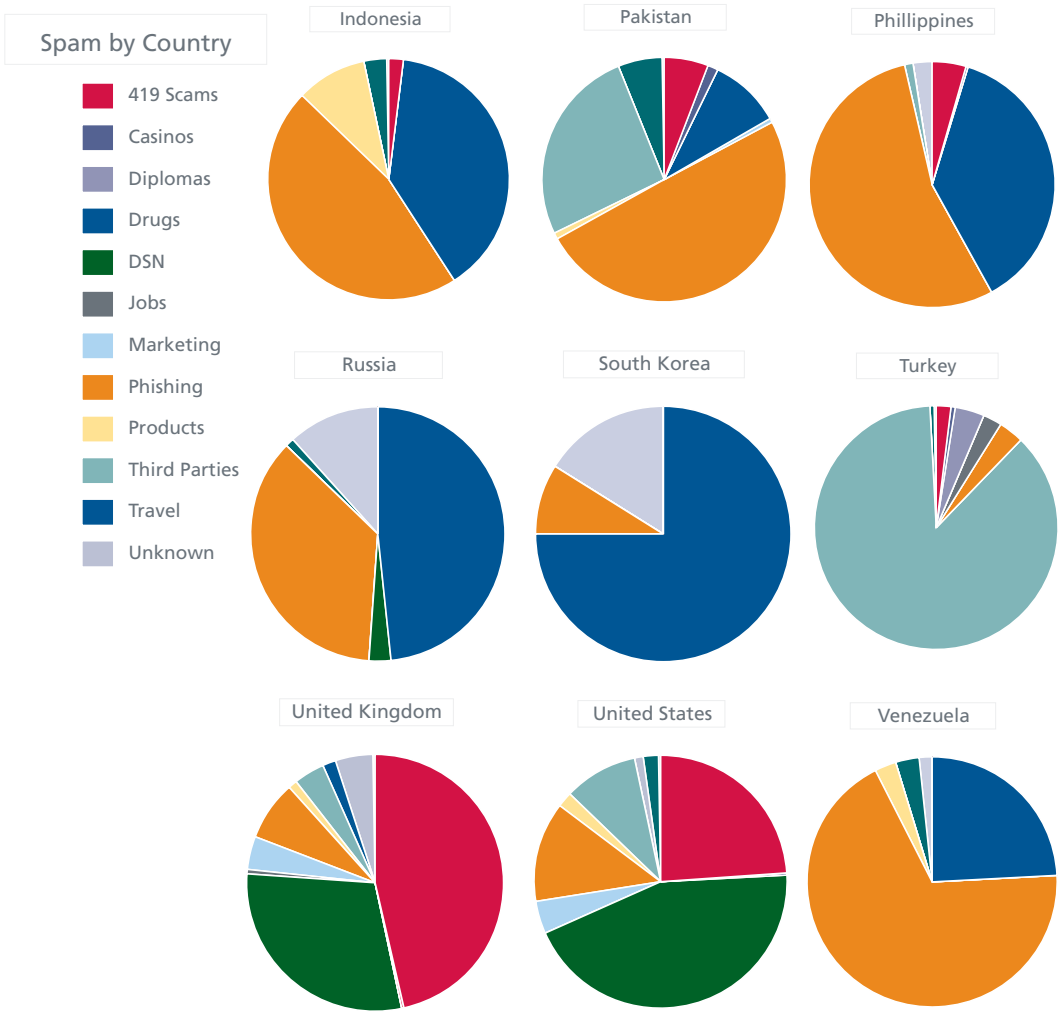
Spam around the globe continues its downward trend, maintaining circa-2007 spam levels. Even though spam volume is way down, McAfee Labs sees targeted spam, often called spearphishing, at its greatest development in years. So, very much like malware, the noise tells us spam levels have dropped, yet the signal we need to hear is that the bad guys have changed their tactics. They are protecting their business models and are doing so with a sophistication that creates a more dangerous threat than before.



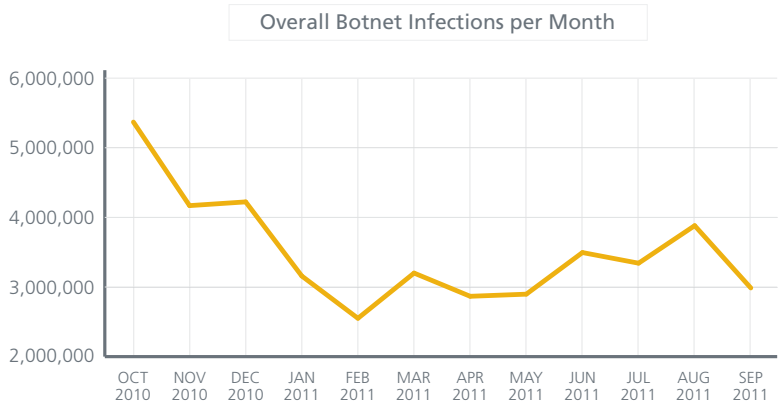
Social Engineering Speaks Your Language

As always, social engineering lures in spam subject lines differ greatly depending on geography and language. The lures can vary by month or season, and often use holidays or sporting events as bait. Attackers show a remarkable insight into what works in different cultures and regions—not just globally but also seasonally. In France phishing may be popular, while in the United Kingdom "419 scams" are the rage. Meanwhile drug spam is hot in South Korea and Russia, while in the United States we see lots of Delivery Service Notifications (fake error messages) as a lure. Attackers continue to show great insight as they attempt to trick users.





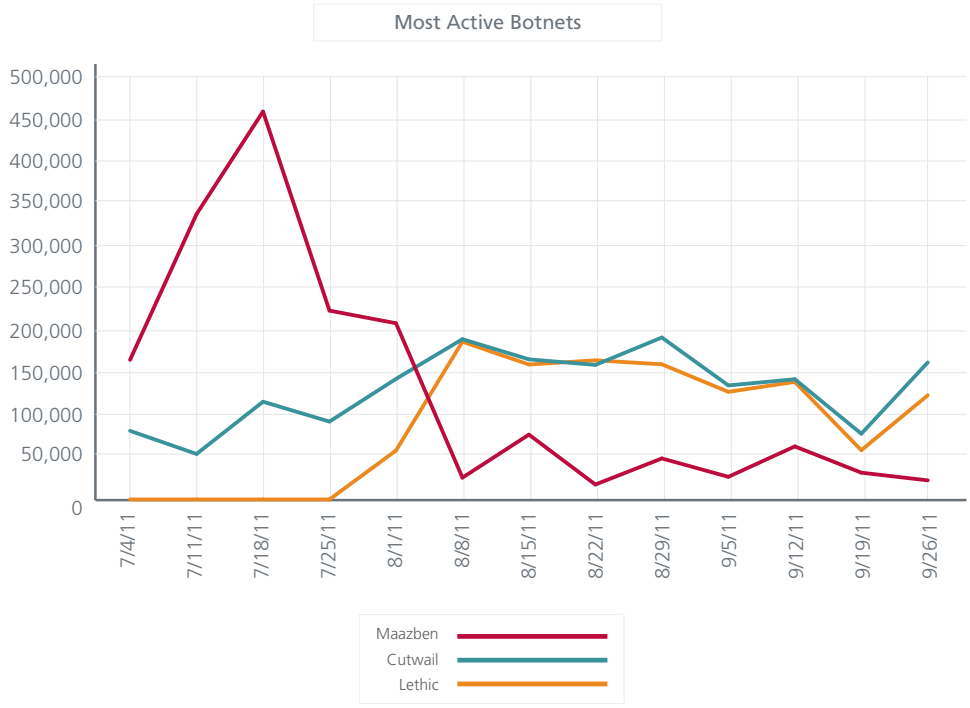
Worldwide overall botnet growth also took a small dip toward the end of this quarter, but our analysis of specific regions shows some significant increases.

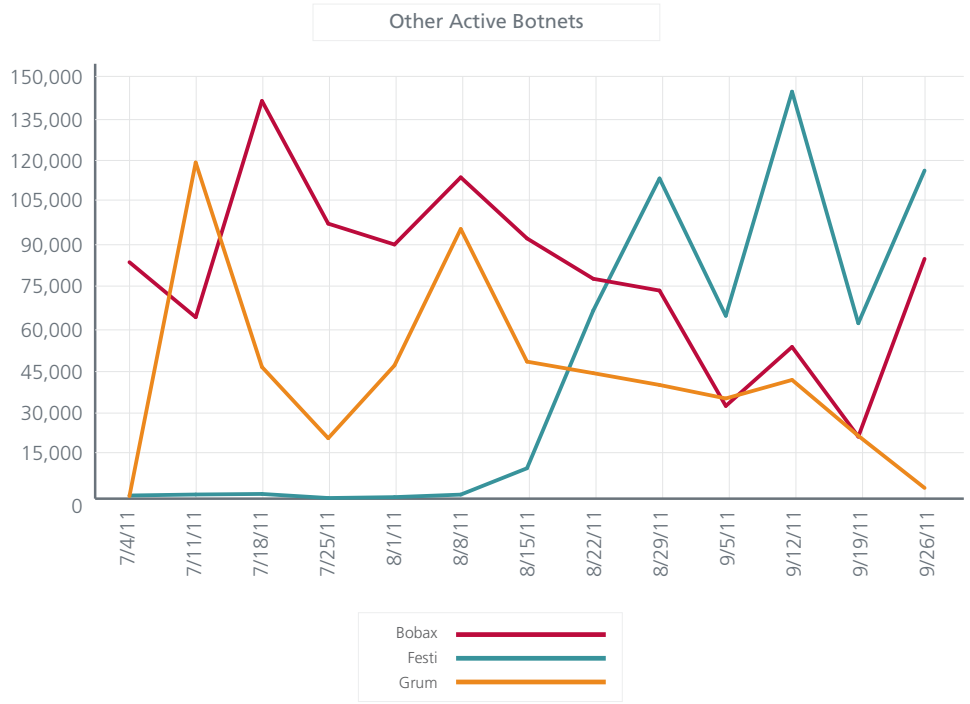



New Botnet Senders by Country
Argentina
60,000
50,000
40,000
30,000
20,000
10,000
0
Australia
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
Brazil
250,000
200,000
150,000
100,000
50,000
0
China
250,000
200,000
150,000
100,000
50,000
0
Columbia
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
France
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
Germany
200,000
150,000
100,000
50,000
0
India
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
OCT 10
NOV 10
DEC 10
JAN 11
FEB 11
MAR 11
APR 11
MAY 11
JUN 11
JUL 11
AUG 11
SEP 11

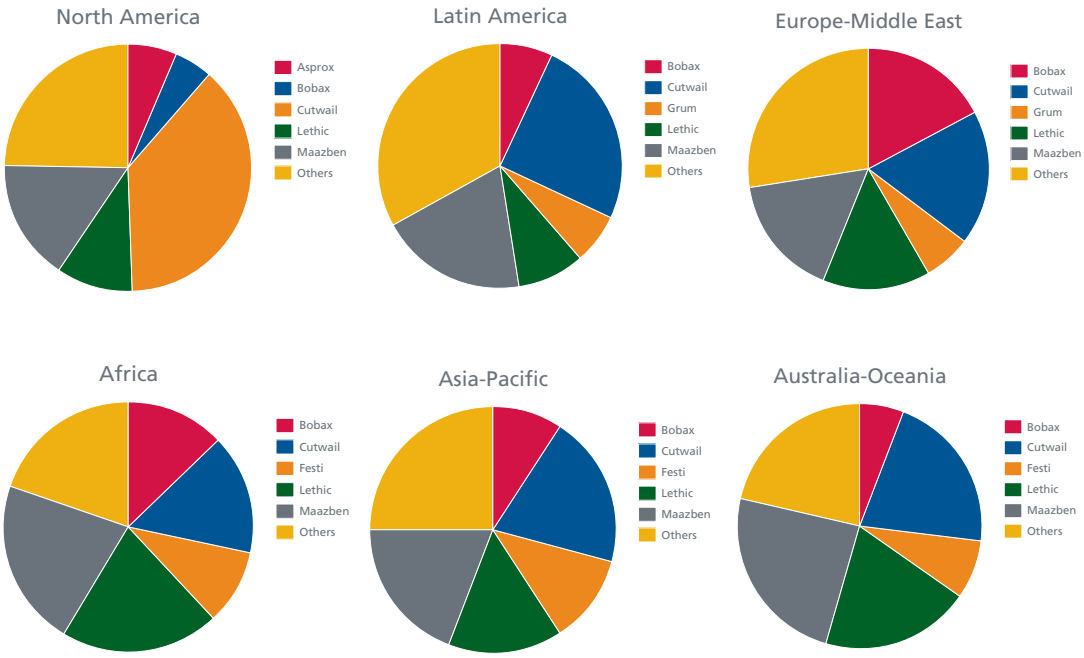

New Botnet Senders by Country
Indonesia
120,000
100,000
80,000
60,000
40,000
20,000
0
OCT 10
NOV 10
DEC 10
JAN 11
FEB 11
MAR 11
APR 11
MAY 11
JUN 11
JUL 11
AUG 11
SEP 11
Italy
100,000
80,000
60,000
40,000
20,000
0
Japan
30,000
25,000
20,000
15,000
10,000
5,000
0
Portugal
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
Russia
300,000
250,000
200,000
150,000
100,000
50,000
0
South Korea
100,000
80,000
60,000
40,000
20,000
0
Spain
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
United Kingdom
150,000
120,000
90,000
60,000
30,000
0
United States
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
Venezuela
150,000
120,000
90,000
60,000
30,000
0

Several countries saw significant growth in botnet infections. Cutwail, Festi, and Lethic lead the pack in new infection activity this quarter, while new infection rates of Grum, Bobax, and Maazben declined.





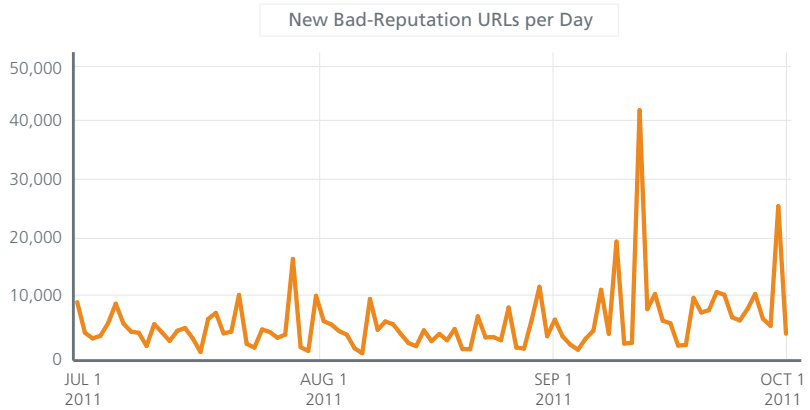
Remember that declining new infection rates do not imply a reduction in overall botnet usage. In our breakdown of botnets by geography, we see that many of them are still quite active, even though new infections may be temporarily slowing.



Web Threats

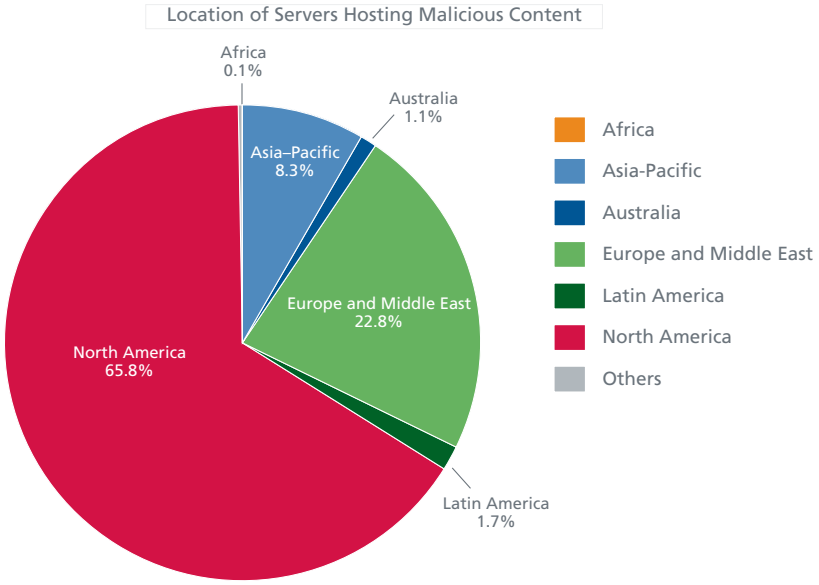
Websites can have bad or malicious reputations for a variety of reasons. Reputations can be based on full domains and any number of subdomains as well as on a specific IP address or URL. Malicious reputations are influenced by the hosting of malware, PUPs, or phishing sites. Often we observe combinations of questionable code and functionality. Many factors go into a site's reputational rating.

Last quarter McAfee Labs recorded an average of 7,300 new bad sites per day; in this period that figure dropped a bit to 6,500 sites, which is comparable to the same time last year. In August we saw an average of more than 3.5 sites rated "red" each minute.

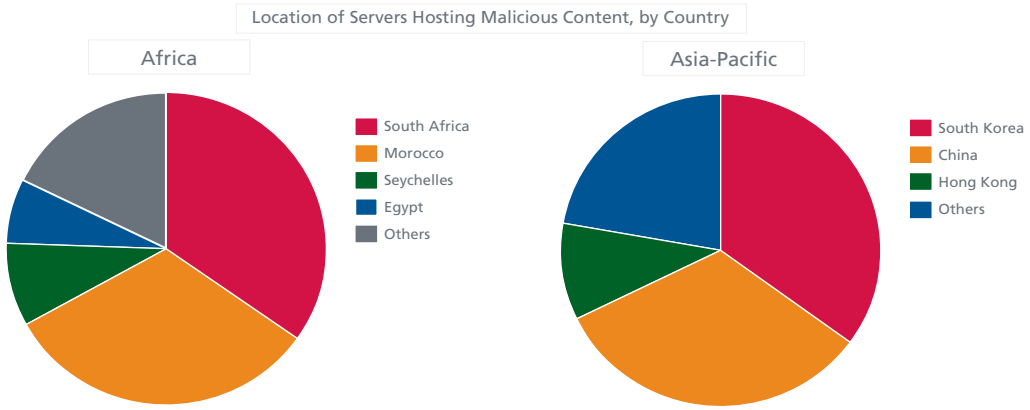


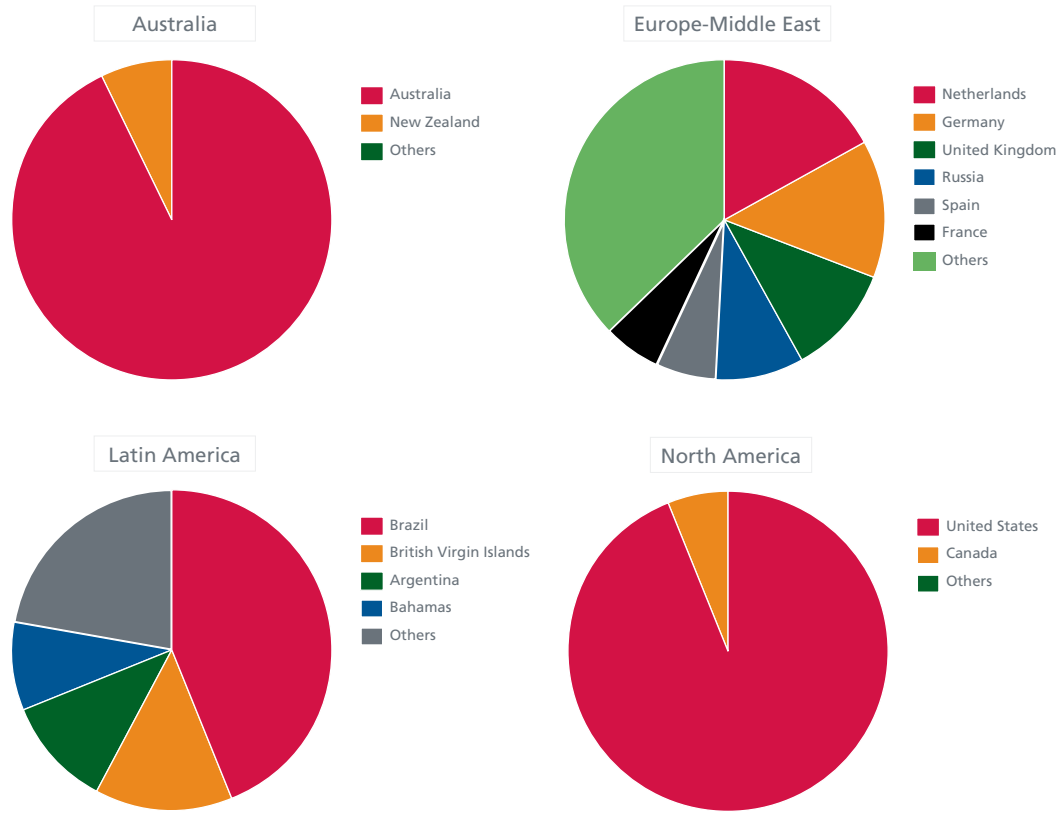
We saw four significant spikes in malicious web content this quarter. They are not linked to any particular attack but to updates to the internal or external sensors that periodically send data to our web threat database. We'll highlight these spikes in the following paragraphs.

The vast majority of new malicious sites are located in the United States. Next in line, we find the Netherlands, Canada, Germany, South Korea, China, and the United Kingdom. Last quarter we saw the same top seven countries though they finished in a different order. Our regional breakdown reveals where most malicious servers reside.

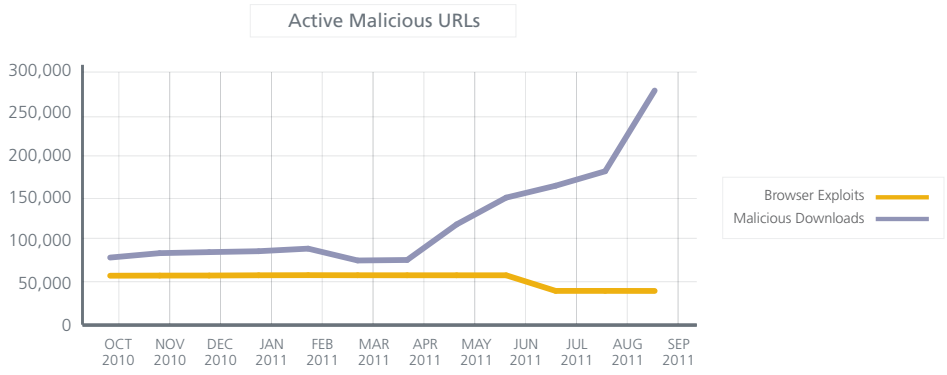


North America still leads by a large margin (with 66 percent of servers this quarter, 60 percent last quarter, and 68 percent in the first quarter). Europe and the Middle East remain in second rank (23 percent, 25 percent, and 18 percent). Let's take a closer look by region.

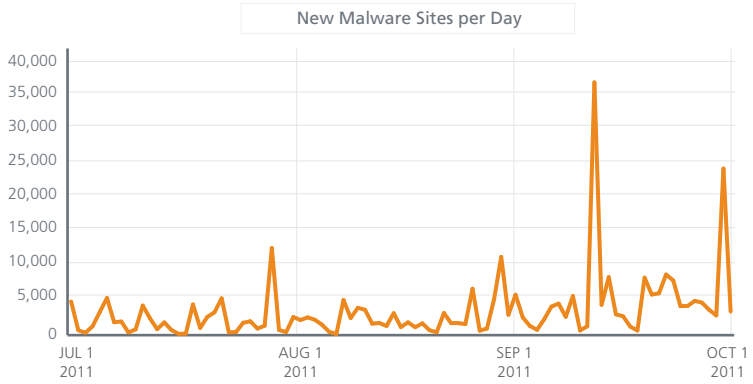




This quarter, the number of websites hosting malicious downloads continued to increase, while the number of sites hosting browser exploits slightly decreased.



The following chart provides a picture of the number of websites delivering malware and PUPs that McAfee Labs detected this quarter.

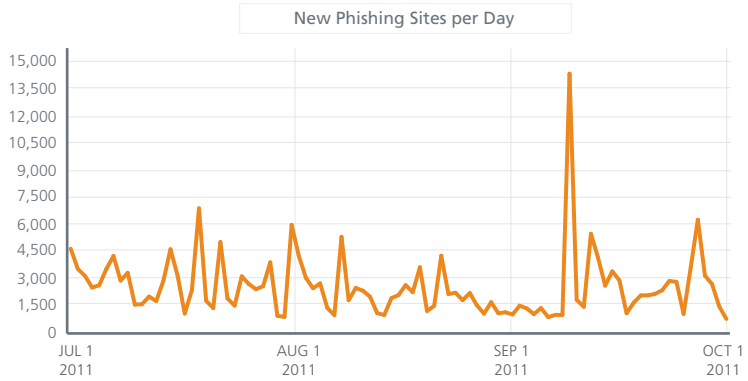


We saw an increase this quarter, with around 3,500 new sites per day compared with 3,000 per day during the prior quarter.

The two most significant spikes, on September 12 and 30, were caused by major updates to our sensors that list URLs distributing malware.

During the quarter we identified approximately 2,700 phishing URLs per day, very similar to our figures for last quarter. During the same period last year, we counted 2,900 URLs per day.

On September 9, we saw a spike of more than 14,000 hits. This jump is due to an update of our phishing sensors. That day, Taobao (an online Chinese store), Citibank, Numericable (French ISP), Bank of America, PayPal, and Wells Fargo were the largest targets.



Cybercrime

This quarter, we continue our overview of prices in the underground marketplace.

In September, security maven Brian Krebs analyzed some activities linked with the TDSS botnet and especially awmprowy.net. This service, offering anonymous Internet access via hijacked computers, was billed as "the fastest anonymous proxies" for Internet access.[1] Before this underground marketplace disappeared, we were able to record their prices. Within a short time AWM Proxy reopened at a new website and URL. Cybercriminals are rarely gone for long and can often regain control of their businesses.

Exclusive and Individual Proxies

These are used for anonymous browsing, ICQ, and FTP; or for online games (casino, poker, and roulette). The seller claims that proxies are unique to each customer.

Name of product		Exclusive-100	Exclusive-200	Exclusive-500
Number of proxies		100	200	500
Number of changes in the list per day		50	100	200
Automatic substitution of "dead" proxies by choosing a priority country			All Russia United States or Canada	
Cost	1 week	US$90	US$160	US$300
	2 weeks	US$160	US$290	US$550
	30 days	US$290	US$550	US$1,000

Name of product		Individual-5	Individual-15	Individual-30
Number of proxies		100	200	500
Number of changes in the list per day		50	100	200
Cost	2 weeks	US$40	US$60	US$100
	30 days	US$60	US$100	US$160

Personal Proxies

Browser proxies can anonymously access porn sites, entertainment resources for online casinos, payment systems, and other sites that block access from certain countries.

Period	Daily	Biweekly	Monthly
Cost (for unlimited traffic)	US$3	US$15	US$25
Number of IPs for access	1	3	3
Duration (in days)	1	14	30

Private HTTP Proxies

These allow buyers to profit from a static IP in a particular country or to improve performance in mailing campaigns.

	Elementary	Advanced	Professional	Unlimited	Unlimited-90
Cost	US$35	US$50	US$60	US$95	US$240
Term			Monthly		90 days
Number of IPs for access	1	2	3	3	3
Number of threads per account	100	200	400	Unlimited	Unlimited

HTTP/SOCKS Proxies

These include HTTP, HTTPS, SOCKS4, and SOCKS.

	Biweekly	Monthly/ Limited	Monthly/ Unlimited	Unlimited-90
Cost (email prohibited)	US$65	US$95	US$195	US$500
Cost (email allowed)	NA	US$350	US$550	US$1,400
Number of IPs for access	Each customer gets access to the entire base of proxies (that is why so many proxies end up on blacklists)			
Number of Threads	350	350	Unlimited	Unlimited

Crimeware Tools

The most notable new product during the last several months is a Linux exploit pack available via Russian underground circles. The developer is getozz.

Name of Tool	Prices (all in US$)	Advanced
LinuQ (appeared in July)	200 (public version) $1,500 (with private exploit)	Part bot, part exploit pack, this package is designed to compromise Linux servers. In its public version, it uses four PMA vulnerabilities: CVE-2009-1148 (unconfirmed) CVE-2009-1149 (unconfirmed) CVE-2009-1150 (unconfirmed) CVE-2009-1151 (confirmed)
BlackHole Exploit Kit Version 1.2.0 (September)	Annual license: $1,500 Half-year: $1,000 3 months: $700	Last quarter, we listed Version 1.1.0. The new version contains the same nine exploits (with six from 2010).
Bleeding Life Version 3 (August)	New Buyers: $1,000 Discount for previous buyers: $250	We listed Version 2 in our first-quarter report. This more expensive version, with 10 exploits, is now on the market.

Actions Against Cybercriminals

Location	Description
Hong Kong (August)	Hong Kong police arrested a 29-year-old man suspected in a cyberattack on the city's stock exchange website. The attack halted trading in the shares of seven companies, including banking giant HSBC, on August 10.[2]
Ukraine (August)	Ukraine's security service SBU arrested four people for allegedly creating fake payment cards with stolen information in an operation estimated to have caused US$20 million in damages.[3]

Hacktivism

This quarter, people calling themselves Anonymous launched many attacks.[4] These attacks were numerous but also confusing because in many cases their goals were unclear. At the same time, on the same IRC channel, some called for increased protests against PayPal, while others suggested opening PayPal accounts to receive donations again. Some called for attacks on Facebook, while others created pages to promote their opinions and operations. Highlights for the quarter:

- July 1: Arizona Fraternal Order of Police
- July 3: Democratic Party of Orange County (California)
- July 11: Booz Allen Hamilton
- July 12: Monsanto
- July 29: ManTech
- August 14: Bay Area Rapid Transit (California)
- August 19: Vanguard Defense Industries
- September 2: Texas Police Chiefs Association
- September 26: Austrian Police
- September 27: Goldman Sachs

Main Events

On July 28, South Korean authorities claimed that hackers from China may have stolen personal information belonging to as many as 35 million users of the Nate portal and Cyworld blogging sites, both operated by SK Communications.

The South Korea National Police Agency said this attack is the nation's worst hacking case and originated from a Chinese IP address.[5] It allowed hackers to obtain the names, resident registration numbers, birthdays, gender, email addresses, telephone numbers, home addresses, and user names of the 35 million account holders.

After the Comodo incident reported on March 15 and the RSA attack announced on March 17, the Iranian attacker who claimed responsibility for these attacks appears to have continued his assaults. This quarter, he claimed responsibility for the break-in at the Dutch certificate authority DigiNotar that was detected on July 19.[6] That day, DigiNotar detected an intrusion into its Certificate Authority infrastructure, which resulted in the fraudulent issuance of public-key certificate requests for a number of domains, including Google.com, Yahoo, Mozilla add-on's, and several intelligence agencies. This company has since gone out of business. (Taking control of a Certificate Authority (or just using rogue certificates) makes an attack far more likely to succeed. Stuxnet and Duqu took this approach.)

A Touch of Cyberwar

Location	Description
East Turkestan (July)	Approaching the second anniversary of the ethnic unrest in East Turkestan, the World Uyghur Congress (WUC) website has again been the victim of cyberattacks. Webmasters say that the attacks seem to originate from China.[7]
United Kingdom (September)	Russia's embassy in London said on September 11 its website crashed in a suspected hacking attack just before U.K. Prime Minister David Cameron began the first visit by a British leader to Moscow since the 2006 killing in London of Alexander Litvinenko, a Kremlin critic and former Russian spy who died from poisoning by radioactive polonium-210.[8]
Japan (September)	Mitsubishi Heavy Industries, a major Japanese defense contractor, discovered cyberattackers had breached its computer network in August.[9]

About the Authors

This report was prepared and written by Toralv Dirro, Paula Greve, David Marcus, François Paget, Craig Schmugar, Jimmy Shah, and Adam Wosotowsky of McAfee Labs.

About McAfee Labs

McAfee Labs is the global research team of McAfee. 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

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled Global Threat Intelligence, 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. McAfee is relentlessly focused on finding new ways to keep our customers safe. www.mcafee.com

1. http://krebsonsecurity.com/2011/09/rent-a-bot-networks-tied-to-tdss-botnet/
2. http://www.physorg.com/news/2011-08-hong-kong-stock-exchange-hacking.html
3. http://www.pcworld.com/businesscenter/article/238579/ukraine_arrests_four_in_carding_scam.html
4. For more on this amorphous phenomenon, see https://blogs.mcafee.com/mcafee-labs/the-rise-and-fall-of-anonymous
5. http://www.reuters.com/article/2011/07/28/us-hackers-attack-idUSTRE76R19M20110728
6. http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx
7. http://www.unpo.org/article/12841
8. http://uk.reuters.com/article/2011/09/11/uk-russia-britain-website-idUKTRE78A1IX20110911
9. http://www.pcadvisor.co.uk/news/security/3304711/cyberattackers-hit-japanese-defense-giant-with-trojan/

McAfee
An Intel Company

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

38401rpt_quarterly-threat-q3_1111_fnl_ETMG