Report

McAfee Threats Report: First Quarter 2012

By McAfee Labs™

Table of Contents

The Greek philosopher Heraclitus, known for his doctrine of change as central to the universe, once wrote that "everything flows, nothing stands still." The first quarter of 2012 embodies Heraclitus' doctrine in almost all areas of the threat landscape. Although we observed declines in the numbers of many areas of malware and threats at the end of 2011, this quarter is almost its polar opposite. PC malware had its busiest quarter in recent history, and mobile malware also increased at a huge rate. We saw growth in established rootkits as well as the emergence of several new families. Many of the familiar malware we analyze and combat rebounded this quarter, but none more so than password-stealing Trojans. In this edition of the *Threats Report* we introduce our tracking of new threats such as the ZeroAccess rootkit and signed malware. We also have prepared our most detailed breakout to date of network attacks.

Spam volume grew again early in the quarter but then resumed its downward trend. We saw an increase in malware targeting the Mac. The trend was not extreme, but the growth is there nonetheless.

Despite spam numbers remaining relatively low around the world, we still see diversity and growth in certain geographies, including Germany and China. New botnet infections leveled off during this period, though several countries, especially Spain and Japan, showed growth.

The United States once again hosted the greatest amount of malicious web content in the world. You will note this trend as well in our expanded network-based attack section, which contains detailed geographical breakdowns from the perspective of both attackers and victims. Active malicious URLs continued the upward growth that was clearly established the previous quarter. The web is a dangerous place for the uninformed and unprotected.

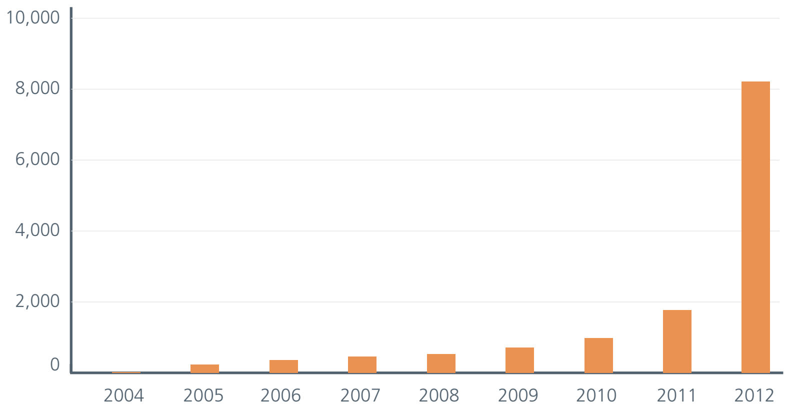
Java and Flash exploits were popular in crimeware tools and toolkits this quarter. Law enforcement made some very significant arrests and moves against cybercriminals and hacktivists. The most famous are probably the kelihos/waledac botnet takedown and the very public arrests of members of Anonymous and LulzSec. It is always a positive thing to see successful legal action in these areas, although other threats will remain with us.

Threats continue to evolve, and attackers continue to push the envelope. We remain vigilant in defending against them.

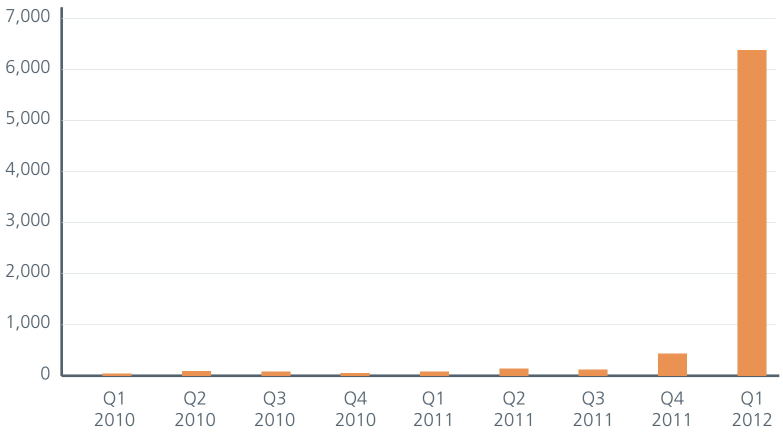
Mobile Threats

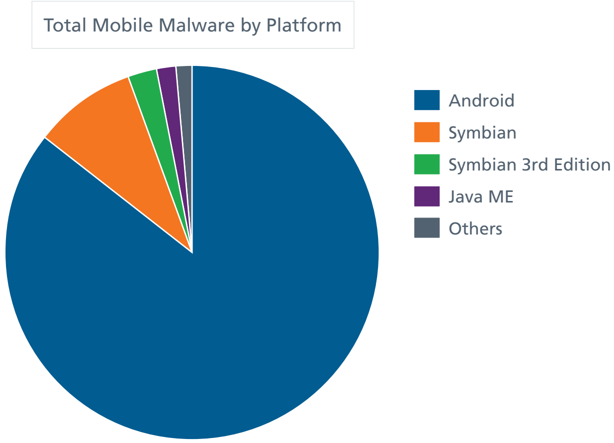
This quarter we report a large increase in mobile malware. The jump was targeted almost solely at the Android platform. Hundreds of Android threats in the middle of 2011 have moved into the thousands this year. Due to significant improvements in our ability to collect, process, and detect mobile malware, the count further accelerated this quarter: Android threats now reach almost 7,000, with more than 8,000 total mobile malware in our database.

Total Mobile Malware Samples in the Database



New Mobile Malware





The great majority of mobile attacks, and their malware, stem from and attack third-party markets, particularly in China and Russia. In most cases, we do not find this malware in the official Android market. Google's app store has suffered from some incidents, but so far those counts are moderate. McAfee Labs advises customers to use install software only from the official market. That step should greatly reduce the risk of compromising your Android device.

This quarter we saw significant amounts of new adware and mobile backdoor malware, along with some very simple premium-rate SMS-sending malware. Mobile adware displays ads on a victim's phone without permission. (This does not include ad-supported games or apps.) Adware ranges from wallpaper with added sales pitches (Android/Nyearleaker.A) to fake versions of games that send visitors to advertising sites (Android/Steek.A). Adware doesn't necessarily reduce users' security, but it does subject them to unwanted ads.

Backdoor Trojans on Android have gotten a bit more sophisticated. Instead of performing just one action, they use root exploits and launch additional malware. Android/FoncyDropper.A, for example, uses a root exploit to gain control of the phone and launch an IRC bot that receives commands from the attacker. It also sends premium-rate SMS messages based on the country of the SIM card.

In a similar vein, Android/Rootsmart.A uses a root exploit to download Android/DrdLive.A, a backdoor Trojan that sends premium-rate SMS messages and takes commands from a control server.

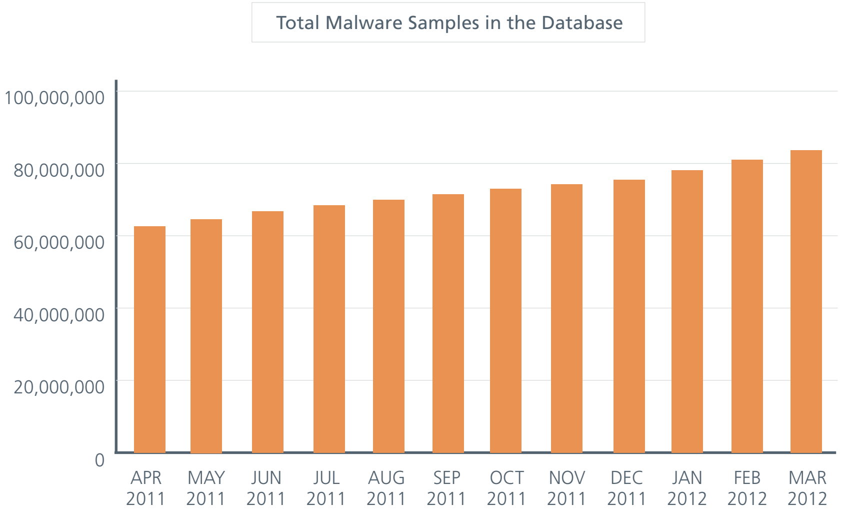
Android/Stiniter.A uses a root exploit to download additional malware and sends information from the phone to sites under the control of the attacker. It also sends text messages to premium-rate numbers. The attacker's control server updates the message body and the number the hijacked phone sends to.

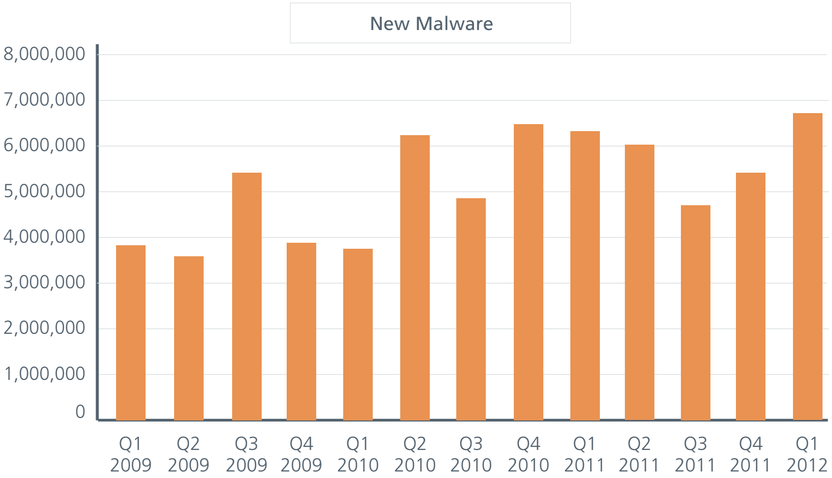
This quarter, malware writers created one of the first destructive Android Trojans, Android/Moghava.A. Instead of damaging apps or other executables this malware goes after photos. Moghava.A searches for photos stored on the SD card, and adds the image of the Ayatollah Khomeini to each picture. The malware is also a bit buggy, so it will continue to add to the pictures until there is no more space on the card.

The writing is clearly on the wallpaper: We must protect all devices, mobile or otherwise, that have valuable data. If not, today's cybercriminals will be happy to handle it for us.

Malware Threats

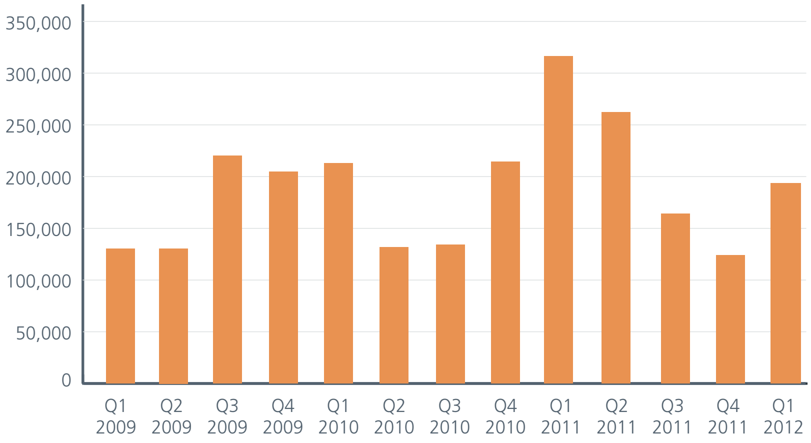
To kick off our malware discussion, we'll crib Thin Lizzy and say that the boys are back in town. The respite from the overall growth of PC-based malware that McAfee Labs saw throughout the past two quarters of 2011 seems to have ended. We shouldn't say just "ended"; in fact this period shows the largest number of malware detected per quarter in the last four years! Going into 2012 we had collected more than 75 million samples in our combined "malware zoo," but with the tremendous growth this quarter we have already topped 83 million pieces of malware. We don't know when we will top the 100 million mark, but it will certainly happen in the next few quarters. With increases in rootkits and their functionality, signed malware, and rampant growth across most other threat vectors, 2012 might prove to be a bumpy year on the security superhighway.



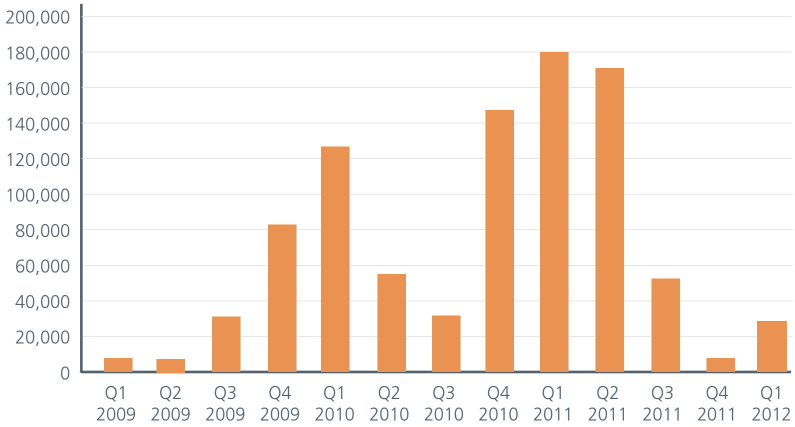


Growth in rootkits bounced back this quarter, with more activity from Koutodoor, though it's nowhere near the malware's height of 12 months ago. Beginning with this report, we break out the rootkit ZeroAccess. This malware is already popular with cybercriminals and other malicious actors. Rootkits, or stealth malware, are one of the nastiest classifications of malware. They have a heavy influence on almost all other areas of malware and are designed to evade detection and "live" on a system for prolonged periods.

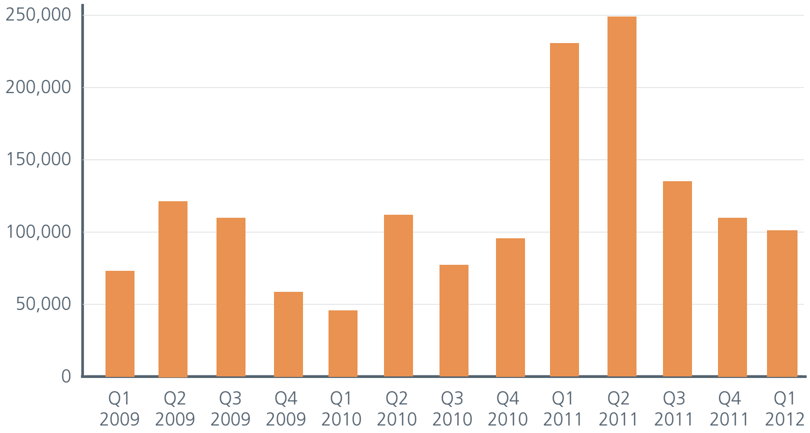
Unique Rootkit Samples Discovered

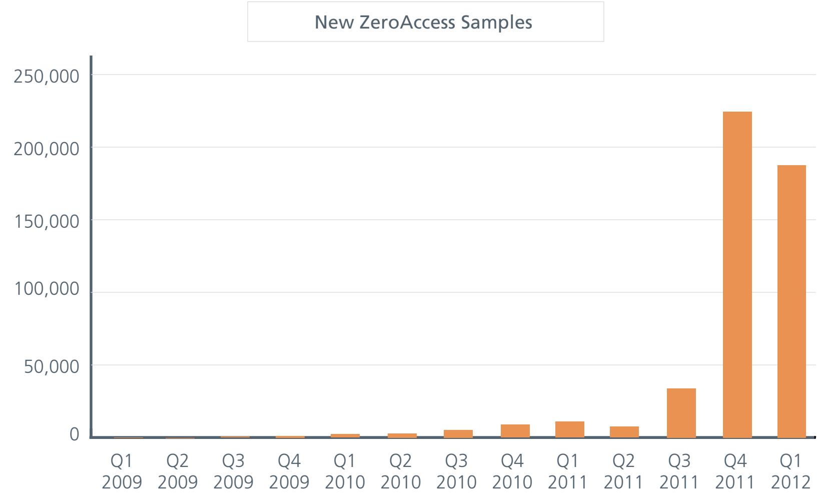


New Koutodoor Samples

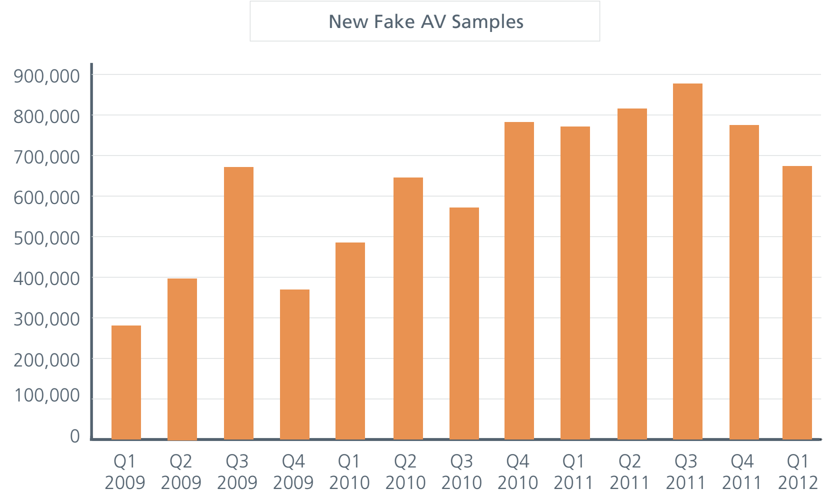


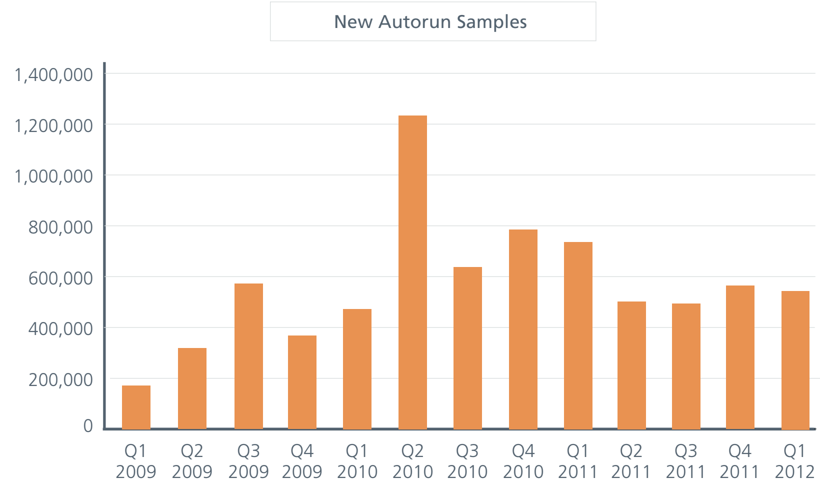
New TDSS Samples

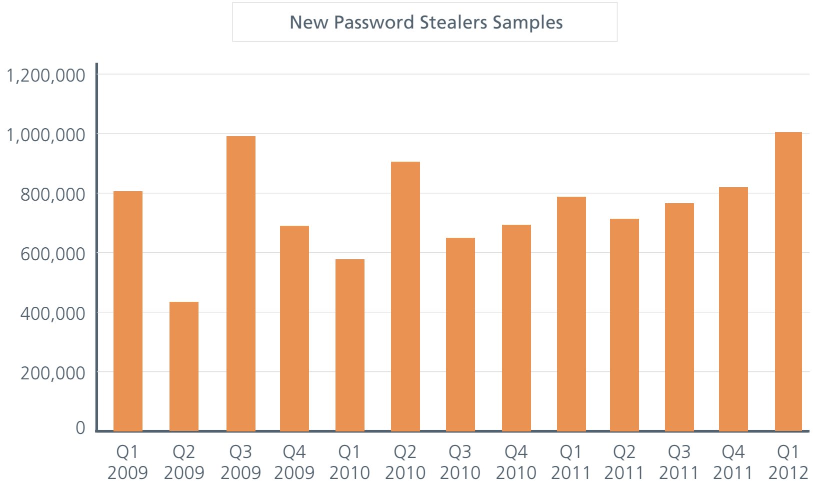




Let's turn to our other "favorites": Fake AV (bogus security software), AutoRun, and password-stealing Trojans are still with us. The first two have continued to drop slightly while password stealers showed a strong surge this quarter.





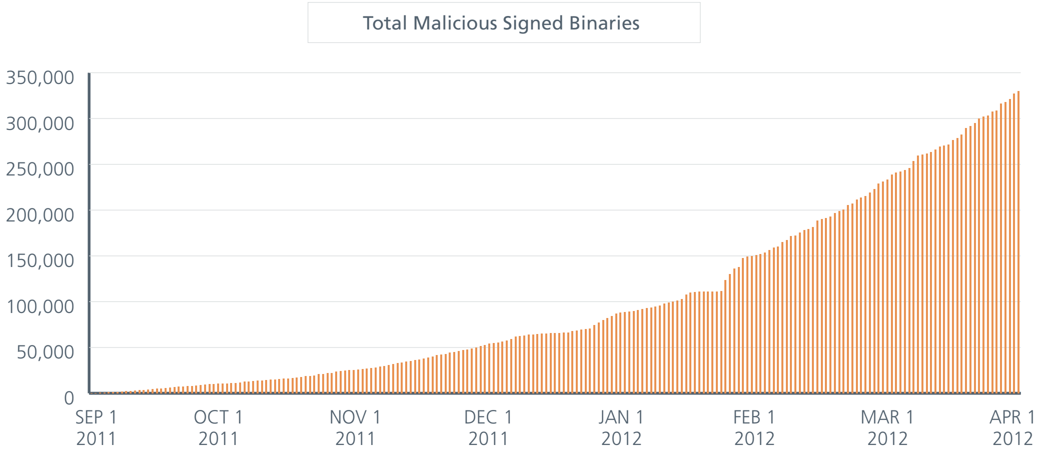


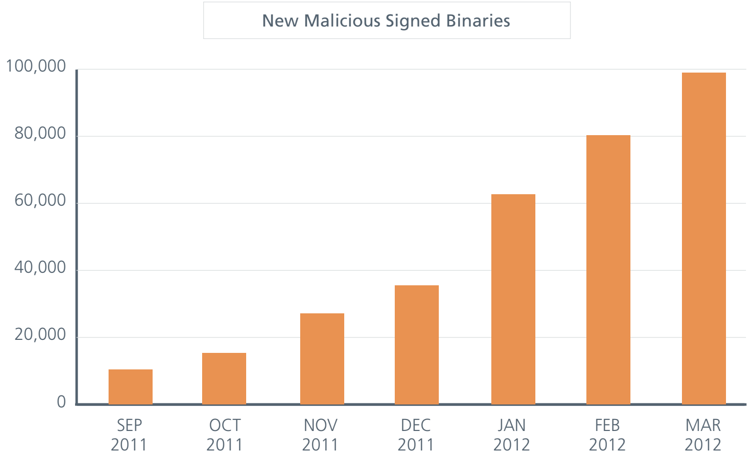
Signed Malware

In an excellent McAfee Labs blog, senior researcher Craig Schmugar discussed why malware writers use digital signatures with their malware:

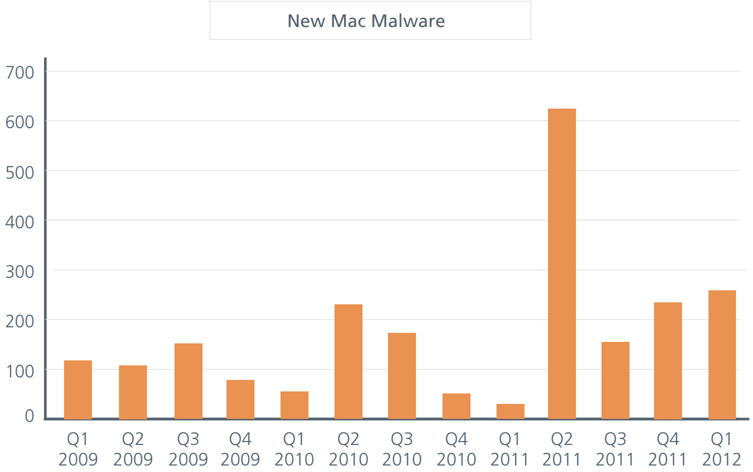
> "Attackers sign malware in an attempt to trick users and admins into trusting the file, but also in an effort to evade detection by security software and circumvent system policies. Much of this malware is signed with stolen certificates, while other binaries are self-signed or 'test signed.' Test signing is sometimes used as part of a social engineering attack."[1]

This quarter more than 200,000 new and unique malware binaries have been found with valid digital signatures. In our *2012 Threats Predictions* we foresaw that this technique, likely inspired by the success of Duqu and Stuxnet, would rise.[2] After three months it certainly seems to be coming to fruition.

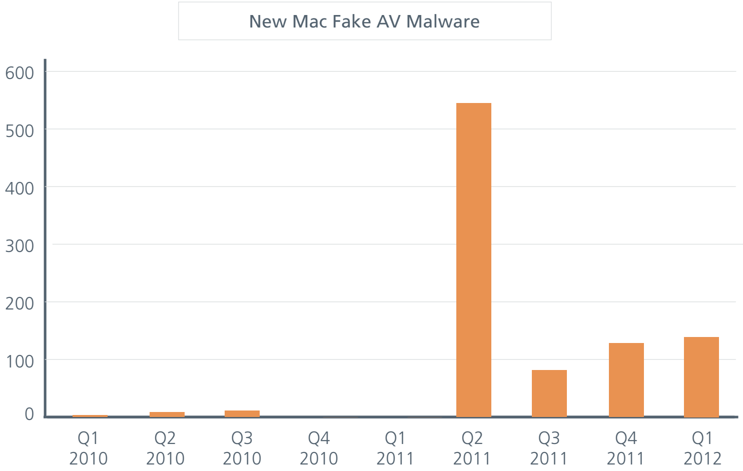




Malware for Apple's Mac continues to show consistent growth. As always, malware on the Mac appears relatively tame when compared with PC malware, but malware can be written for any operating system and platform. All users must take precautions.



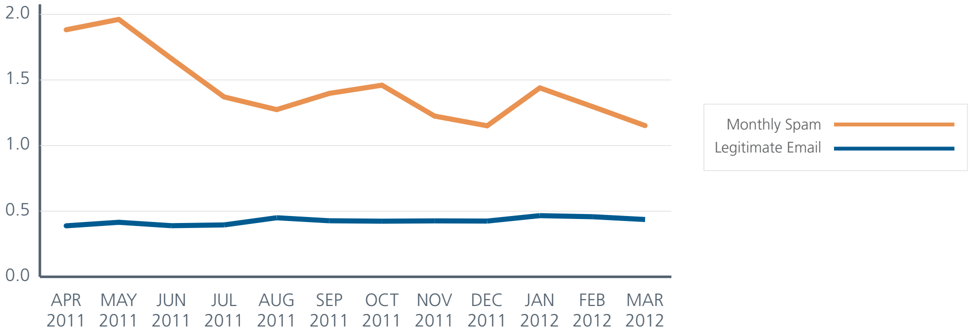
After its big spike in the middle of last year, Fake AV malware for the Mac has apparently found some consistency.



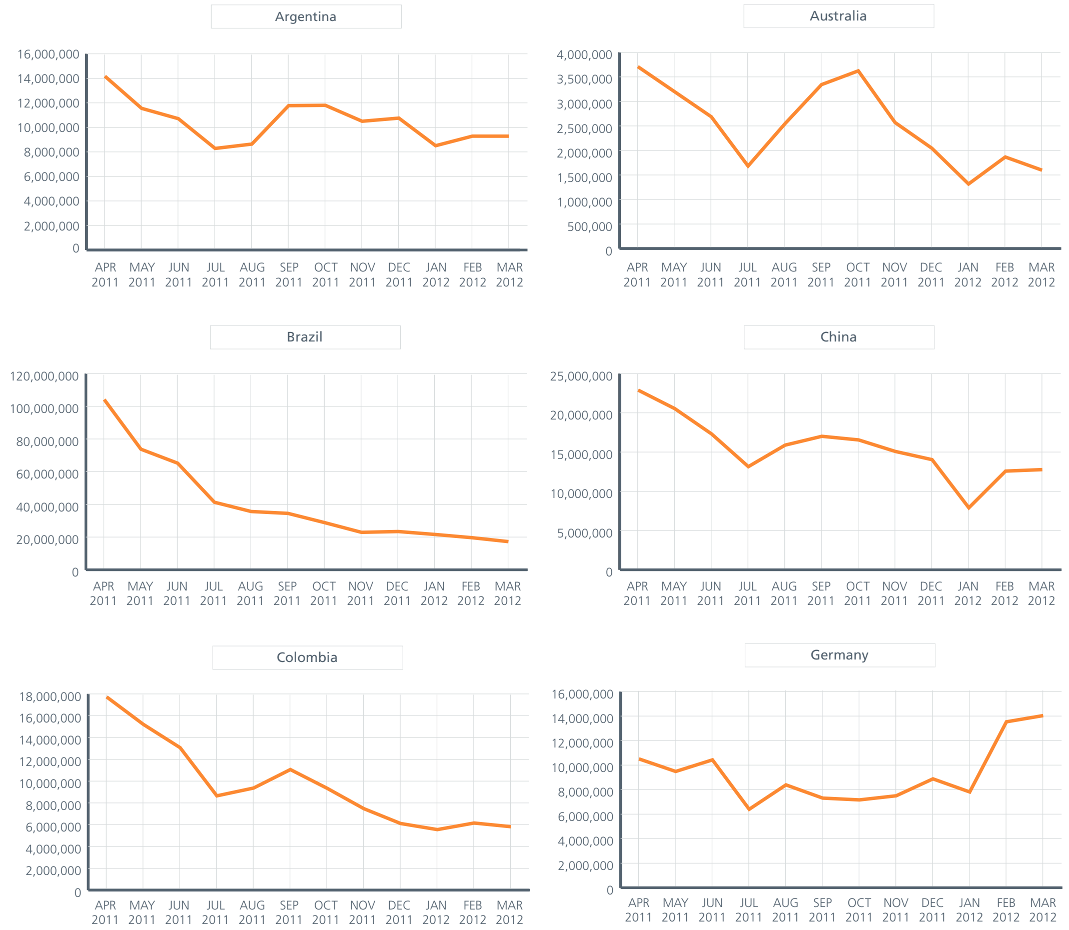
Messaging Threats

We noted in our last edition that we saw spam levels reach record lows at the end of 2011. Although another spike occurred in January, by the end of the quarter spam levels had again fallen to the lows of the previous period. In the last three months, we observed increases in China, Germany, Poland, Spain, and the United Kingdom; but volumes in Brazil, Indonesia, and Russia declined. Despite global levels dropping, spearphishing and spam are as dangerous as ever; consumers and businesses must remain vigilant. The sophistication of today's threats remains high.

Global Email Volume, in Trillions of Messages



Spam Volume



Argentina

Australia

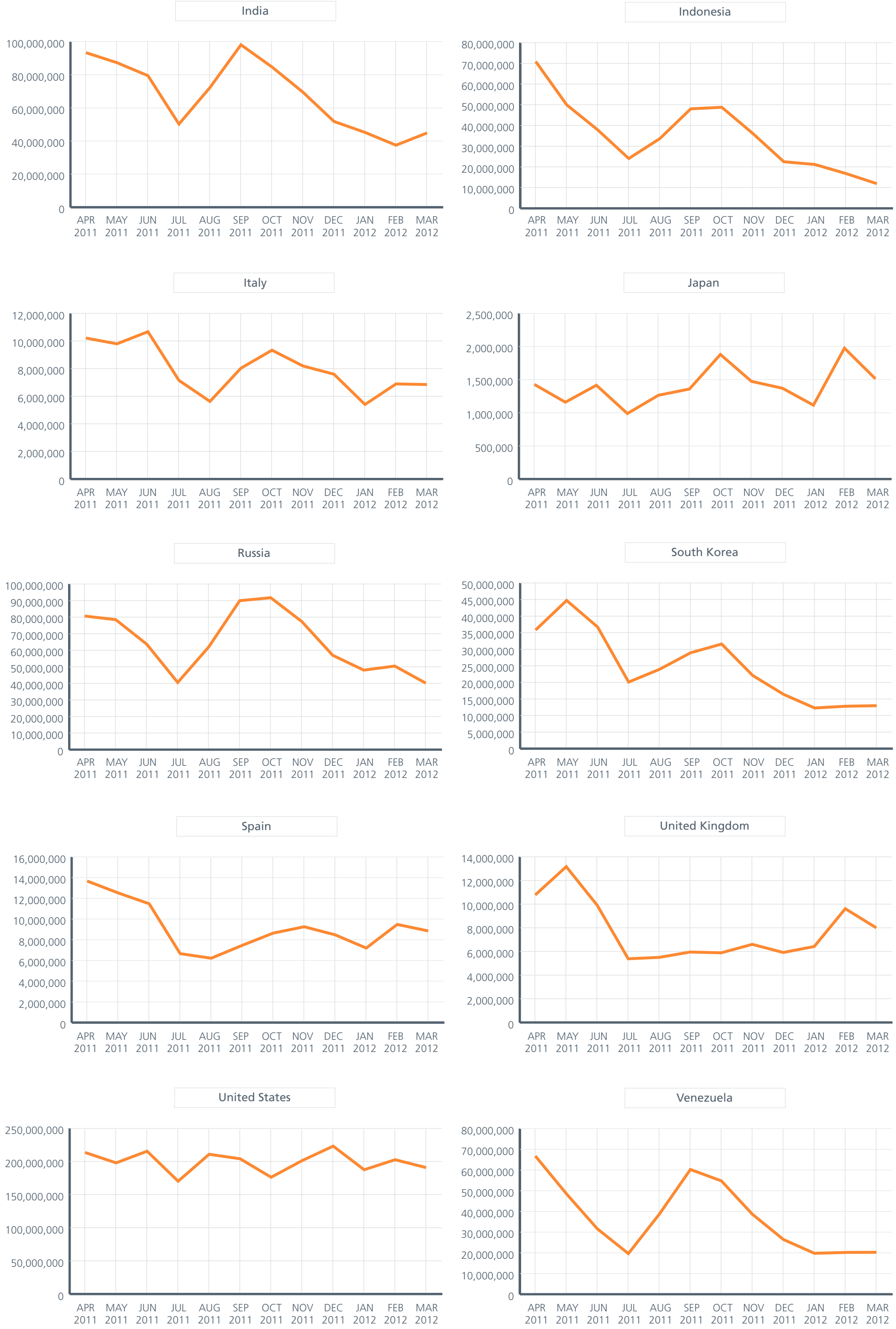
Brazil

China

Colombia

Germany

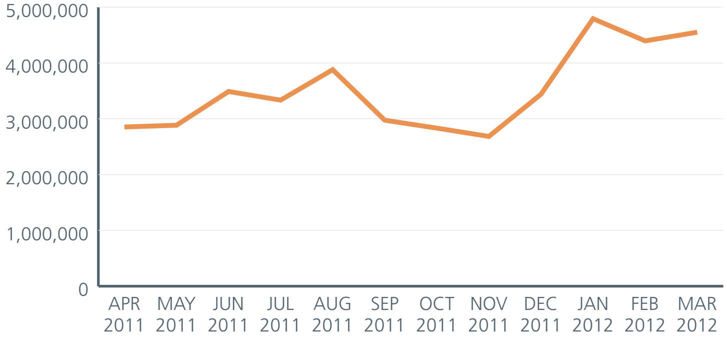
Spam Volume


India
0
20,000,000
40,000,000
60,000,000
80,000,000
100,000,000
Indonesia
0
10,000,000
20,000,000
30,000,000
40,000,000
50,000,000
60,000,000
70,000,000
80,000,000
Italy
0
2,000,000
4,000,000
6,000,000
8,000,000
10,000,000
12,000,000
Japan
0
500,000
1,000,000
1,500,000
2,000,000
2,500,000
Russia
0
10,000,000
20,000,000
30,000,000
40,000,000
50,000,000
60,000,000
70,000,000
80,000,000
90,000,000
100,000,000
South Korea
0
5,000,000
10,000,000
15,000,000
20,000,000
25,000,000
30,000,000
35,000,000
40,000,000
45,000,000
50,000,000
Spain
0
2,000,000
4,000,000
6,000,000
8,000,000
10,000,000
12,000,000
14,000,000
16,000,000
United Kingdom
0
2,000,000
4,000,000
6,000,000
8,000,000
10,000,000
12,000,000
14,000,000
United States
0
50,000,000
100,000,000
150,000,000
200,000,000
250,000,000
Venezuela
0
10,000,000
20,000,000
30,000,000
40,000,000
50,000,000
60,000,000
70,000,000
80,000,000
APR 2011
MAY 2011
JUN 2011
JUL 2011
AUG 2011
SEP 2011
OCT 2011
NOV 2011
DEC 2011
JAN 2012
FEB 2012
MAR 2012

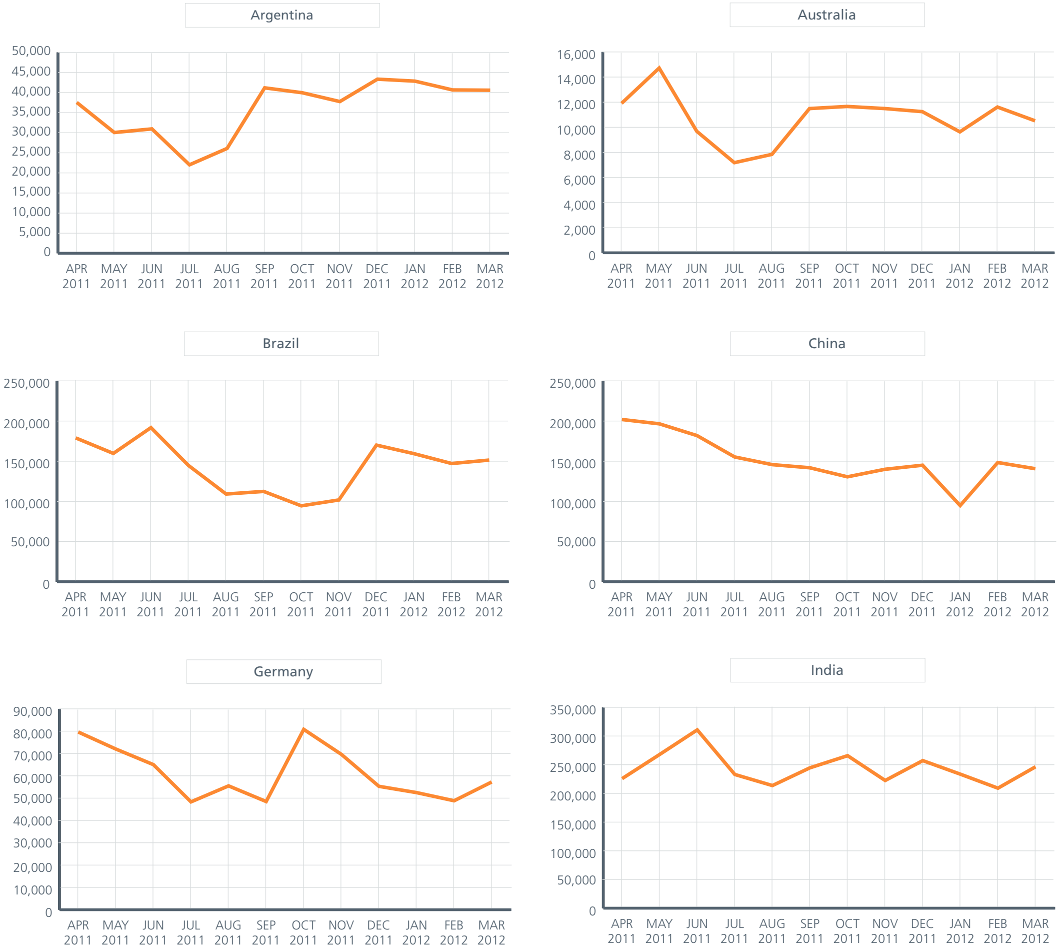
Botnet Breakdowns

Overall messaging botnet growth jumped up sharply from last quarter. Infections rose in Colombia, Japan, Poland, Spain, and the United States. Indonesia, Portugal, and South Korea continued to decline.

Global Botnet Infections



New Botnet Senders



Argentina

Australia

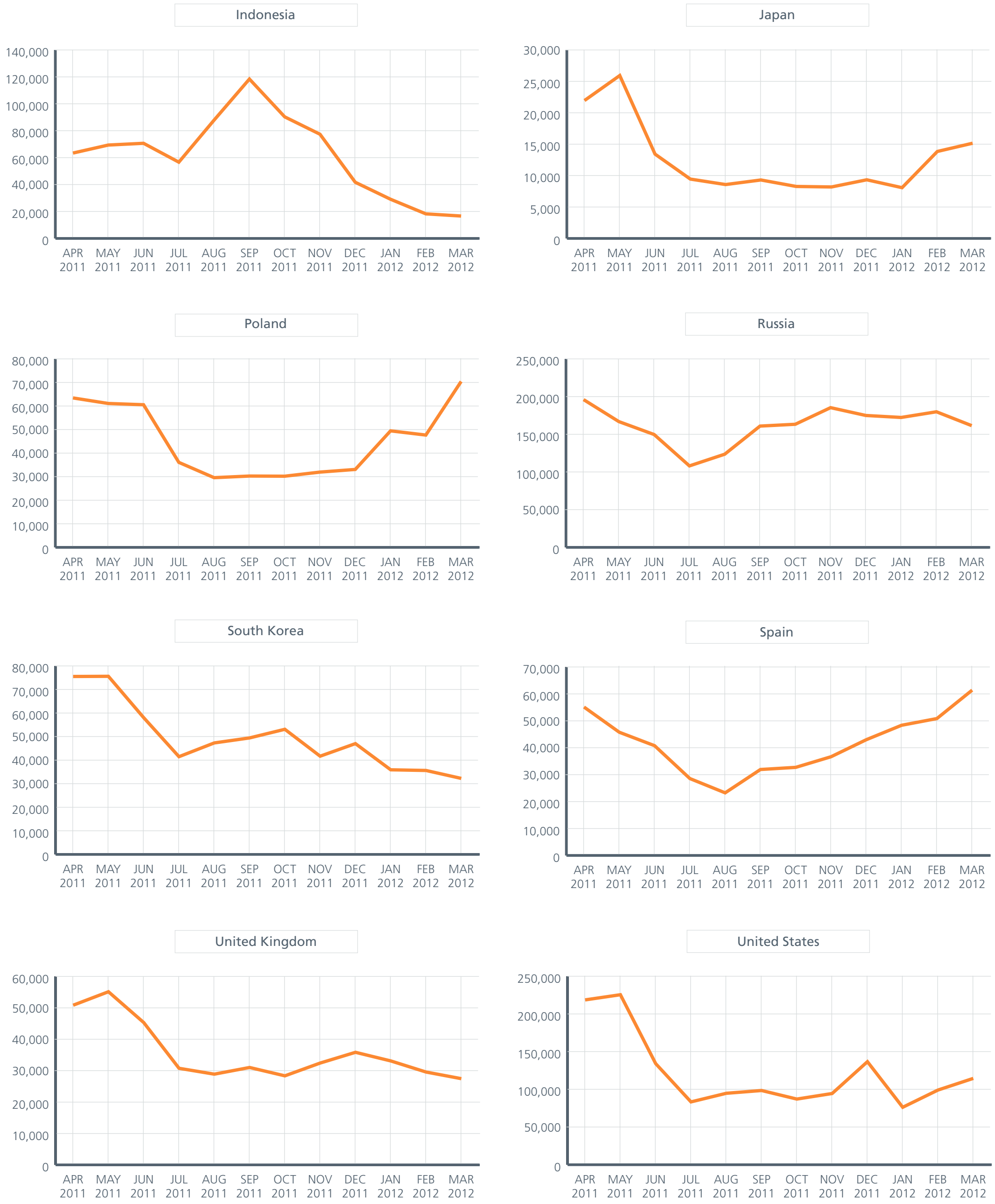
Brazil

China

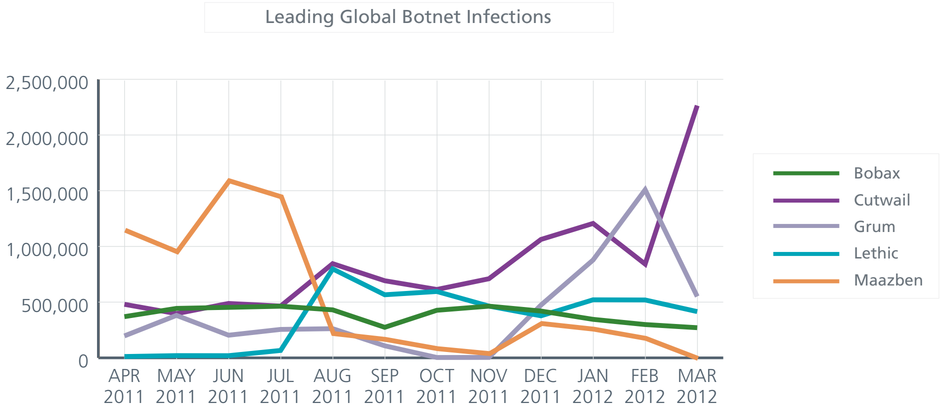
Germany

India

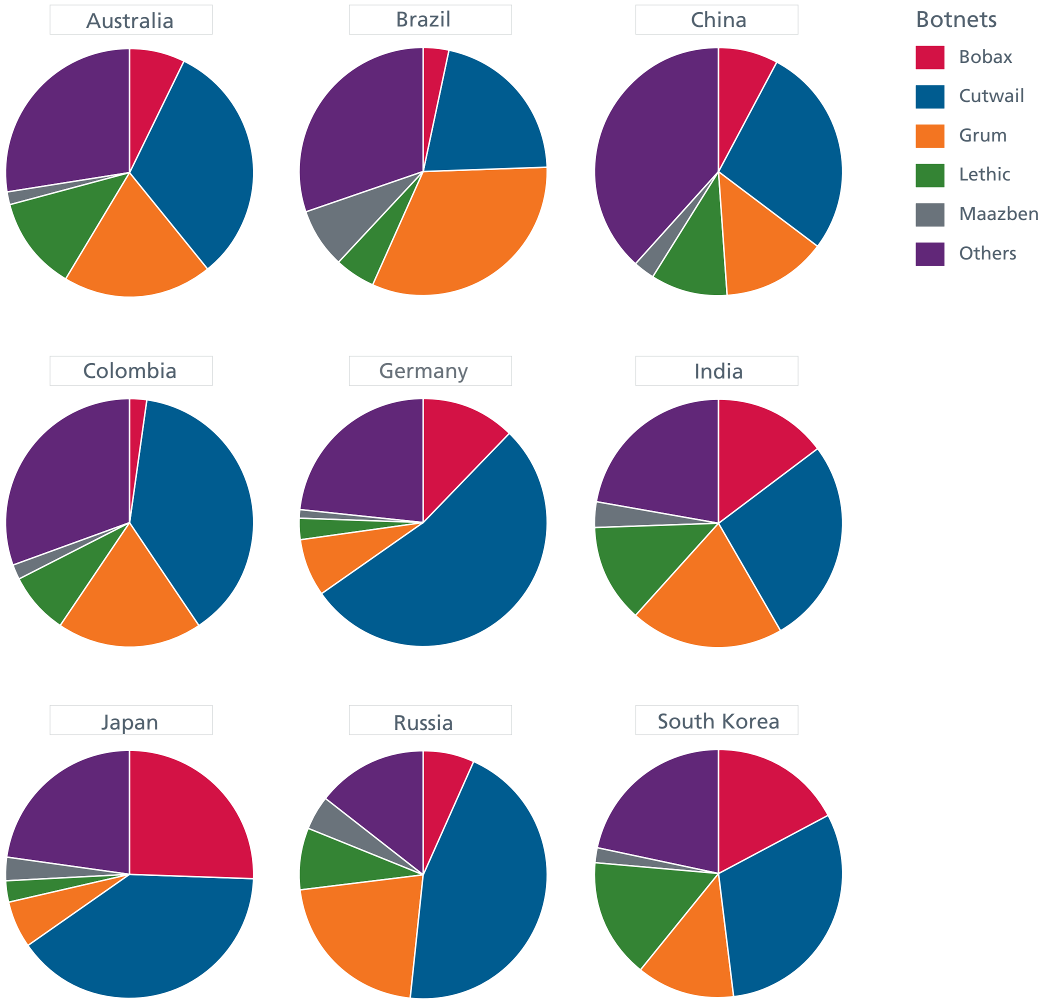
New Botnet Senders

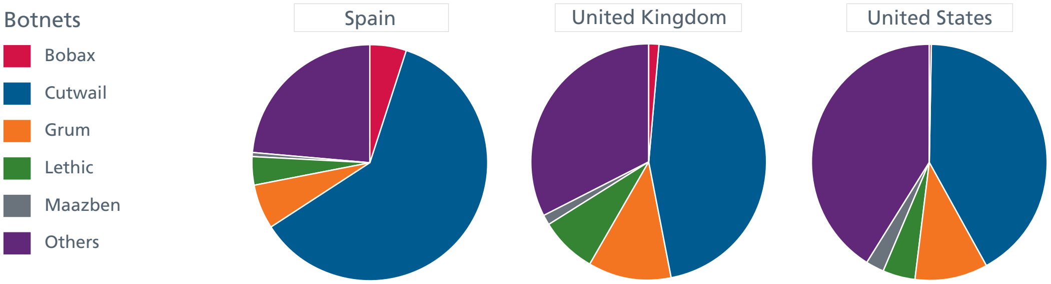


Many of the leading messaging botnets this quarter showed flat growth or a decline in new infections—with the exception of Cutwail, which increased significantly.

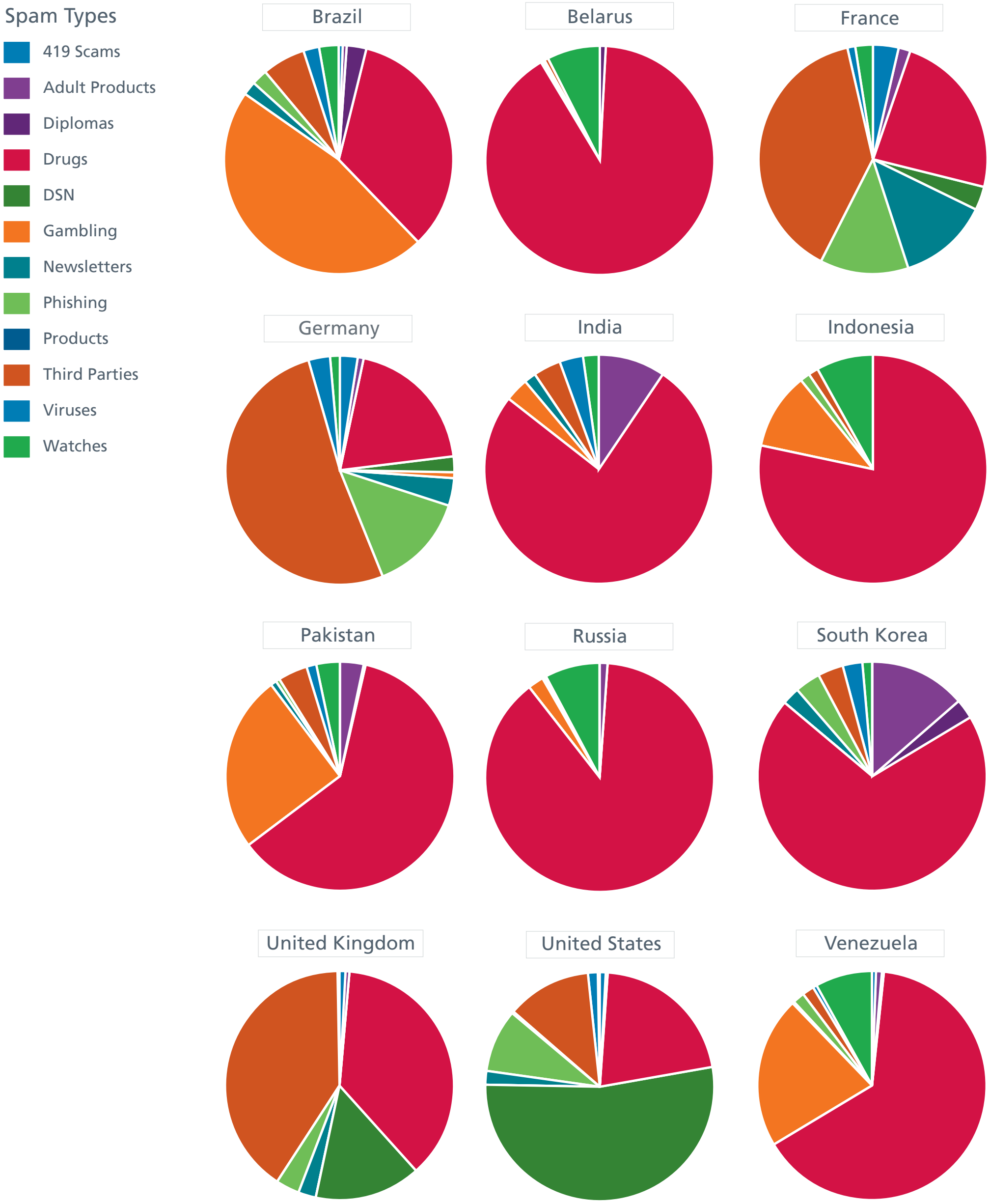


Remember that *new* infections do not mean that current infections have gone away. Our breakdown of botnets by country shows that many of these botnets are still quite active around the world, even though the rate of new infections may be on the decline. Cutwail is the global leader in new infections and in current infections except in Brazil, where Grum is most prevalent.





As always, social engineering lures and spam subject lines vary greatly depending on the part of the world in which we find them. Lures vary by month or season, often taking advantage of holidays, sporting events, and tragedies. In Brazil, gambling-related spam was popular while drug-centric spam was the top subject line in many countries. The United States, on the other hand, was plagued by bogus domain system notifications (DSN). Different lures appeal to different cultures.



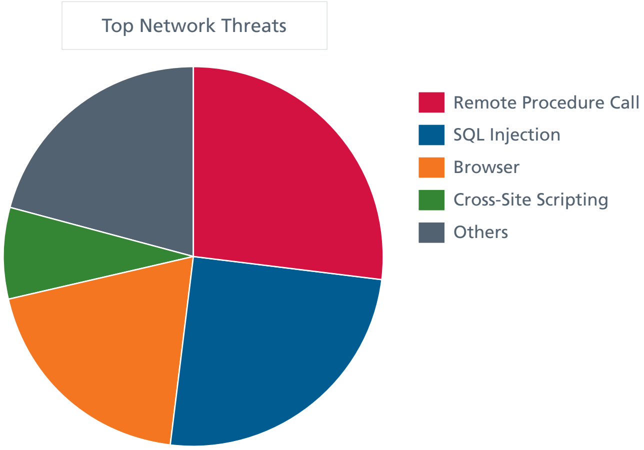
Network Threats

Is the United States the biggest source of cyberattacks? Determining the origination and attribution of attacks is a complex business. Just a few years ago most customers, whether consumer or enterprise, did not ask "Where did this attack come from?" or "Who is responsible for this attack?" Today we hear these queries, yet it's difficult to answer them accurately. Most attribution or attack sourcing relies heavily on IP addresses and basic geographic functions. These elements are a good start, but no more than a start because location or IP address does not imply identity or actor.

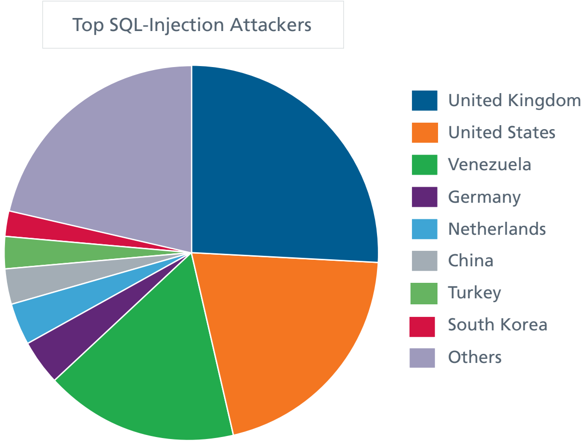
Many times a compromised machine is used as a proxy for spam, botnets, denial of service, or other types of malicious activities. These machines can be located anywhere in the world and, judging by this quarter's numbers, many are located in the United States.

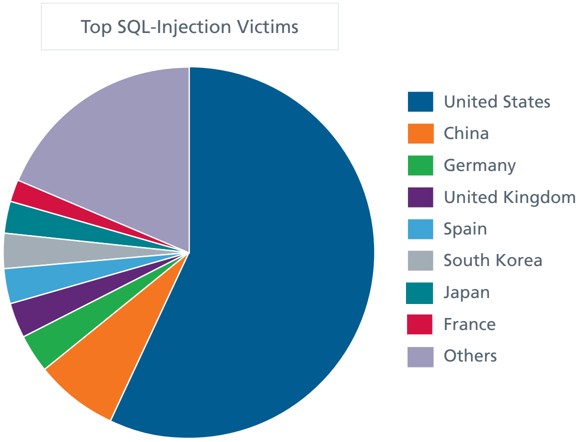
Let's dig into a few areas as collected and analyzed from the McAfee Global Threat Intelligence™ network. We have also significantly expanded our network-based analysis reports for this quarter's Threats Report.

The leading network threats were again remote procedure call and SQL injection attacks. Cross-site scripting threats dropped quite a bit, to 8 percent from 19 percent last quarter.

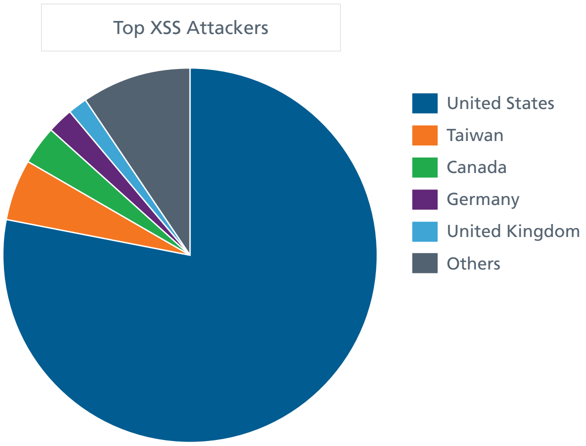


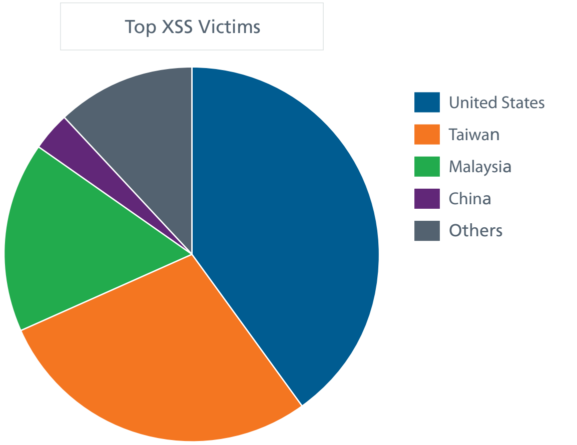
For SQL Injection attacks, the United States took the top spot as the source of attacks as well as the targets.





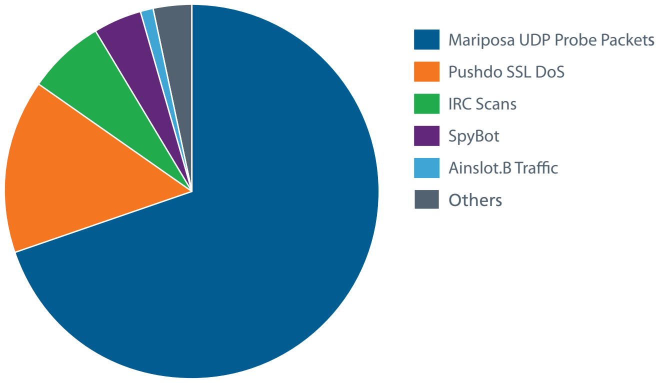
The United States by a large margin topped the list of sources of detected cross-site scripting (XSS) attacks this quarter, and it was also the primary victim country, with Taiwan in second place.





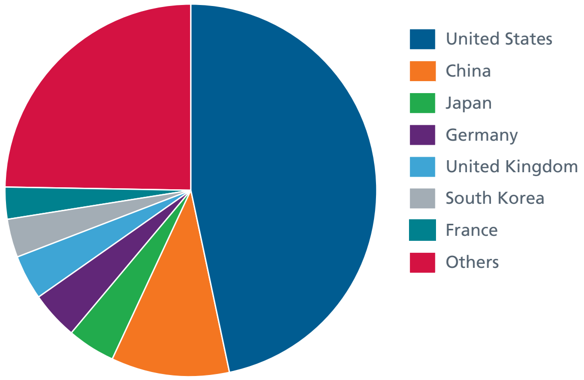
This quarter we have also added a view of top network botnet detections. The clear leader was Mariposa, a financial botnet that steals credit card and banking data. Pushdo (an alias for Cutwail) was a distant second.

Top Botnet Detections



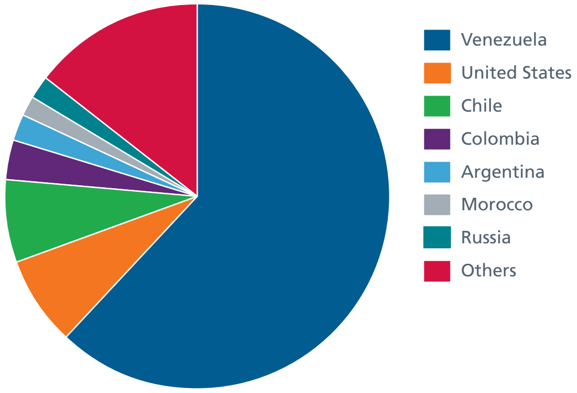
The United States topped another of our network lists. Almost half of new botnet control servers detected by McAfee Global Threat Intelligence reside in the United States.

Top Botnet Control Servers



Botnet victims, also a new section for this report, were most prevalent in Venezuela, with the United States well behind in second place.

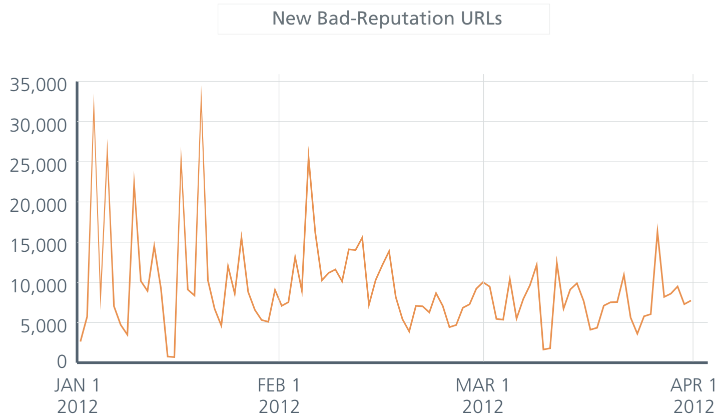
Top Botnet Victims



Web Threats

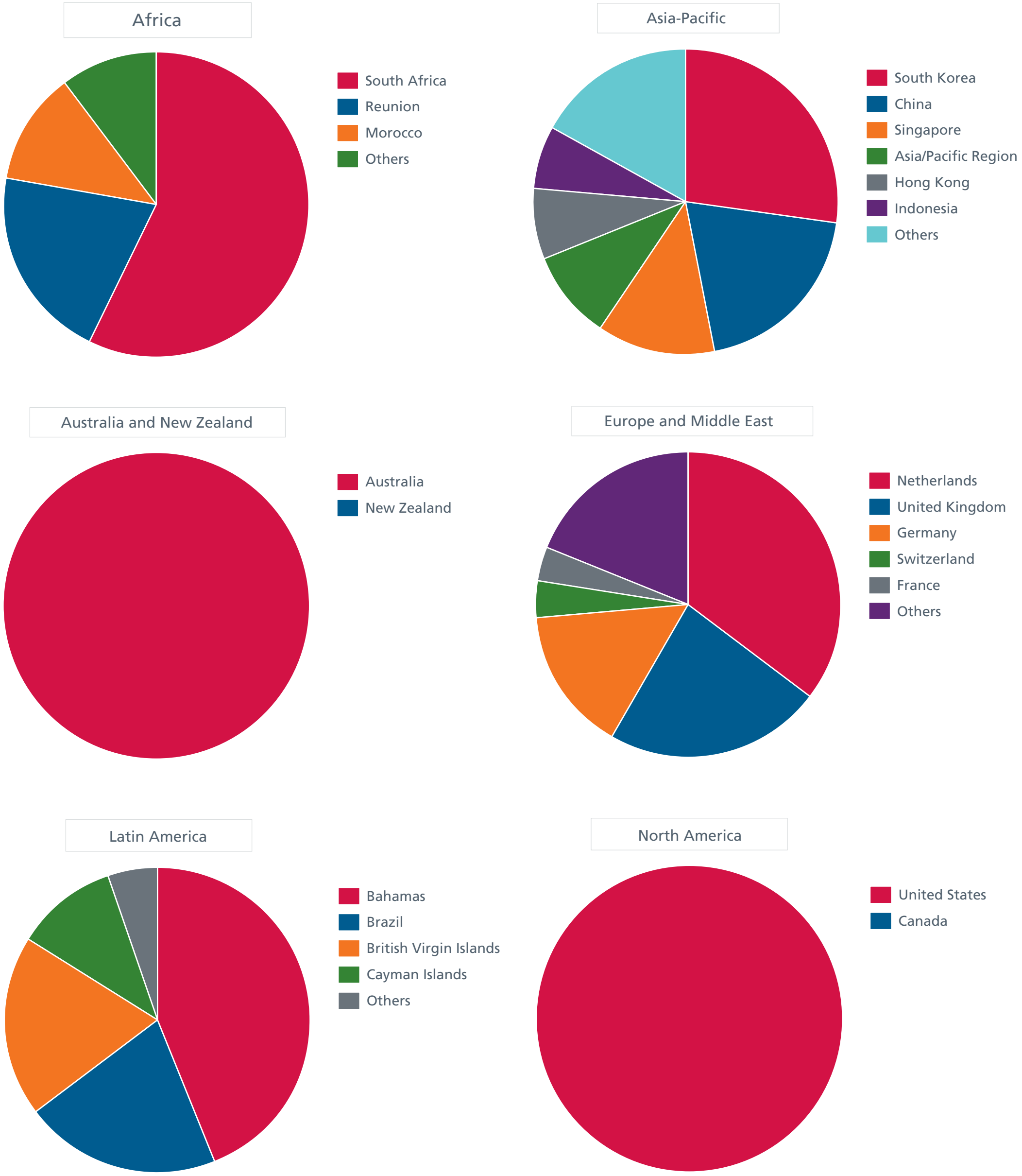
Websites can gain bad or malicious reputations for a variety of reasons. Reputations can be based on full domains and any number of subdomains, as well as on a single IP address or even a specific URL. Malicious reputations are influenced by the hosting of malware, potentially unwanted programs, or phishing sites. Often we observe combinations of questionable code and functionality. These are several of the factors that contribute to our rating of a site's reputation.

Last quarter McAfee Labs recorded an average of 9,300 new bad sites per day. Including spam email URLs, this figure reached 11,000 hits per day. During this period, however, the latter figure dropped to 9,000 hits per day.



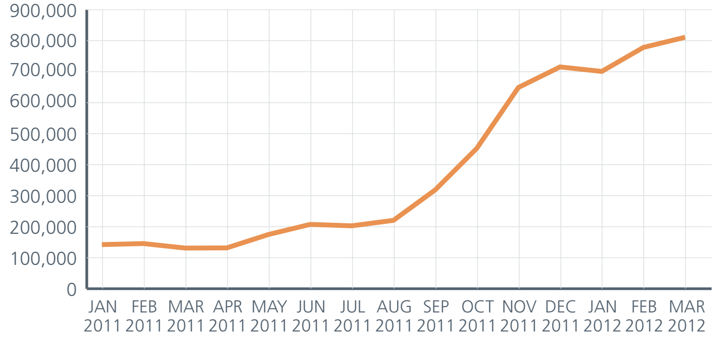
Although the number of "bad" URLs is decreasing, the number of our customers being directed to malicious websites is increasing. Last quarter, McAfee on average each day prevented a web-based malware attack on one out of eight customers. (The other seven customers did not visit risky sites.) This quarter, however, that ratio increased to one out of six customers. This number held constant throughout the quarter and represents how successful cybercriminals are in redirecting users to their bad sites. The vast majority of new malicious sites are located in the United States. Looking closely by region, we can see that no area of the global Internet is without risk.

Location of Servers Hosting Malicious Content



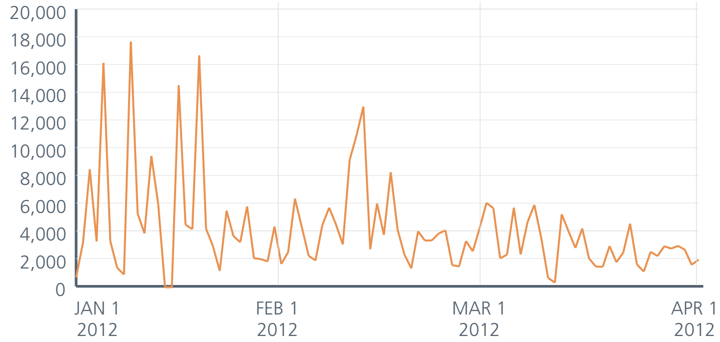
The number of websites hosting malicious downloads or browser exploits is still increasing.

Active Malicious URLs



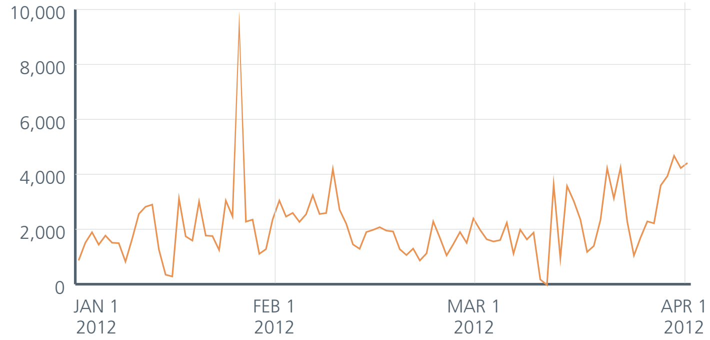
The number of websites delivering malware and potentially unwanted programs dropped by about a third this quarter, with an average of around 4,200 new sites per day, compared with about 6,500 per day during the fourth quarter of 2011.

New Malware Sites



Phishing sites were unchanged from last quarter. We again identified an average of approximately 2,200 new phishing URLs per day this quarter. Phishing sites continue to pose a significant risk to web surfers; more sites host phishing attempts than solely malicious downloads or spam.

New Phishing Sites



Cybercrime

Crimeware tools

This quarter, in addition to the usual updated exploit packs, a wave of newcomers appeared. At first these crimeware tools heavily leveraged the October 2011 disclosure of the Java Rhino vulnerability (CVE-2011-3544) but soon took advantage of two vulnerabilities from this year:

- The MIDI Remote Code Execution Vulnerability in Windows Multimedia Library (CVE-2012-0003), resolved with the January MS012-004 security update.
- The Java Runtime Environment sandbox breach (CVE-2012-0507), remediated in mid-February as part of the Oracle Java SE critical patch update advisory.[3] This exploit is known as Java AtomicReferenceArray.

In the following table only the Phoenix Exploit Kit includes the CVE-2012-0507 Java Atomic exploit. However, on various blogs and forums, we've read about similar updates for BlackHole, Eleonore, and Incognito. We expect many exploits kits to use this vulnerability in the coming months.

Name	Origin	Exploit Details
Sakura 1.0	Russia or Eastern Europe	Three exploits including Java Rhino (CVE-2011-3544)
Hierarchy	Russia or Eastern Europe	16 exploits, with two from 2011: • Flash 10 (CVE-2011-0611) • Java Rhino
Yang Pack January	China	Four exploits, including: • Flash 10.3.181.x (CVE-2011-2110) • Flash 10.3.183.x (CVE-2011-2140) • Java Rhino
Zhi Zhu February	China	Five exploits, including: • HTML+TIME (CVE-2011-1255) • Flash 10.3.181.x • Flash 10.3.183.x • WMP MIDI (CVE-2012-0003)
Gong Da Pack February	China	Three exploits: • Flash 10.3.183.x • Java Rhino • WMP MIDI
Phoenix Exploit Kit 3.1 March	Russia	In our Threats Report for the fourth quarter of 2011, we noted Version 3.0, which included the Java Rhino exploit (CVE-2011-3544). Version 3.1 includes Java Atomic (CVE-2012-0507).

We recommend the Kahu Security blog for those searching for details regarding the preceding Chinese packs.

Bots and botnets

Underground forums offer numerous advertisements for botnet packages. The following tables show that certain botnets command a premium:

Name	Prices (in U.S. dollars)
Darkness by SVAS/Noncenz Distributed Denial of Service (DDoS) bot	Update to Version 10 in January: $120 Packages • Minimum: DDoS bot, no free updates, no modules = $450 • Standard: DDoS bot, 1 month free updates, password grabber module = $499 • Bronze: DDoS bot, 3 months free updates, password grabber module, 1 free rebuild = $570 • Silver: DDoS bot, 6 months free updates, password grabber module, 3 free rebuilds = $650 • Gold: DDoS bot, lifetime free updates, password grabber and "hosts" editor modules, 5 free rebuilds, 8% discount on other products = $699 • Platinum: DDoS bot, lifetime free updates, password grabber module, unlimited free rebuilds, 20% discount on other products = $825 • Brilliant: DDoS bot, lifetime free updates, unlimited free rebuilds, all modules for free, 25% discount on other products = $999 Other: • Rebuild (changing URLs) = $35. • Sources = $3,500–$5,000 • Web-panel reinstallation (first time is free) = $50
Citadel[5] Zeus variant, financial botnet	• Bot builder and admin panel = $2,399 plus $125 monthly "rent" (price as of December 2011) • Automatic update facilities for antivirus evasion = $395. Each update costs $15.
THOR by TheGrimReap3r Multipurpose peer-to-peer botnet	• $8,000 for the package without modules. Discount of $1,500 for the first five buyers. • Expected modules under development are advanced bot killer, DDoS, form grabber, keylogger/password stealer, and mass mailer
Carberp Financial botnet	• Loader, grabbers, all basic functionality (except for the following) = $2,500 • The preceding plus back-connect 500 connections and Internet Explorer and FireFox injection = $5,000 • The preceding plus hidden browser (similar to VNC) = $8,000

The Carberp offer is surprising. It was dated March 21, yet on March 20 Russian authorities announced the arrest of the Carberp gang. (Read the next section for more details.)

Actions against cybercriminals

During this quarter law enforcement and other good guys enjoyed some significant takedowns and actions against cybercriminals. In January, Microsoft filed a complaint against a Saint Petersburg, Russia, inhabitant suspected of controlling the Kelihos (alias Waledac) botnet.[6] According to security maven Brian Krebs, from 2005 to 2007 the suspect was a senior system developer and project manager for a Russian antivirus firm named Agnitum.[7] In an interview with the Gazeta.ru newspaper, the alleged operator denied the charges.[8]

A Russian citizen detained in Zurich, Switzerland, since March 2011 was extradited to New York in January. Along with his son, who remains at large, he has been charged with eight counts of conspiracy, mail fraud, wire fraud, computer fraud, aggravated identity theft, and securities fraud via bogus websites since 2005.[9]

On March 16, the U.S. Secret Service, in coordination with U.S. Immigration and Customs Enforcement, announced the results of "Operation Open Market" against 50 individuals allegedly engaged in crimes such as identity theft and counterfeit credit card trafficking.[10] The suspects were linked in a transnational organized crime operating on multiple cyberplatforms, buying and selling stolen personal and financial information through online forums. All of the defendants are said to be members, associates, or employees of a criminal organization called Carder.su (which also includes Carder.info, Crdsu.su, Carder.biz, and Carder.pro).

On March 20, the Russian Ministry of Internal Affairs and the Federal Security Service (FSB) announced the arrest of eight alleged cybercriminals who reportedly stole more than 60 million rubles (US$2 million) from at least 90 victims' bank accounts with the help of the Carberp Trojan.[11]

Two men, arrested in May 2011, were charged in March in the United Kingdom with hacking into Sony Music's computers and stealing music valued at approximately GB£160 million.[12] Britain's Serious Organised Crime Agency said the hacking reportedly took place last year just as other hackers accessed the PlayStation Network, and downloaded personal information from 77 million registered users. This case is not believed to be linked to Anonymous or LulzSec attacks.

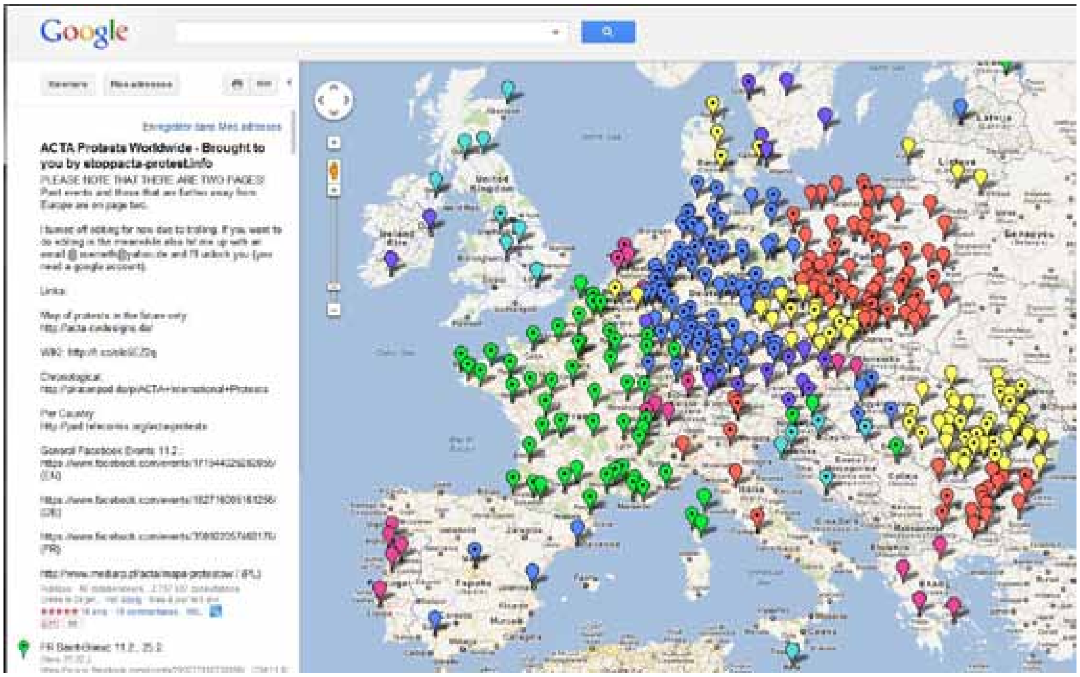
This quarter, several Anonymous members or affiliates were the target of law enforcement operations. After the LulzSec member "Sabu" pleaded guilty in August 2011 and cooperated with FBI, law enforcement agents caught other top members of the computer hacking group. The suspects—who included two men from the United Kingdom, two from Ireland, and two from the United States—were indicted in the Southern District of New York.[13] Earlier in the quarter, Interpol announced the arrest of 25 suspected members of Anonymous in Argentina, Chile, Colombia, and Spain.[14] W0rmer and Kahuna, two members of CabinCr3w, a hacker group close to Anonymous, were arrested on March 20 in the United States.[15]

This quarter we saw that not only the police can disrupt cybercriminal operations. In a January post, the famous researcher Dancho Danchev exposed the identity and data he discovered about a Russian individual linked to the gang behind Koobface.[16] Some days later, *The New York Times* disclosed four other names that a group of security researchers had planned to announce.[17]

We close with Microsoft's Operation B71, which focused on botnets using Zeus, SpyEye, and Ice-IX variants. On March 23, Microsoft unveiled a joint lawsuit with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the National Automated Clearing House Association (NACHA). Microsoft and its agents captured four hours of network traffic and seized servers from two hosting locations in Pennsylvania and Illinois. In addition, more than 1,700 domain names were analyzed to understand their role in this business.[18]

Hacktivism

Aside from events surrounding the arrest of Sabu, attacks in reply to the forced closure of Megaupload were the big news in hacktivism this quarter. Through Twitter accounts and press releases, Anonymous claimed that its OpMegaupload had thousands of people taking part in the takedown of several websites, namely those of the Department of Justice, Recording Industry Association of America, Motion Picture Association of America, BMI, and the FBI. Perhaps more interesting is that in Europe Anonymous was also able to mobilize their sympathizers in the street. Taking the closing of Megaupload as a pretext, demonstrations organized by Anonymous protested on February 11 and February 25 against the controversial SOPA, PIPA, and ACTA laws in more than 100 cities in about 15 countries. This was certainly an interesting mix of digital-based hacktivism and physical world activism. Could this be a portent of things to come?



ACTA Protests Worldwide - Brought to you by stopacta-protest.info

PLEASE NOTE THAT THERE ARE TWO PAGES! Past events and those that are farther away from Europe are on page two.

I turned off editing for now due to trolling. If you want to do editing in the meanwhile also hit me up with an email @ [illegible] and I'll unlock you (you need a google account).

Links:

Map of protests in the future only
http://acta.cedesigns.de/

WIKI: [illegible]

Chronological:
http://piratenpad.de/p/ACTA+International+Protests

Per Country:
[illegible]

General Facebook Events 11.2.:
[illegible]
(EN)

[illegible]
(DE)

[illegible]
(FR)

http://www.mediarp.pl/acta/mapa-protestow/ (PL)

FR Bordeaux 11.2., 25.2.

Anti-ACTA demonstrations were widespread in Europe on February 11.

This quarter, we also noticed dozens of scattered operations around the globe. None had a great impact, and it is difficult for us to highlight some of them:

- #OpGlobalBlackout on March 31 came and went with no global blackout. Security researchers were in almost full agreement that it was never a technically feasible attack. However, it is interesting to note the sheer amount of coverage and discussion this #Op generated. Anonymous continues to show it can shape the news with its media savvy.
- The ArcelorMittal hack: Reacted to the decision to close down two blast furnaces in the Belgian city of Liège[19]
- The Vatican DDoS: An attack not against Catholics around the world, but against the "corrupt" Church[20]
- The Anonymous-OS Linux release immediately announced as a fake[21]

About the Authors

This report was prepared and written by Zheng Bu, Toralv Dirro, Paula Greve, Yichong Lin, David Marcus, François Paget, Craig Schmugar, Jimmy Shah, Dan Sommer, Peter Szor, 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://blogs.mcafee.com/mcafee-labs/signed-malware-you-can-runbut-you-cant-hide
[2] http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf
[3] http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html
[4] http://www.kahusecurity.com/
[5] http://krebsonsecurity.com/2012/01/citadel-trojan-touts-trouble-ticket-system/
[6] http://blogs.technet.com/b/microsoft_blog/archive/2012/01/23/microsoft-names-new-defendant-in-kelihos-case.aspx
[7] http://krebsonsecurity.com/2012/01/microsoft-worm-author-worked-at-antivirus-firm/
[8] http://en.gazeta.ru/news/2012/03/07/a_4030561.shtml
[9] http://www.justice.gov/usao/nys/pressreleases/January12/zdoroveninvladimirandzdoroveninkirillindictmentpr.pdf
[10] http://www.secretservice.gov/press/GPA03-12_OpenMarket2.pdf
[11] http://garwarner.blogspot.fr/2012/03/russian-mvd-announces-arrest-of-carberp.html
[12] http://www.huffingtonpost.com/2012/03/05/michael-jackson-hacking-james-marks-james-mccormick_n_1321912.html
[13] http://www.smashtheman.com/2012/03/news/the-legal-attack-against-anonymous-and-lulzsec
[14] http://www.interpol.int/News-and-media/News-media-releases/2012/PR014
[15] http://blogs.mcafee.com/mcafee-labs/hacker-leaves-online-trail-loses-anonymity
[16] http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html
[17] http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html
[18] http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx
[19] http://www.cyberguerrilla.info/?p=3747
[20] http://geeks.thedailywh.at/2012/03/07/geek-news-anonymous-vatican-hack-of-the-day/
[21] http://www.tomshardware.com/news/Anonymous-Anonymous-OS-Viruses-Trojans-Fake,15027.html

McAfee
An Intel Company

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