Report

McAfee® Labs Threats Report: Third Quarter 2013

Table of Contents

Overview

McAfee Labs researchers have analyzed the threats of the third quarter of 2013. We've seen several familiar trends; others are new:

- Steady growth in mobile and overall malware
- A sharp upturn in worldwide spam
- An increase in the use of digital currencies by cybercriminals to maintain anonymity for their illegal activities
- The shutdown of the online market Silk Road, which sold drugs and other illegal products
- The emergence of the "Deep Web," an online supply for cybercriminals

The McAfee report *Digital Laundry: An analysis of online currencies, and their use in cybercrime*[1] looks into online currencies and the advantages they offer criminals to buy and sell drugs, malware exploits, and other services without using traceable credit cards or other common forms of payment. Law enforcement and the courts are striking back; but as one currency dies, another takes its place.

Our timeline of significant hacks shows the major criminal activity that took place this quarter. Online currency Bitcoin remained in the news. In addition to our profile in Digital Laundry, we highlight recent Bitcoin events, including hidden attempts to hijack systems to "mine" further Bitcoins and judgments regarding the currency's legal status.

The shutdown of the online black market Silk Road was a victory for law enforcement. However, at least one similar site sprang up within hours of Silk Road's disappearance. We examine some of the features of the Deep Web, where online criminals operate mostly unimpeded. It's disturbing to find weapons, child pornography, and even murder-for-hire available for a price.

Activist hackers defaced sites and inspired counterattacks from their opponents. The Middle East was a busy region for political expression, with the Syrian Electronic Army again making headlines by hacking *The New York Times* and other targets.

Our count of mobile malware rose by 33 percent this quarter. New malware of all types exceeded 20 million this period, pushing our all-time tally to more than 172 million binaries. New rootkits, which tunnel into systems and remain hidden, doubled in number this quarter. AutoRun threats, often spread via USB drives, remain numerous. Signed malware, which poses as approved legitimate software, continues to set records, increasing by almost 50 percent.

Ransomware, which holds a computer hostage until the victim pays to free it, is a bad problem getting worse. The number of new samples declined a bit from last quarter, but the overall numbers remain very high. Not only do criminals make relatively safe money from this scheme, they often do not remove their malware—leaving the poor victims' systems as dead as before.

From the McAfee Global Threat Intelligence network we see that browser-based threats, such as hidden iframes and malicious Java code, comprise almost half of the Internet's malicious activity.

Our analysis of web threats found that the number of new suspicious URLs, many in the United States, increased by 14 percent this quarter. The leading industries suffering phishing attacks are online-auction and financial organizations. Spam levels are rising rapidly: This quarter volume reached 4 trillion messages in September, the highest figure we've seen since 2010. We continue to report on the variety of spam subjects and botnet prevalence in selected countries around the world.

Digital Laundry

A fresh report from McAfee examines the role that "Internet money" plays in supporting crime. In *Digital Laundry: An analysis of online currencies, and their use in cybercrime*,[2] we learn that recent actions by law enforcement, and the charges brought by prosecutors, add weight to the theory that digital currencies are a key service for criminals to launder money.

Before its operations were closed, the Liberty Reserve digital currency service was used to launder US$6 billion, a sum that constituted the largest international money-laundering prosecution in history. However, Liberty Reserve is not the only virtual currency that has been used by criminals, and the proliferation of these services helps fuel the growth in cybercrime, and other forms of digital disruption. Further, the challenges facing such currencies go beyond their propensity for use within money laundering—with targeted attacks on financial exchanges, and malware developed to target digital wallets.

Some currencies, such as Bitcoin, allow the creation of new currency through a process known as mining. While initially people used their own computing resources for mining, in June 2011 a JavaScript Bitcoin generator (miner), allowed high-traffic sites to employ visitors' computers to produce Bitcoins. Although in some cases the site would explain this to visitors, the procedure could be done without their knowledge as well—in effect creating malicious bots. One rogue employee of the E-Sports Entertainment Association installed such a miner on some 14,000 computers to secretly mine Bitcoins.

The European Central Bank (ECB) points out notable differences between virtual currency and electronic money schemes. Electronic money uses a traditional unit of currency and is regulated; virtual currencies are unregulated and use an invented currency.

In the report *Redefining Virtual Currency*,[3] the Yankee Group estimated that the virtual currencies market has grown to US$47.5 billion in 2012, and projected a further increase of 14 percent during the next five years to as much as US$55.4 billion in 2017. The report went on to suggest that this remarkable growth can largely be attributed to the proliferation of mobile devices, which hints at an expanding noncriminal market.

Virtual currencies offer a number of benefits to customers: They are reliable, relatively instant, and anonymous. Even when privacy issues have been raised with particular currencies (notably Bitcoin), the market has responded with extensions to provide greater anonymity. Market response is an important point because regardless of law enforcement actions against virtual currency companies, users quickly identify new platforms to launder their funds; shutting down the leading platform will not solve the problem.

Attempts to close down virtual currency services have historically resulted in criminals simply moving their businesses elsewhere, with the migration to and from Liberty Reserve serving as an example. Despite such an attractive proposition for criminals, global law enforcement is collaborating in its efforts both internationally and with the private sector to identify, seize, and arrest those individuals operating such platforms for money laundering.

Virtual currencies will not go away. Despite the apparent challenges posed by denial of service attacks, the use of these exchanges for money laundering, and the facilitation of cybercrime, opportunities also abound for legitimate uses. Ignoring this market opportunity is likely to cost potential legitimate investors significant revenue, but failure to address the potential risks may cost a lot more.

Cybercrime

Browsing underground: Delving into the Deep Web

Sefnit botnet

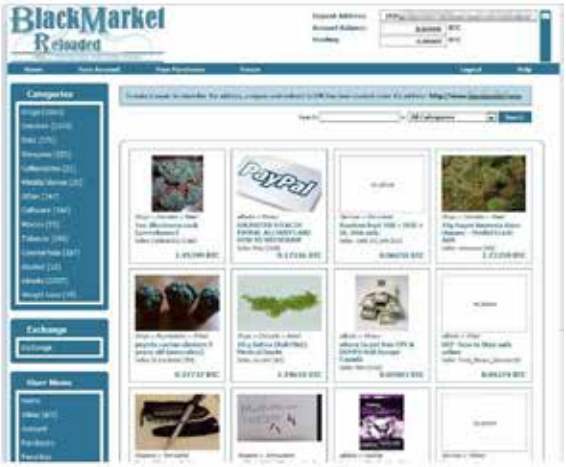
Since mid-August the anonymity network Tor has grown from 500,000 users per day to around 4 million per day. This increase is attributed to a botnet whose components are known as Mevade or Sefnit. According to some reports, this botnet seems to be run by a Ukrainian gang specializing in click fraud.

Deep Web Marketplaces

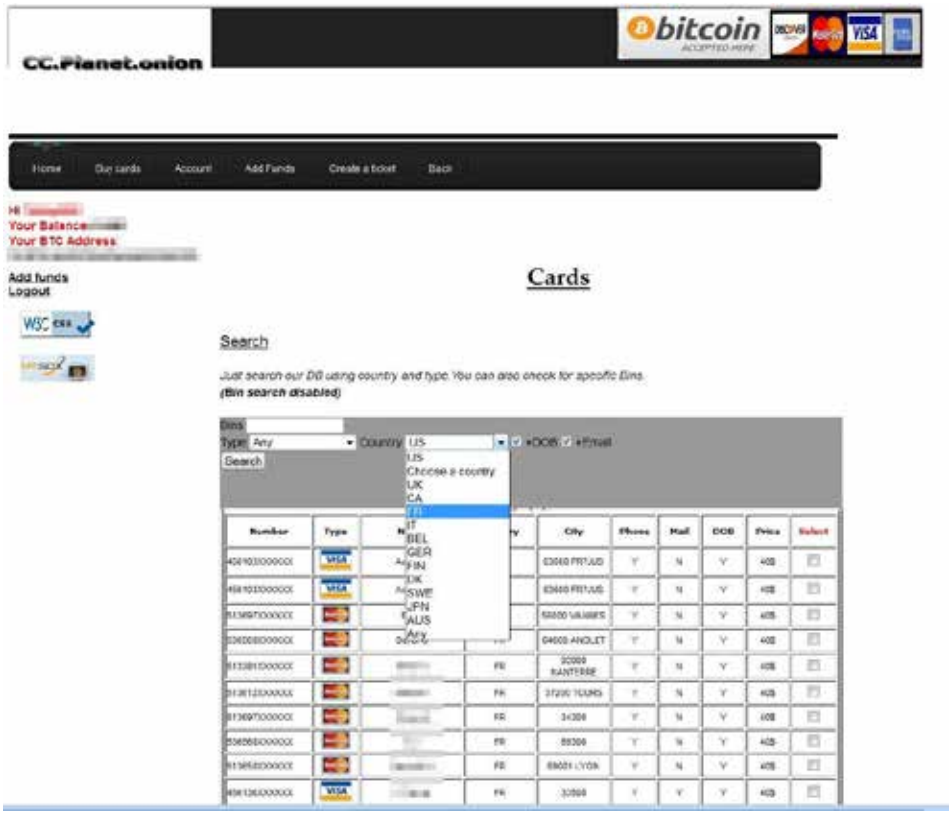
When researchers speak about Tor, the Deep Web, and Bitcoin, they often highlight the underground marketplace Silk Road. Created in February 2011 but closed by the US Federal Bureau of Investigation on October 1,[4] this online cybercrime supermarket operated solely on Bitcoin. It was a bazaar, like eBay or Craigslist, in which those who wished to sell or buy could connect. This location was primarily known as a drug market, but goods were available in more than 200 categories, including other illegal services such as hacking ATMs.

Today, Silk Road is gone, but it was only the tip of the iceberg. Thousands of other locations welcome Bitcoin as payment. Let's look at a few others.

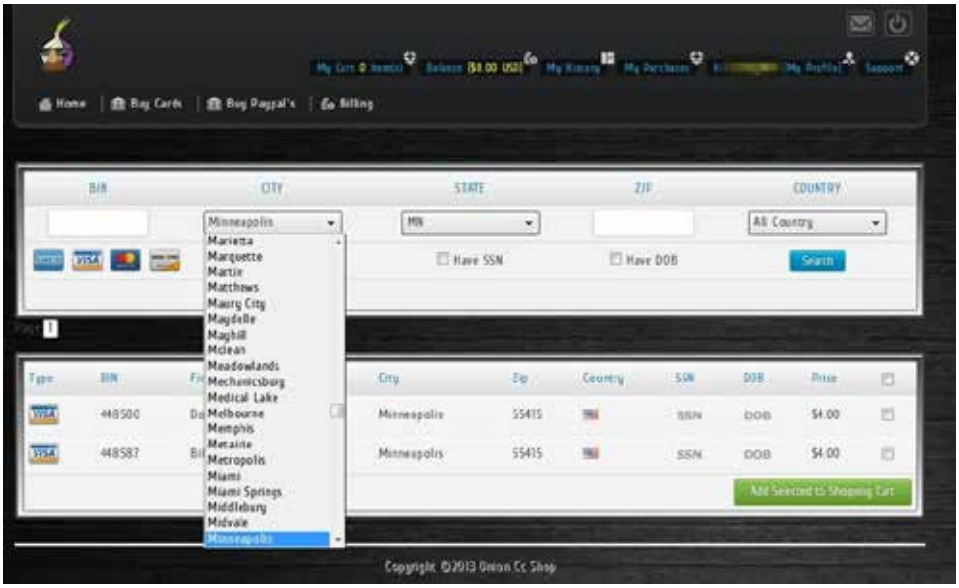
Silk Road had competitors that are still active. Some of them present their products according to the same model as Silk Road:



Elsewhere, online shoppers can buy European premium credit cards. The example below is from France. The price is US$40 (0.3 BTC) each:



US credit cards are less expensive (about US$4). The following screenshot is from another well-stocked service, in which a buyer can search by state and city:

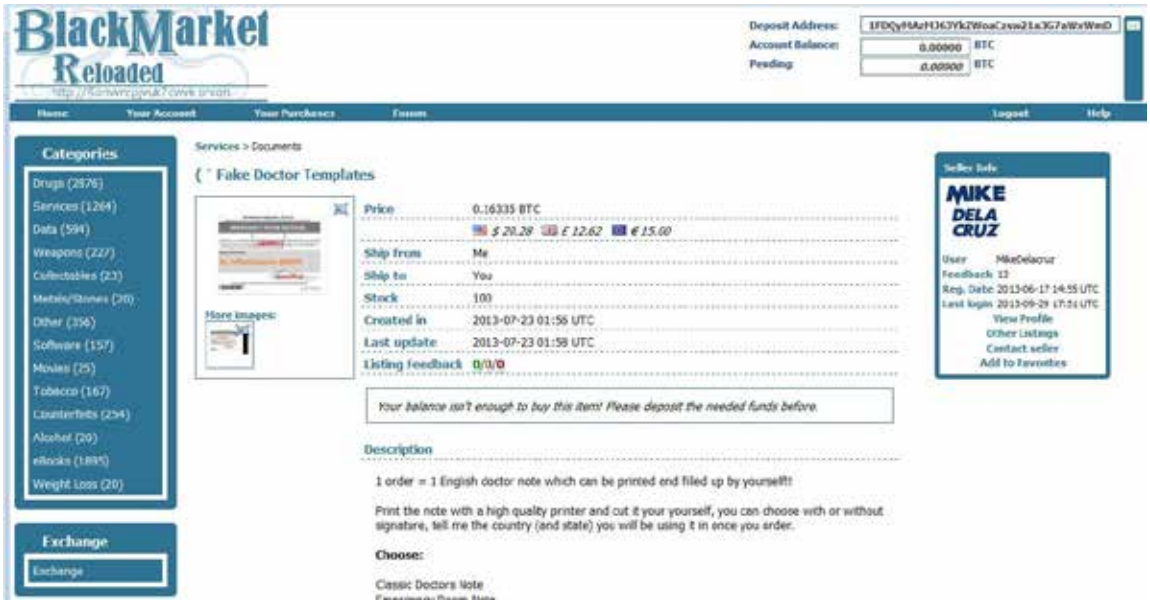


European citizens can buy weapons:

Some examples:

- A Walther PPK, 7.65mm, for €600 (5.8 BTC)
- A Desert Eagle IMI, .44 caliber, for €1,250 (12 BTC)
- A SIG Sauer P226 AL SO DAO, 9mm, for €790 (7.7 BTC)

It is also possible to find false papers, such as this fake doctor template:

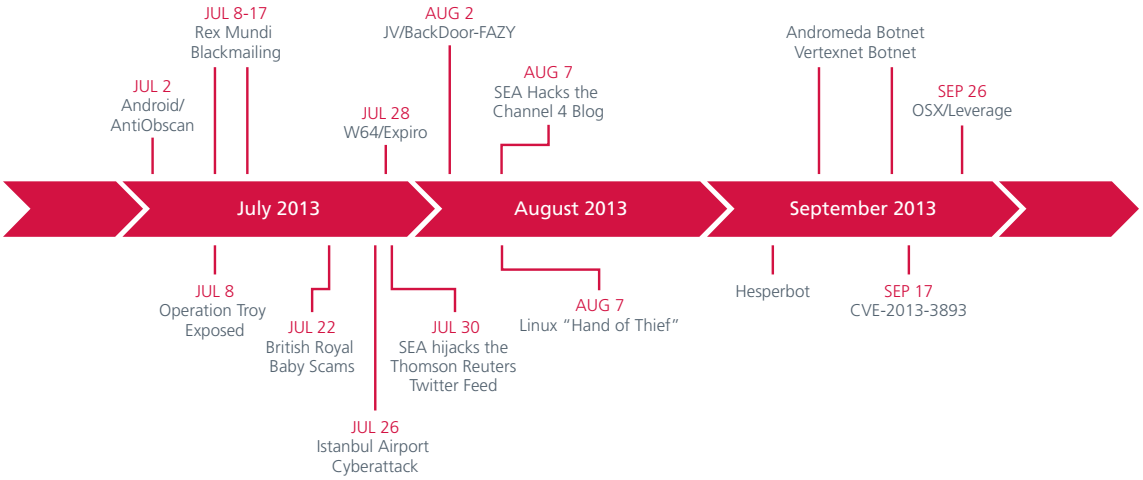


It seems a buyer can even pay for murder. There is no indication that such an offer would actually fulfill its promise (the site is now unreachable), and verifying this would likely come at some personal risk. Still, such sites demonstrate that confidence in the privacy of virtual currencies has enabled the sale of some frightening services.

Despite the closure of the Freedom Hosting site, the child pornography community is still active:

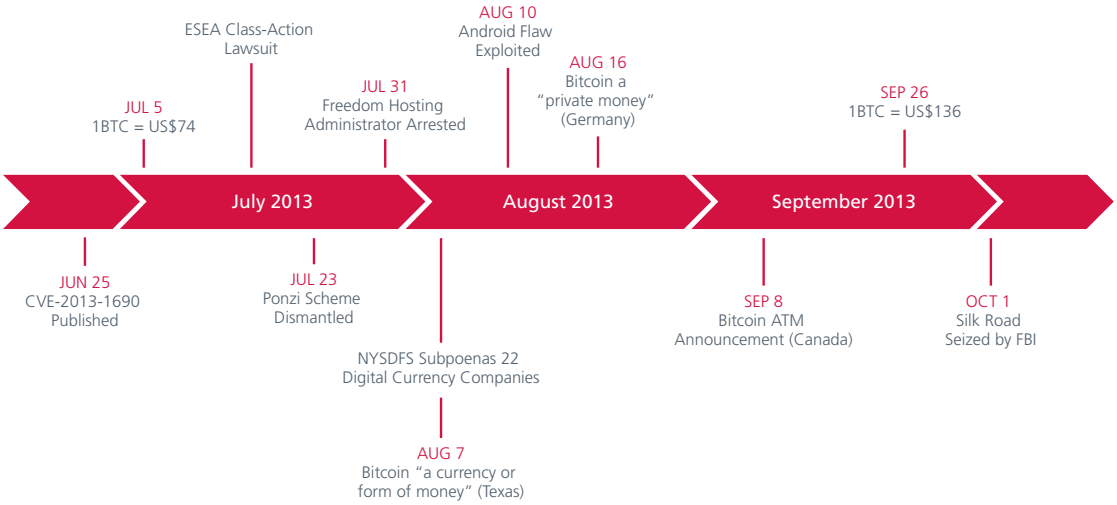
As are opportunities to donate to Al Qaeda:

Malware, vulnerabilities, and hacking



- July 2: McAfee Mobile Security announced it had identified a new Android Trojan, Android/AntiObscan, embedded in a pirated copy of an exclusive app from rapper Jay-Z.[5]
- July 8: McAfee exposed Operation Troy, a long-running case of cyberespionage in South Korea.[6]
- July 17: The Rex Mundi group published stolen customer data from 6,000 customers and prospects of Numericable after the cable TV company refused to pay a ransom of €22,000.[7] On July 8, the same group targeted Websolutions.it.[8]
- July 22: As expected, news of the birth in the British royal family became a powerful lure for malware delivery. McAfee recorded a high number spam messages regarding the event.[9]
- July 26: The passport control system at the departure terminal of the Istanbul Atatürk Airport was hit by a cyberattack. Meanwhile, local media said the passport control system at the Sabiha Gökçen International Airport in Istanbul also broke down.[10]
- July 28: McAfee announced detection for W64/Expiro, a new version of an old malware. This version can infect 32- and 64-bit files.[11]
- July 30: The Syrian Electronic Army hijacked Thomson Reuters' Twitter feed.[12] The group posted seven violent and graphic cartoons. The same day, the group announced it compromised three personal email accounts belonging to staff members at the US White House.[13]
- August 2: McAfee received the malware binary JV/BackDoor-FAZY, a JAR package that opens a back door for an attacker to execute commands and acts as a bot after infection.[14]
- August 7: The British Channel 4 blog was hacked by the Syrian Electronic Army.[15]
- August 7: RSA announced the "Hand of Thief," a Linux financial Trojan including form grabbers and backdoor capabilities.[16] In August, McAfee spotted an increase in the use of AutoIt scripts by malware authors. These malicious scripts primarily concerned Bitcoin miners.[17] In September, further alerts concerned the Andromeda botnet,[18] and the Vertexnet botnet.[19]
- September 6: McAfee announced that the Hesperus, or Hesperbot, banker malware was very active in Turkey and the Czech Republic.[20]
- September 17: Microsoft issued Security Advisory KB2887505 to address an actively exploited remote code execution vulnerability in Internet Explorer (CVE-2013-3893).[21] The exploit code was widely available.
- September 26: The new Trojan OSX/Leverage targeted Apple OS X computers and attempted to install a permanent backdoor. After infection, it connects to its control server on port 7777. The malware exploits the Java vulnerabilities CVE-2013-2465 and CVE-2013-2471.[22]

The Bitcoin saga (continued)



In the last edition of the *McAfee Labs Threats Report*, we published a timeline of news related to online currencies. You'll find further details in our report *Digital Laundry*, summarized on Page 4. Other highlights:

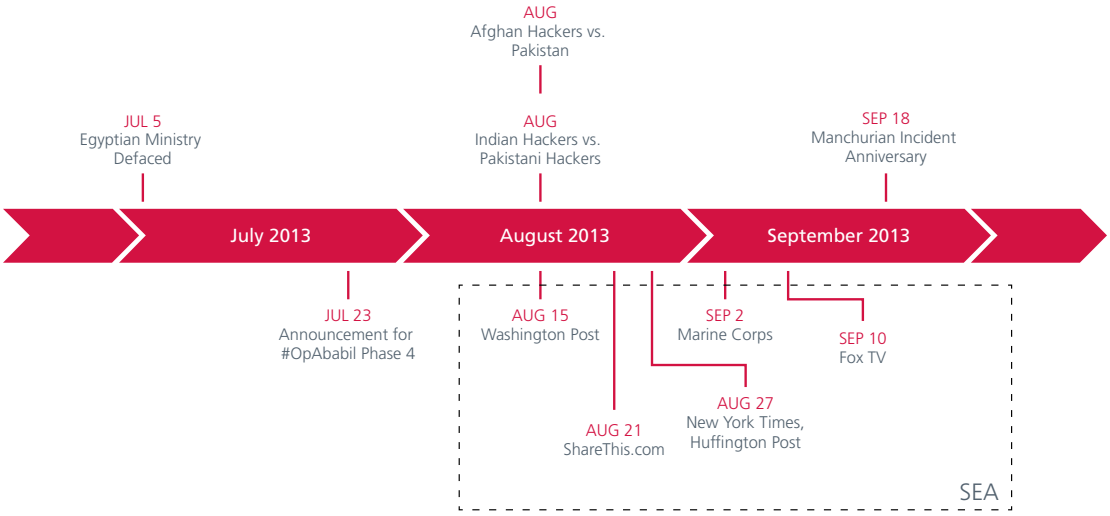
- In April, an employee at the ESEA gaming network used the company's servers to generate Bitcoins for personal use.[23] At the start of July, the company was served with a class action lawsuit following these revelations.[24]
- July 23: The US Securities and Exchange Commission sued a Texas man over claims he operated a Ponzi scheme involving Bitcoin. According to the SEC, starting in September 2011 the suspect raised at least 700,000 Bitcoin through his firm Bitcoin Savings and Trust and improperly used the currency from new investors to cover withdrawals. He falsely promised investors as much as 7 percent interest weekly on purported trades, including selling the online currency to individuals who wished to buy it "off the radar" quickly or in large quantities, the SEC said.[25]
- July 31: An alleged child porn peddler was arrested in Ireland. He was accused of owning and operating Freedom Hosting, the biggest service provider on the anonymous Tor network.[26] The United States has formally sought his extradition. The authorities described him as the "largest facilitator of child porn on the planet." According to the DailyDot website,[27] the suspect two years ago created Onion Bank, operated by Freedom Hosting and offering anonymity for escrow, mixing, and merchant payments. According to some advertising available on a hidden wiki, this bank worked "like PayPal for Bitcoins." During the Blackhat 2013 conference in Las Vegas, an announcement revealed that a Mozilla Firefox zero-day attack specifically targeting the Tor Browser Bundle[28] (CVE-2013-1690/MFSA 2013-53, published June 25) was possibly used by the FBI and National Security Agency to identify the suspect.
- August 7: A federal judge in Texas recognized Bitcoin as "a currency or form of money" and declared that its investment funds and transactions fell under the jurisdiction of US securities law.[29] The New York State Department of Financial Services subpoenaed the major Bitcoin players to learn more about Bitcoin.[30] It asked them to hand over information regarding their money-laundering controls, consumer protection practices, sources of funding, pitch books (for Bitcoin startups), and investment strategies (for Bitcoin investors).
- August 10: Users on the bitcointalk.org forums noticed more than 55 BTC were stolen thanks to a severe vulnerability in the Android implementation of the Java SecureRandom random number generator.[31] Four Android Bitcoin clients—Bitcoin Wallet, Blockchain, Mycelium Bitcoin Wallet, and BitcoinSpinner—were fixed, according to a notice on Bitcoin.org the next day.
- August 16: The German Finance Ministry recognized the digital currency as a "private money" that can be used like cash in multilateral clearing circles.[32]
- September: The press announced the first Bitcoin ATMs would operate in October in Vancouver, Canada. (This is not the first time such an announcement has been made; others have failed to appear.)[33]

Actions against cybercriminals

During the quarter, we noted the following law enforcement efforts:

- July: US federal authorities charged four Russians and a Ukrainian with stealing more than 160 million credit card numbers, which the prosecution says has resulted in hundreds of millions of dollars in losses for major corporations worldwide. The gang is thought to be responsible for the 2007 breach at credit card processor Heartland Payment Systems that exposed some 130 million card numbers, as well as the 2011 breach at Global Payments that involved nearly a million accounts and cost the company almost US$100 million.[34]
- A major player in "high roller" poker tournaments around the world was arrested with eight other people for his company's involvement in an alleged malware ring that netted nearly US$4 million.[35] They allegedly used the malware program Android/Enesoluty to collect information on victims' mobile phones and send invitations to a bogus dating website that charged users but provided no actual services. In total, the malware was claimed to collect more than 37 million email addresses from 810,000 Android phones and tablets.
- September 19–20: London police arrested eight men in connection with a £1.3 million (US$2.1 million) computer-aided robbery from a Barclays Plc branch in the UK's capital. Investigators discovered a KVM switch[36] attached to a 3G router that was connected to one of the branch computers. This was the second time in a week that London police announced arrests over suspected bank hacking. On September 13, the Metropolitan Police detained 12 men due to an attempt to hack into Banco Santander SA computers, using similar equipment.[37]

Hacktivism



In August, an FBI official told *The Huffington Post* that various arrests in 2012 had stopped the expansion of the Anonymous movement.[38] (McAfee Labs foresaw the decline of Anonymous in our *2013 Threats Predictions.)*[39] Indeed, the hacker collective did not conduct any high-profile cyberattacks this quarter, leaving the field open to various "pseudo" cyberarmies and their more obscure objectives.

On July 5, a hacker claiming to be part of Anonymous Jordan defaced eight Egyptian Ministry websites to protest the removal of the Muslim Brotherhood government.[40]

On August 14, Pakistan celebrated its independence day. The day after, the same celebration occurred in India. For hackers, these days were an occasion to express some ill-suited patriotism. In India, several websites, including Mumbai's Mahanagar Telephone Nigam Limited and Pune Traffic Police, were hacked—apparently by Pakistani hackers from the Napsters Crew.[41] Returning the favor, Indian hackers targeted sites in Pakistan. A hacker known as Godzilla breached and defaced the official website of the Pakistan Army. In addition to reaching the website, he also gained unauthorized access to three Pakistani Army Facebook pages.[42] During the same period, a hacker group calling itself the Afghan Cyber Army defaced roughly 300 Pakistani government and business websites with nationalistic messages decrying rocket attacks against Afghan villagers along the Pakistani border.[43]

In previous *McAfee Labs Threats Reports*, we have highlighted activities from two groups: the Iranian Izz ad-Din al-Qassam Cyber Fighters and the Syrian Electronic Army. The first are known for launching a series of attacks against US banks and financial-services companies. They justified the attacks as a response to the "Innocence of Muslims" video they wish to see removed from Internet. The latter support the Syrian regime of President Bashar al-Assad and attack interests and media from countries they consider as enemies.

On July 23, the Cyber Fighters announced the upcoming launch of Phase 4 of Operation Ababil. On August 15, the US banks JPMorgan Chase and Citigroup were victims of distributed denial of service attacks.[44]

Also on August 15, the SEA hacked the *Washington Post* website and redirected some readers to their own site. Furthermore, one Post staff writer's personal account was used to send out an SEA message.[45]

Other attacks followed:

- August 21: The SEA redirected the online content-sharing site ShareThis.com to its official website.[46]
- August 27: Several domains, including those of *The New York Times* and *The Huffington Post*, were redirected after the SEA compromised the companies domain name registrar, Melbourne IT.[47]
- September 2: The SEA defaced the US Marine Corps recruitment website. The SEA, which supports Syria's embattled regime, left a statement denouncing President Obama and urged Marines to disobey any orders to fight in Syria.
- September 10: The official Hootsuite account of Fox TV was hacked and used to post online content to international Fox television networks around the world.[48] The SEA claimed to have accessed to more than 200 linked Facebook and Twitter accounts.

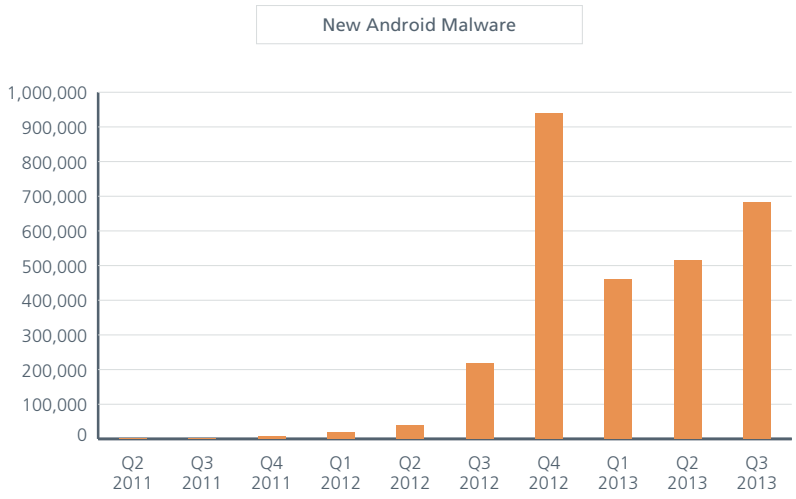
These attacks on government and media giants have caused the FBI, on August 30, to officially place the SEA on an advisory list. The FBI calls the SEA a "proregime hacker group" that emerged during Syrian antigovernment protests in 2011.[49]

Despite these hacking successes, some people wonder about the SEA's skills. On August 31, the French site reflets.info announced a group claiming association with Anonymous compromised the SEA databases and servers.[50] The leaked data, said to be available on the Deep Web, includes hundreds of working usernames and passwords to various Hotmail, Outlook, and Gmail accounts, as well as more than six gigabytes of email messages downloaded from those accounts.[51]

Elsewhere in the world, the Chinese hacktivists of the Honker Union marked the anniversary of the Japanese invasion of Manchuria (September 18, 1931) by launching online attacks against Japanese targets.[52] The day before, a reverse attack took place: Unknown hackers posted pictures critical of the Chinese government on the Shaoxing government website.[53]

Mobile Threats

To speak of malware that infects mobile devices is to speak of Android malware. Threats against other mobile operating systems, including Apple's iOS, are insignificant compared with malicious Android apps. This quarter our count of Android malware grew by one-third, to more than 680,000 samples. That's a steeper increase than between the two previous quarters. Will we soon see numbers that exceed the high-water mark of late 2012?



This quarter we saw one major mobile threat, Exploit/MasterKey.A, that affected many versions of Android. We also observed two-part malware, consisting of a Trojan app that downloads a second-stage malware to a device. Attackers have not forgotten about where the money is and have released a new banking Trojan.

The key to all Androids?

A vulnerability that affects nearly all Android devices has been discovered by computer security researchers. This vulnerability allows an attacker to bypass the signature checking of installed apps. Known as MasterKey, this bug was publicly announced at the Black Hat computer security conference. The researchers had earlier informed Google and provided full details on the vulnerability. Google has produced a patch and has provided it to manufacturers of Android devices.

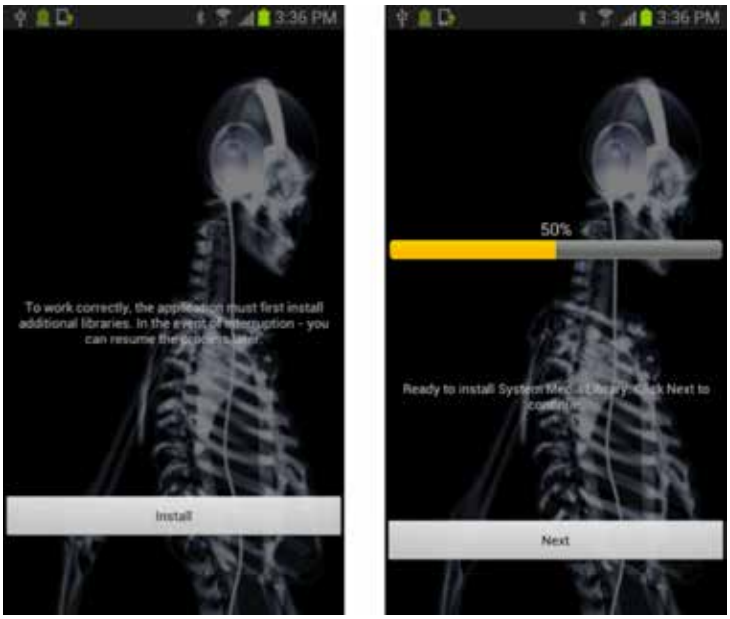
Digital certificates are used to sign Android apps (APKs) and verify that they come from the same developer. When you upgrade an app, Android checks if the upgrade was signed by the original developer. This prevents criminals from creating a bad or malicious upgrade that can take over your phone. Currently an attacker needs to craft a special Android app and have a victim install it. APKs modified this way are detected as Exploit/MasterKey.A.

Google claims that no specially crafted APKs exploiting the MasterKey vulnerability are in the official Play store. Those who acquire apps from third-party stores or websites should make sure to install mobile security software.

Two-part malware

Attackers often attempt to avoid detection by breaking up the functionality of their malware among a number of components. One part will do nothing but access the Internet to download a second or third malicious part. Because the user doesn't download the malicious portion, the malware as a whole can get on a device without raising suspicions.

The Android/Repane family consists of a downloader, Android/RepaneDropper.A, and a malicious portion that sends user information to the attacker. The dropper tries hard to not be noticed by the user, pretending to be an app that lets users x-ray things with their Android devices. Because neither phone nor tablet cameras emit x-rays, there is no technical way for the app to work. That doesn't stop attackers from trying to get the gullible to run it, nor does it stop users from trying to scan their friends or dogs. Unfortunately the only thing that happens is that the phone ends up with a download of Android/Repane.A.



Android/Repane.A is delivered as a novelty x-ray app.

Once Android/Repane.A is downloaded, the victim still needs to install it. That's solved by Android/RepaneDropper.A telling users that they should install a new mandatory system library so they can go back to scanning their friends.

Banking Trojans look for the money

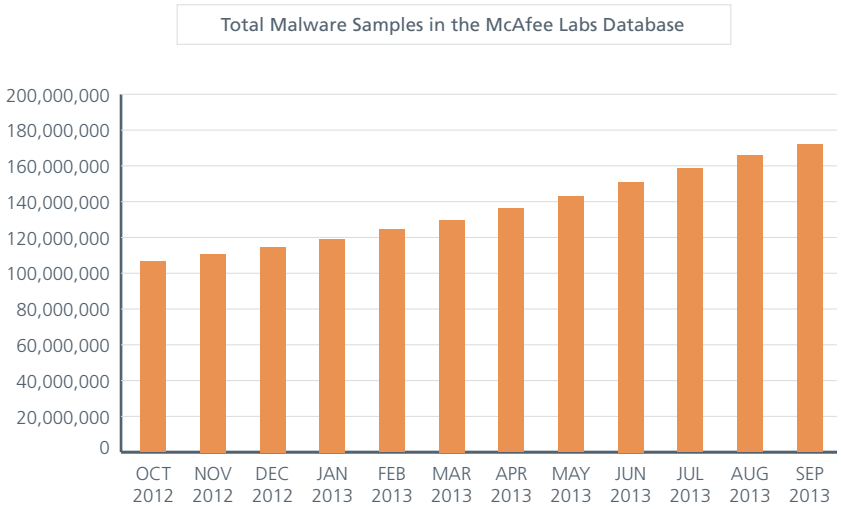
Attackers know that bank accounts tend to hold more money than wallets, so they continue to go after the bigger prize. This quarter Android/Hesperbot attacked users in Turkey and the United Kingdom.

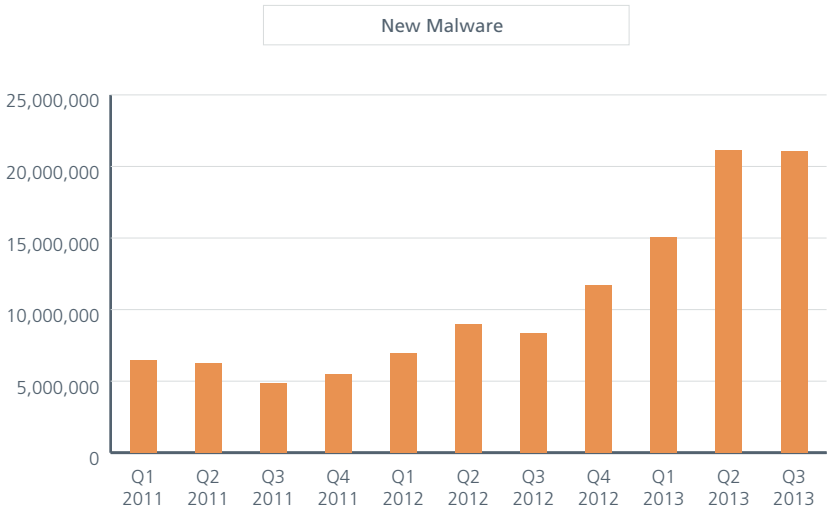
Android/Hesperbot.A also tries to hide from its victims. It deletes its icon so that it won't be noticed. It's still visible in the process list, but under the misleading name Certificate. That's not something a user would typically try to delete; a certificate sounds like something essential.

The malware pretends to be an app that produces authentication codes for online banking, but instead steals the victim's login information. An unsuspecting user will type in the code to get the final authentication code to log into the bank. However, the malware actually sends the user-entered code to the attacker, allowing the bad guys use the code to generate a valid authentication code and access the account.

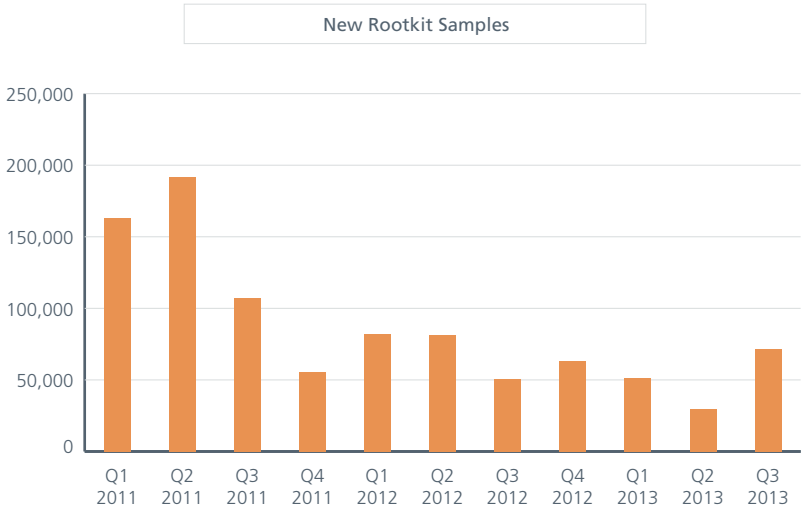
General Malware Threats

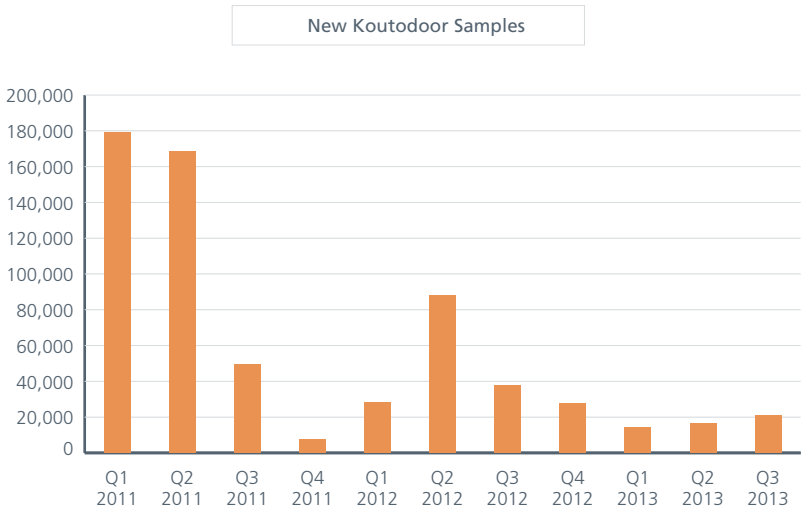
Malware growth declined slightly this quarter, but that's no comfort because this period's 20 million new threats represent the second highest quarter we've recorded. We now have almost 172 million samples in our malware "zoo."

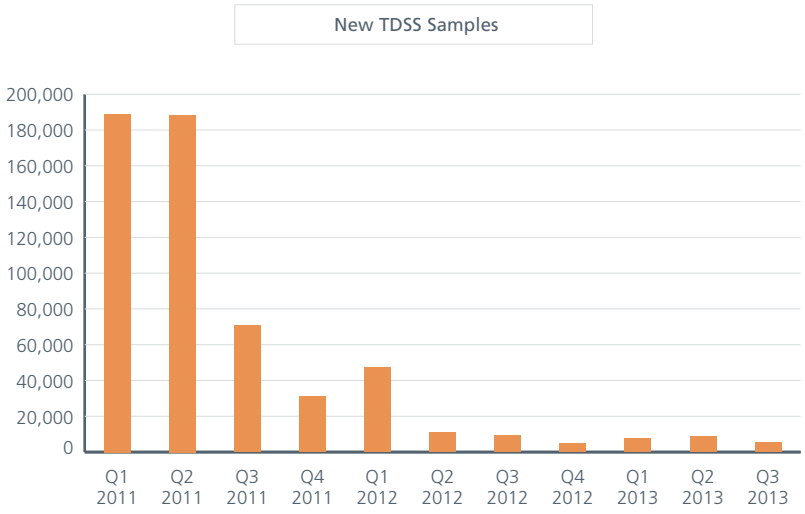


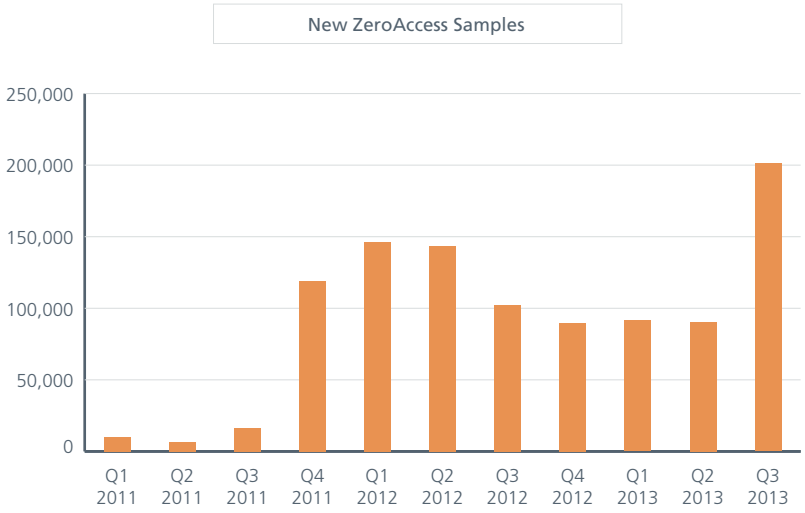


Rootkits, or stealth malware, are designed to evade detection and reside on a system for prolonged periods. Growth in new rootkit samples had been on a downward trend since the middle of 2011, but this quarter rebounded, as we counted more than twice as many new samples as last quarter. (You'll notice the total number of ZeroAccess files exceeds that of all new rootkits. That's because ZeroAccess is a malware family that uses a rootkit, but not all ZeroAccess files are rootkits.)

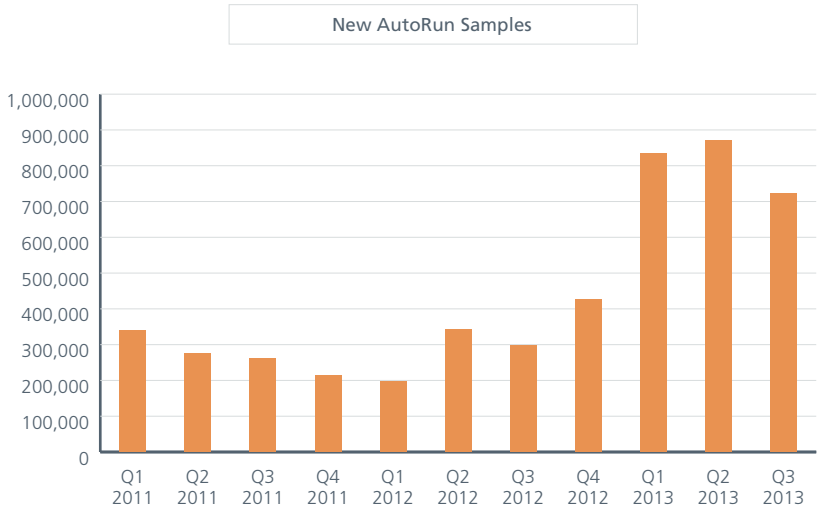


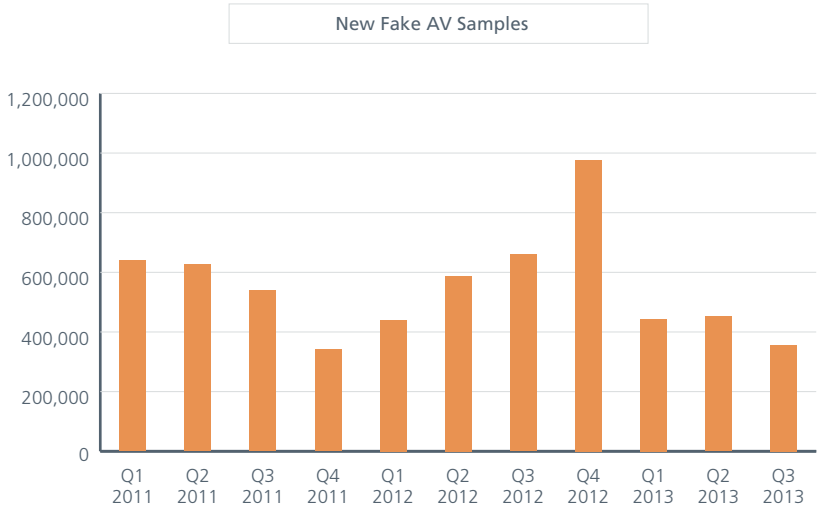


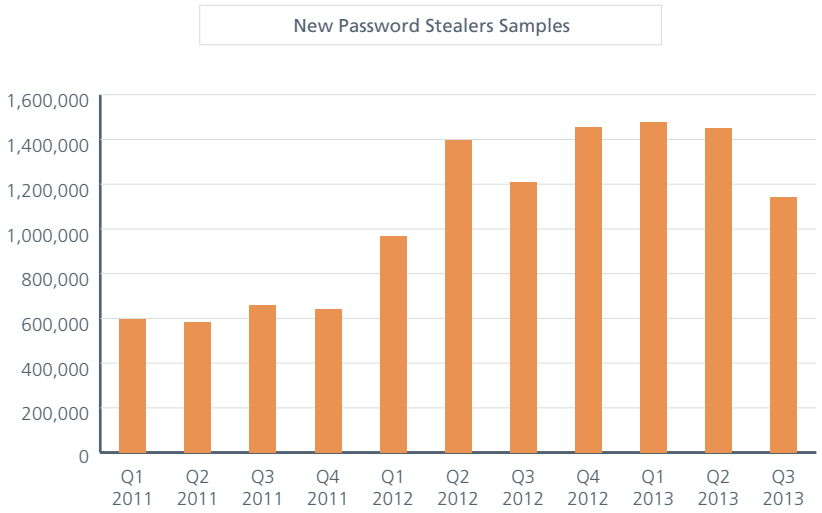




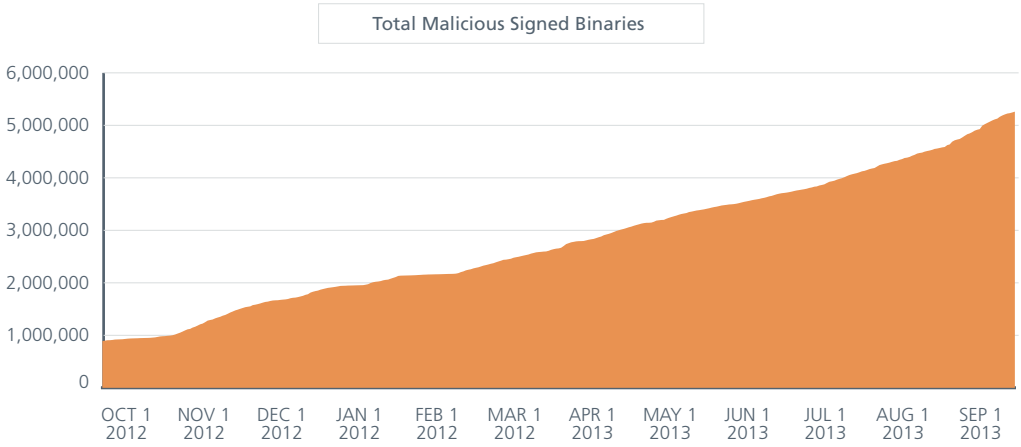
AutoRun malware, which often hides on USB drives and can allow an attacker to take control of a system, doubled at the start of the year and remains high this quarter. The number of fake AV (malware) products—which scare victims into believing their systems are infected—has fallen from a record high of almost a million new samples in 2012 to 356,000 this quarter. Password-stealing Trojans, which attempt to raid victims' bank accounts, fell by more than 20 percent, to fewer than 1.2 million new samples—still a very large number.

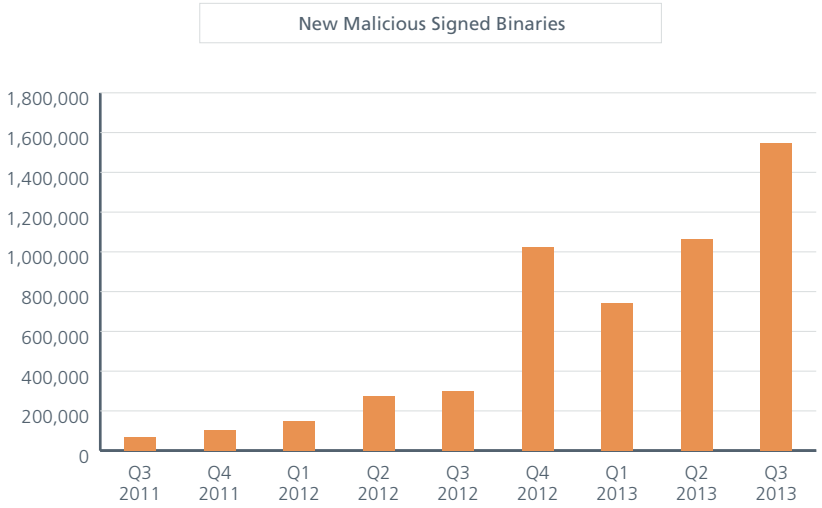

New AutoRun Samples
1,000,000
900,000
800,000
700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013
Q2 2013
Q3 2013


New Fake AV Samples
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013
Q2 2013
Q3 2013

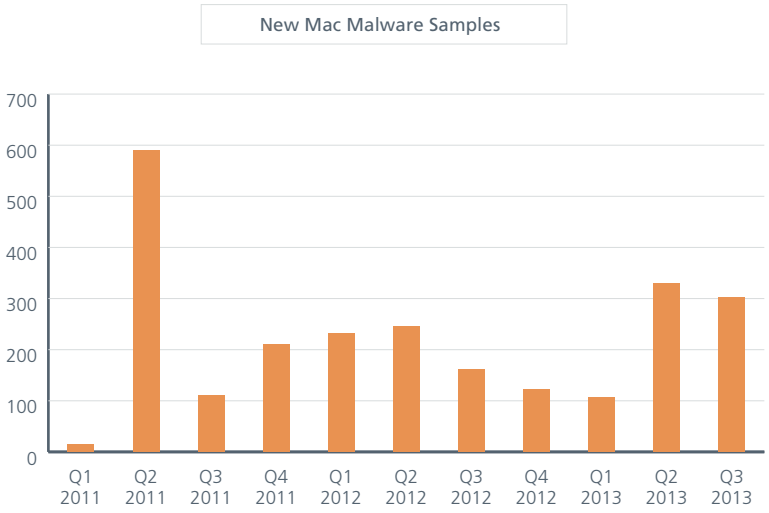

New Password Stealers Samples
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013
Q2 2013
Q3 2013

Signed malware continued its rapid rise, increasing by almost 50 percent this quarter and recording another new high mark, with more than 1.5 million new samples discovered.

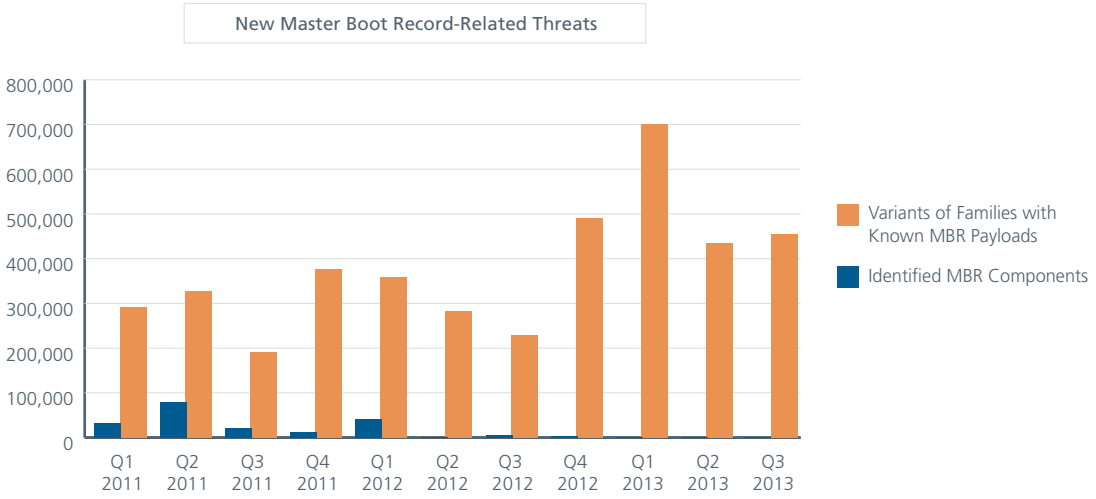




In the second quarter, new malware that attacks the Mac more than tripled, after declining for three quarters. This quarter that figure declined by about 10 percent, to 300 new samples.



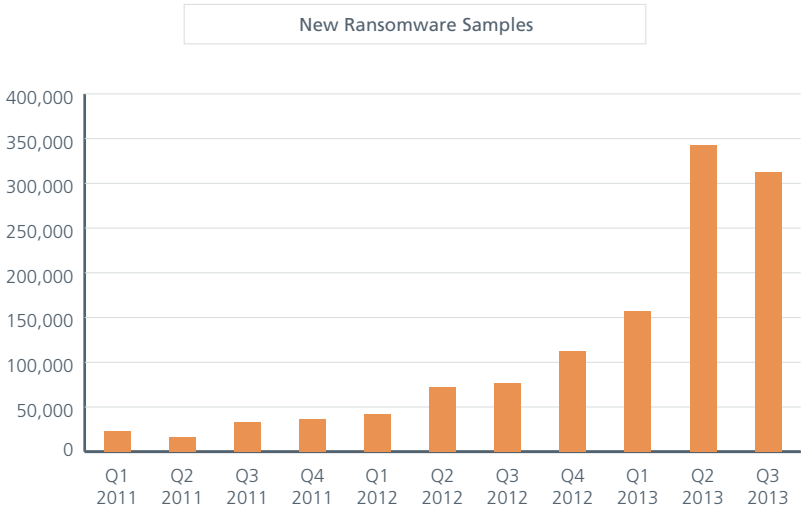
One strain of malware targets a computer's master boot record (MBR)—an area that performs key startup operations. Compromising the MBR offers an attacker a wide variety of control, persistence, and deep penetration. Two quarters ago we saw this threat reach a record level; this quarter's figure shows a slight increase from the last period.



Ransomware

Ransomware has become an increasing problem during the last several quarters, and the situation continues to worsen. The number of new, unique samples this quarter is greater than 312,000, slightly less than last quarter but still the second-highest figure we've recorded.

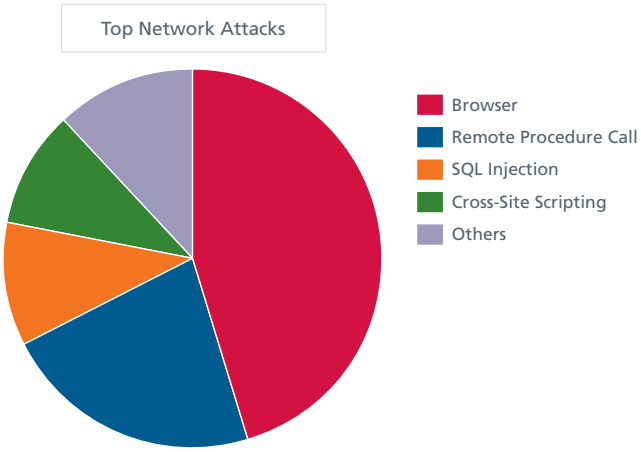
One reason for ransomware's growth is that it is a very efficient means for criminals to earn money because they use various anonymous payment services. This method of cash collection is superior to that used by fake AV products, for example, which must process credit card orders for the fake software. Another reason is that an underground ecosystem is already in place to help with services such as pay-per-install on computers that are infected by other malware, such as Citadel, and easy-to-use crime packs are available in the underground market.



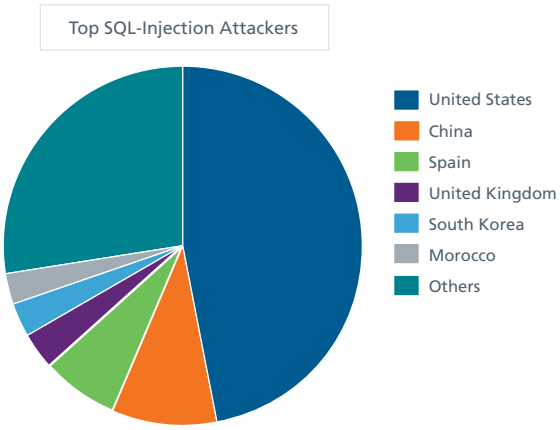
Network Threats

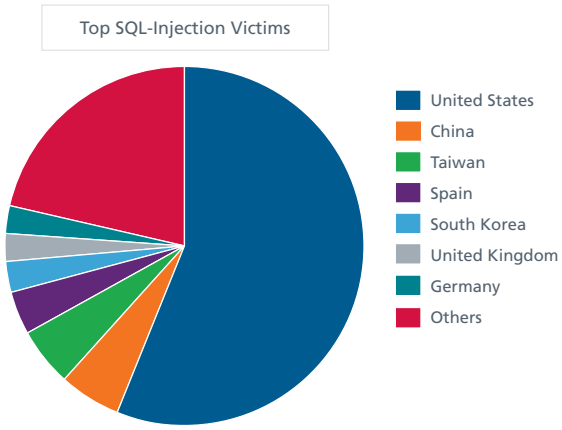
Browser-based threats dropped to 45 percent of all attacks we measured, compared with 73 percent last quarter, according to the McAfee Global Threat Intelligence network. Remote procedure calls doubled, to 22 percent of attacks this quarter. The first pair of the following four very common detection signatures this quarter underline that browser attacks were the most frequently blocked. The latter two are remote procedure call attacks:

- HTTP: Mozilla Firefox Click Event Classification Vulnerability
- RTSP: Apple QuickTime Overly Long Content-Type Buffer Overflow
- DCERPC: Suspicious DCERPC Call
- NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability

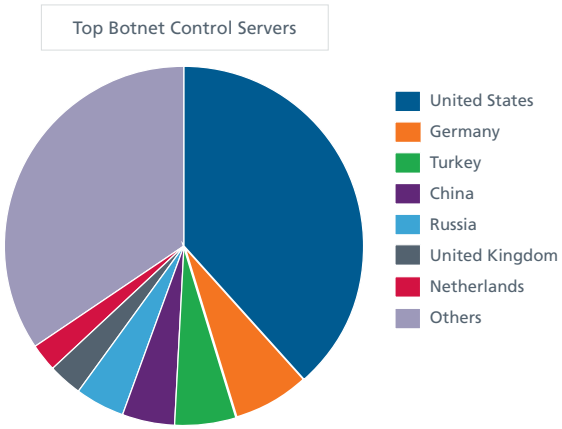


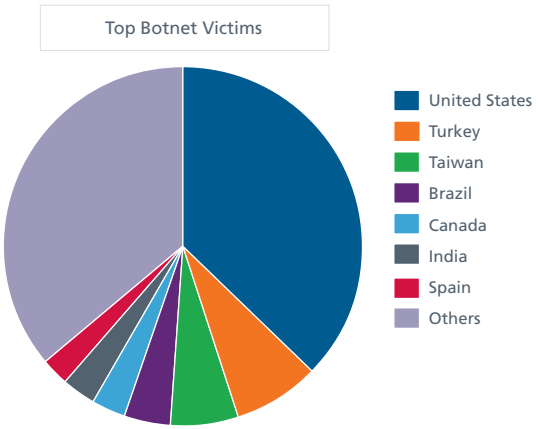
As the host of SQL-injection attacks, which poison legitimate websites, the United States' piece of the pie grew again this quarter, to almost half of all incidents. China moved into second place, hosting 9 percent. Most victims of these attacks (56 percent, down from 60 percent last period) are in the United States.



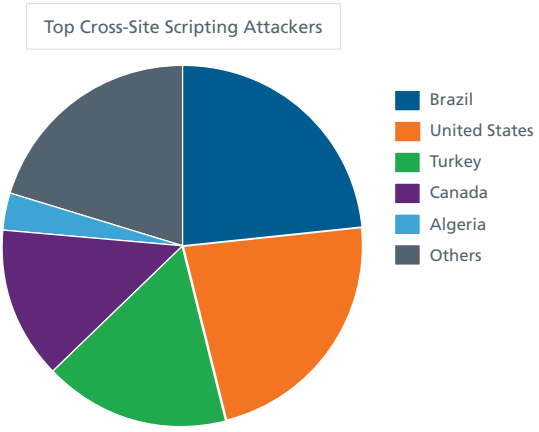


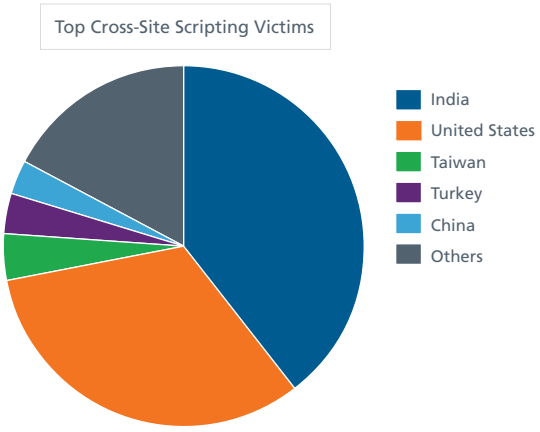
In our botnets tracking, the United States and the rest of the top countries recorded almost identical results as last quarter, both in location of control servers and of victims.





The United States doesn't lead the world in everything: With cross-site scripting threats, Brazil takes first place as the origin of attacks, while India suffers more assaults than any other country.

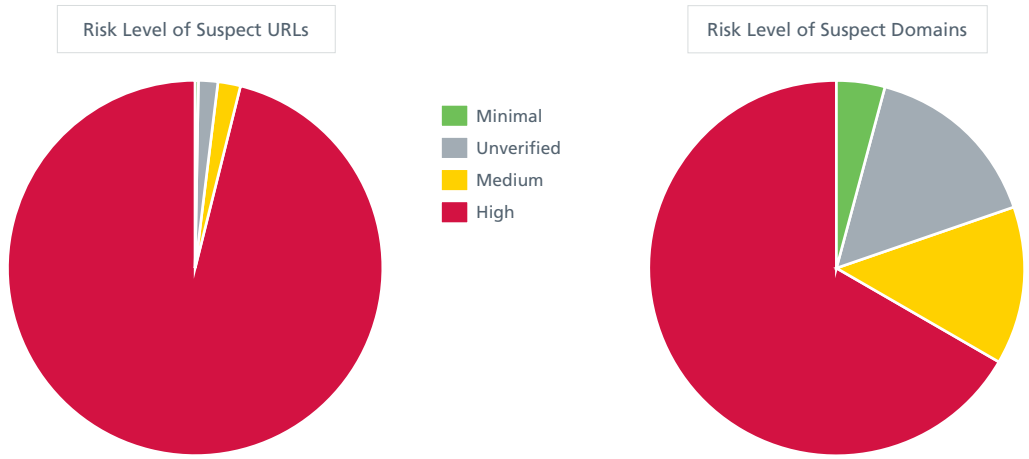




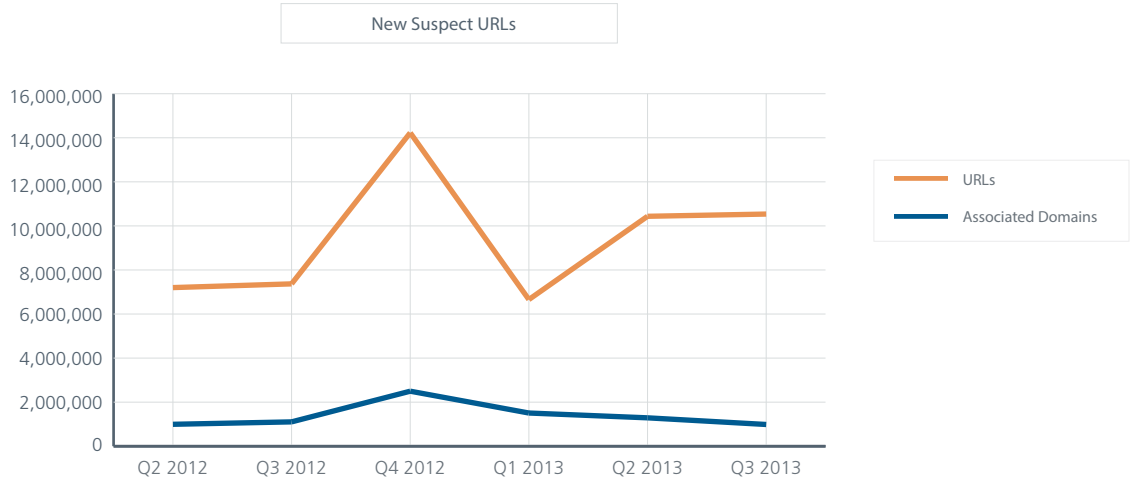
Web Threats

Websites can gain bad or malicious reputations for a variety of reasons. Reputations are determined at specific domains, subdomains, IP addresses, and specific URLs, as well as by many other network and file attributes, to help users understand the risk level of particular web objects. Malicious reputations are influenced by the hosting of malware, potentially unwanted programs, registrations, hosting patterns, and other aspects. Often we observe combinations of questionable code and functionality. These are just a few of the factors that contribute to our rating of a site's reputation.

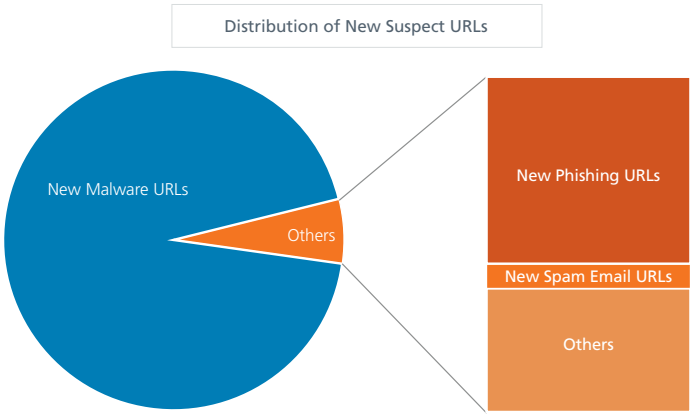
By September's end, the total number of suspect URLs tallied by McAfee Labs surpassed 85 million, which represents a 14 percent increase over the previous quarter. These URLs refer to 30 million domain names, up 3 percent from the previous period.



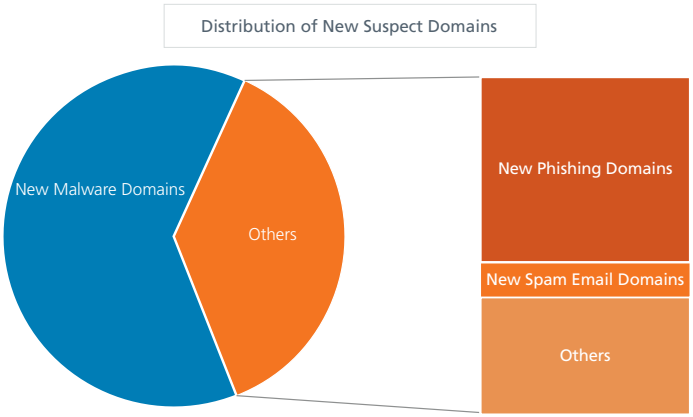
This quarter, we recorded an average of 3.5 million new suspect URLs per month related to about 330,000 domains.



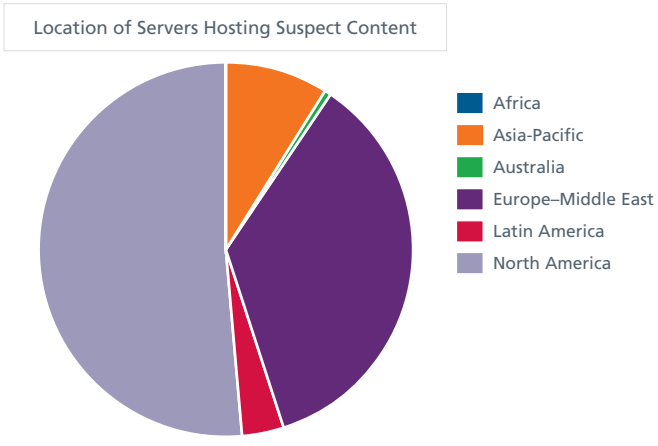
Most of these suspicious URLs (94 percent) host malware, code, or exploits that have been designed specifically to compromise computers. Phishing and spam email represent 3.5 percent and 0.4 percent, respectively.



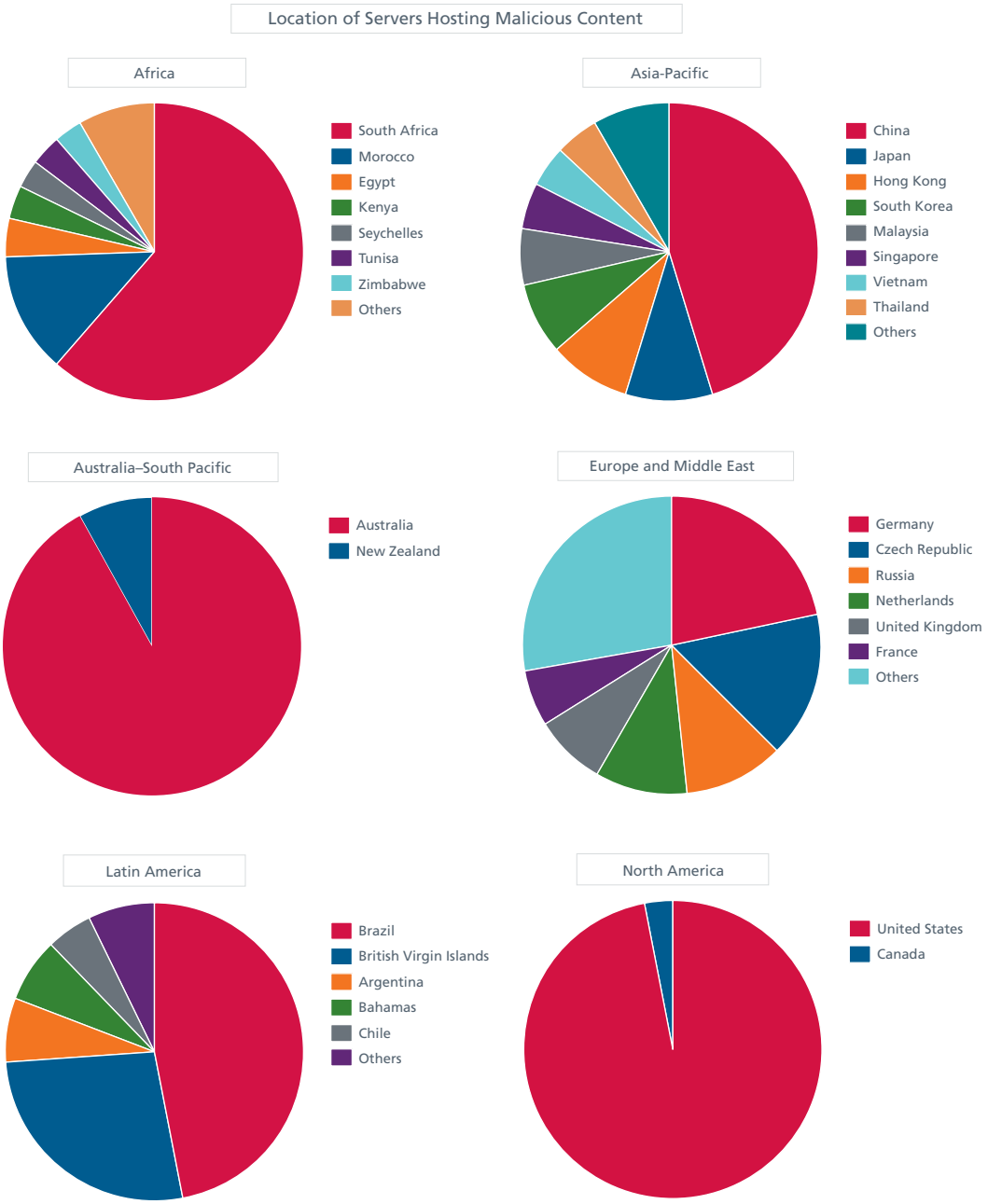
Distribution at the domain level gives us a different outlook, with 20 percent phishing domains and 4 percent spam email domains.



The domains associated with newly suspect URLs are mainly located in North America (chiefly the United States) and Europe and the Middle East (chiefly Germany). This trend is not new; North America historically hosts quite a bit of malware and suspect content. However, its scope has decreased to 51 percent this quarter compared with 74 percent in the first quarter of 2013.

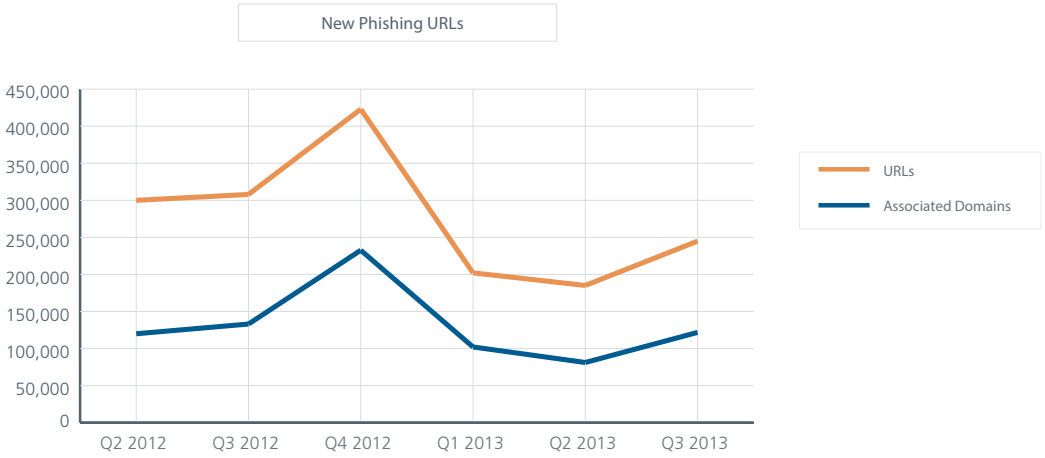


Digging into the location of servers hosting malicious content in other countries we see quite a global diversity. Apart from Europe, each region has one or two clearly dominant players:

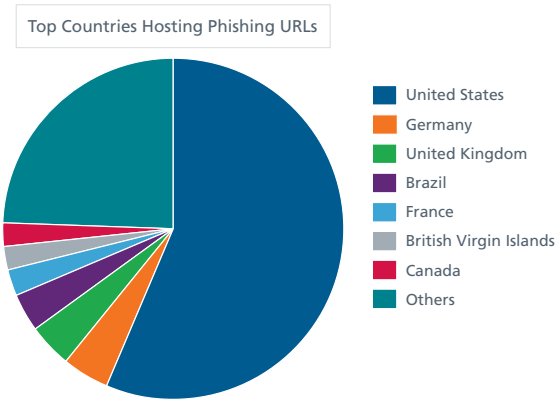


Phishing

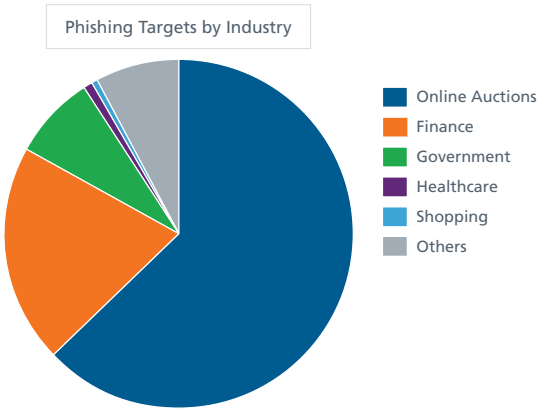
After peaking during the last quarter 2012, the number of new phishing URLs dropped considerably in the first half of 2013. We observed another increase this quarter.



Most of these URLs are hosted in the United States.

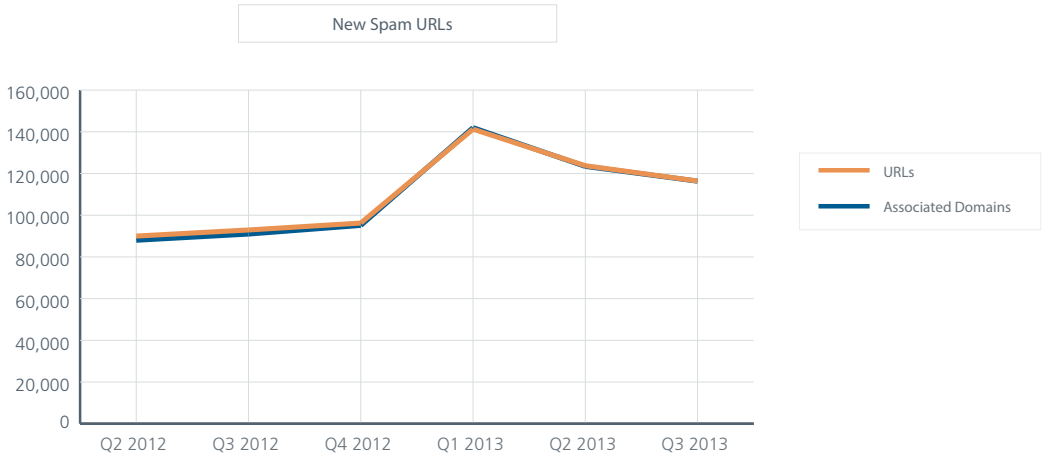


Phishers go after several key industries. The top three are online auctions, finance, and government.

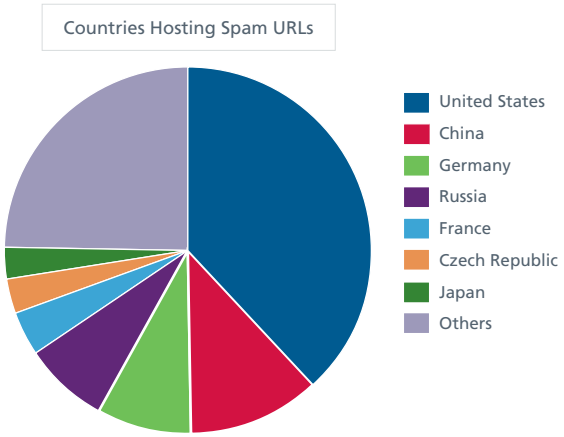


Spam URLs

Spam URLs are those that arrive in unsolicited spam emails. Also included in this family are sites built only for spamming purposes, such as spam blogs or comment spam.

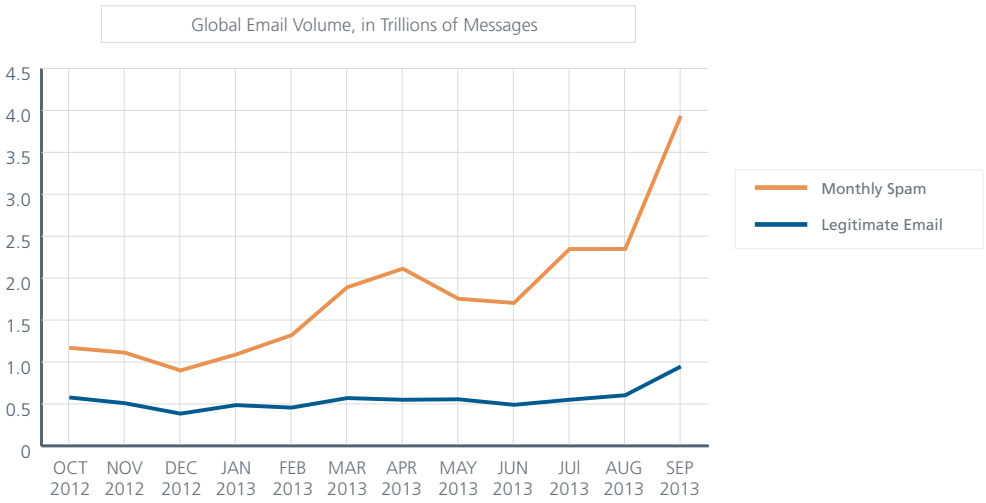


The main countries hosting these URLs are the United States, China, Germany, and Russia.



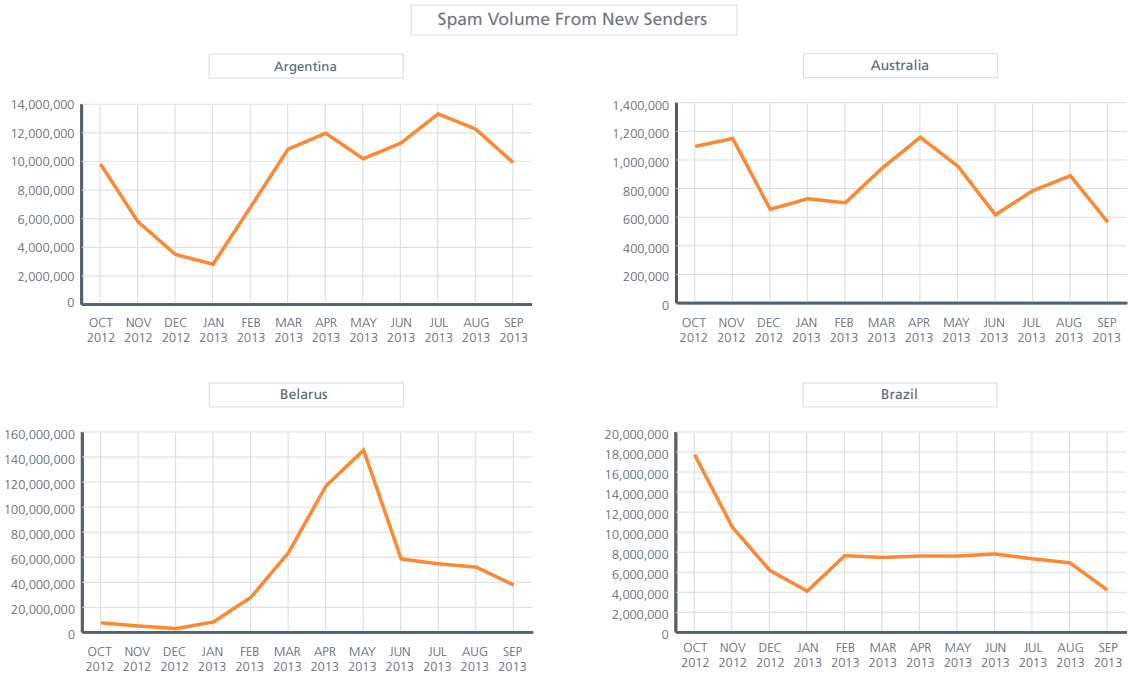
Messaging Threats

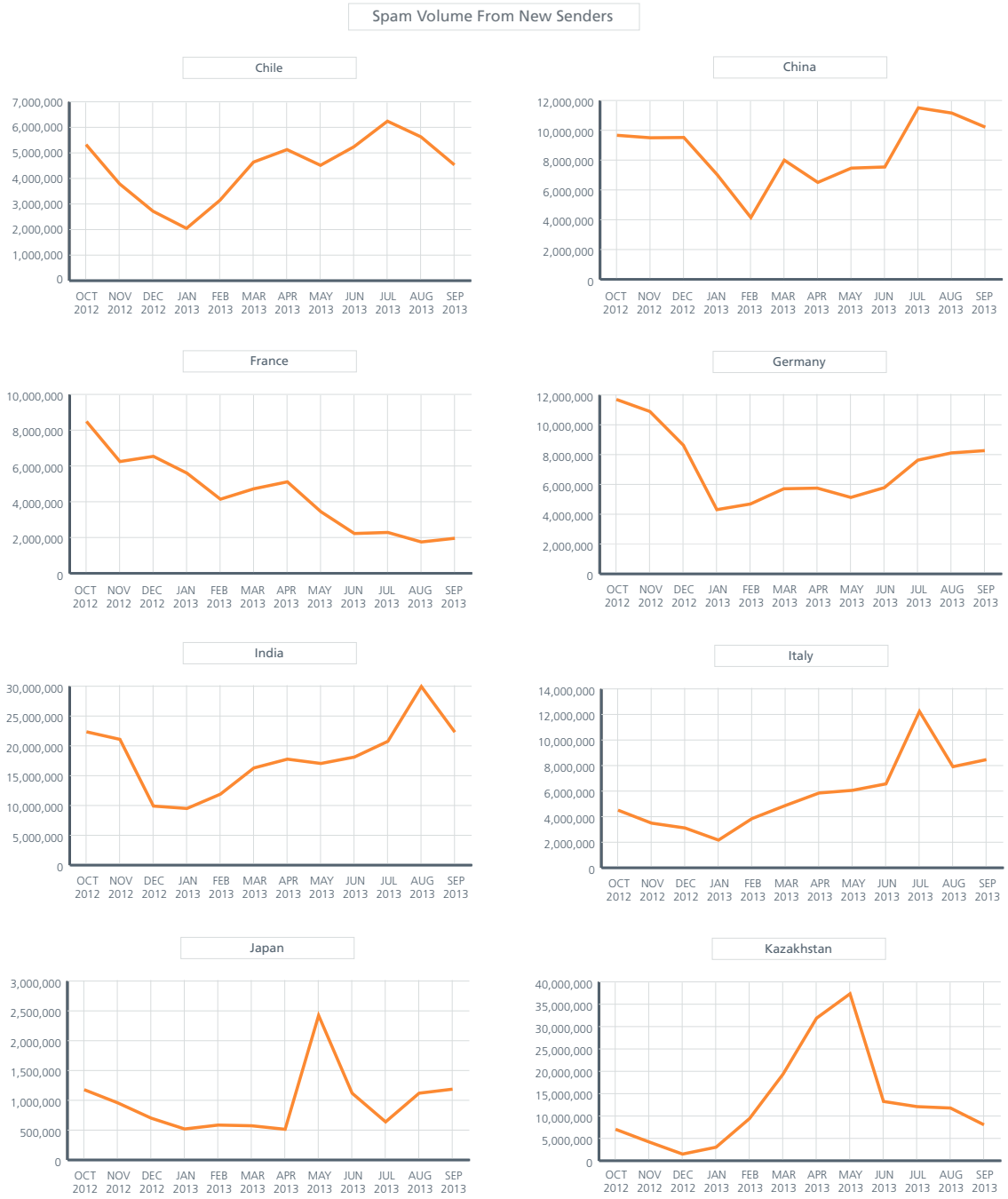
After a slight decline in May and June the volume of worldwide spam has more than doubled this quarter. Spam volume hasn't been this high since August 2010.



Spam volume

Looking closely at new spam senders in various countries, our statistics show marked differences from quarter to quarter. China and Italy had an increase of greater than 50 percent this period. Meanwhile, Kazakhstan (down 61 percent), Belarus (down 55 percent), and Ukraine (down 51 percent) enjoyed large declines.



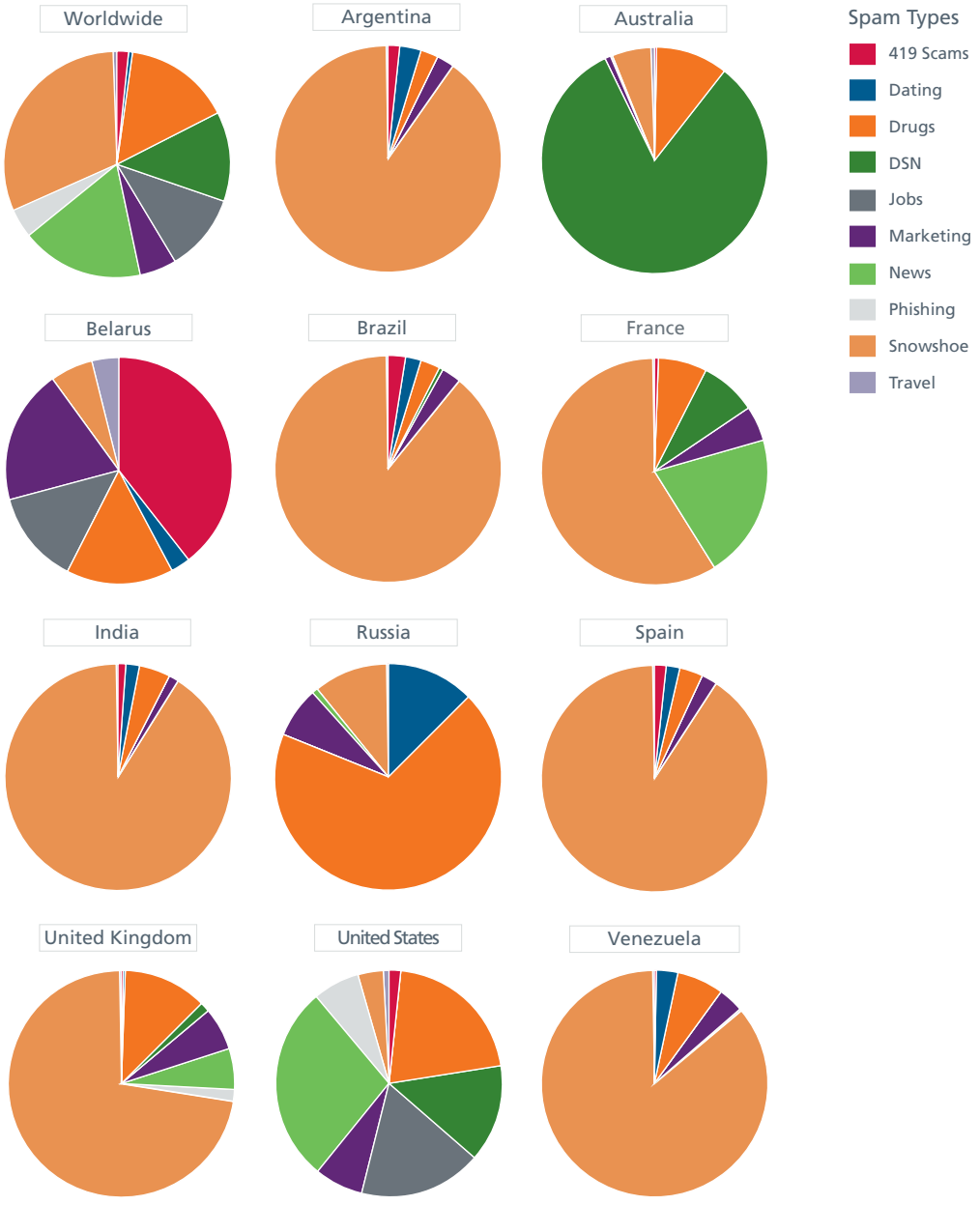

Spam Volume From New Senders
Chile
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
China
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
France
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
Germany
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
India
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
Italy
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
Japan
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
Kazakhstan
40,000,000
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
OCT 2012
NOV 2012
DEC 2012
JAN 2013
FEB 2013
MAR 2013
APR 2013
MAY 2013
JUN 2013
JUL 2013
AUG 2013
SEP 2013


Spam Volume From New Senders
Peru
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
OCT 2012 NOV 2012 DEC 2012 JAN 2013 FEB 2013 MAR 2013 APR 2013 MAY 2013 JUN 2013 JUL 2013 AUG 2013 SEP 2013
Romania
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
OCT 2012 NOV 2012 DEC 2012 JAN 2013 FEB 2013 MAR 2013 APR 2013 MAY 2013 JUN 2013 JUL 2013 AUG 2013 SEP 2013
Russia
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
OCT 2012 NOV 2012 DEC 2012 JAN 2013 FEB 2013 MAR 2013 APR 2013 MAY 2013 JUN 2013 JUL 2013 AUG 2013 SEP 2013
South Korea
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
OCT 2012 NOV 2012 DEC 2012 JAN 2013 FEB 2013 MAR 2013 APR 2013 MAY 2013 JUN 2013 JUL 2013 AUG 2013 SEP 2013
Spain
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
OCT 2012 NOV 2012 DEC 2012 JAN 2013 FEB 2013 MAR 2013 APR 2013 MAY 2013 JUN 2013 JUL 2013 AUG 2013 SEP 2013
Ukraine
40,000,000
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
OCT 2012 NOV 2012 DEC 2012 JAN 2013 FEB 2013 MAR 2013 APR 2013 MAY 2013 JUN 2013 JUL 2013 AUG 2013 SEP 2013
United Kingdom
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
OCT 2012 NOV 2012 DEC 2012 JAN 2013 FEB 2013 MAR 2013 APR 2013 MAY 2013 JUN 2013 JUL 2013 AUG 2013 SEP 2013
United States
180,000,000
160,000,000
140,000,000
120,000,000
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
OCT 2012 NOV 2012 DEC 2012 JAN 2013 FEB 2013 MAR 2013 APR 2013 MAY 2013 JUN 2013 JUL 2013 AUG 2013 SEP 2013

Spam travels the world via snowshoes

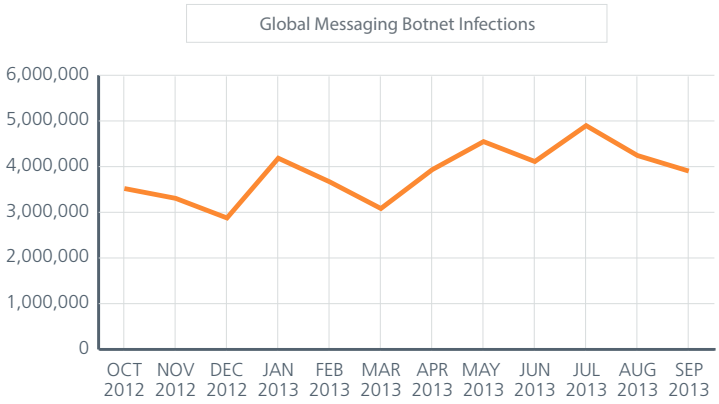
The most popular type of spam this quarter was "snowshoe" spam, so named because it spreads the load across many IP addresses to avoid rapid eviction by ISPs. Most of the countries we track saw a predominance of snowshoe spam—often representing 85 percent to 95 percent of the high-volume subject types. We see this as a sign of a country's excess hosting capacity being put to use: This type of spam generally involves renting servers in hosting facilities and sending spam until the hosting facility evicts the spammer or gets blacklisted.

In Belarus "419" scams are most popular. These are appeals to send money to some unfortunate, usually a "wealthy" African, who will later richly reward anyone who helps. You can guess what happens after you send money. In Australia and the United States, delivery service notifications (DSNs) are common. Drugs and online bride spam are big in Russia. In the United States spammers employ a balanced attack, with bogus news and jobs as well as drugs as leading lures. Our "worldwide" pie represents only the countries shown on this page, not the entire globe.

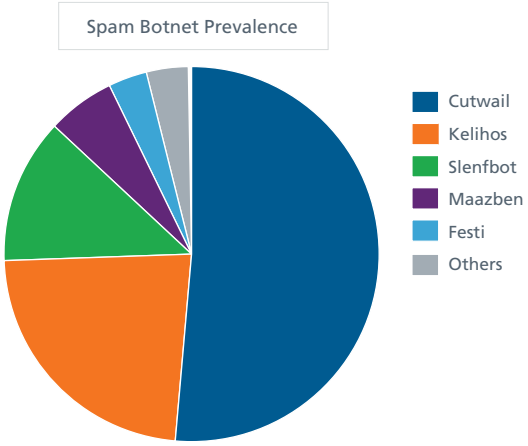


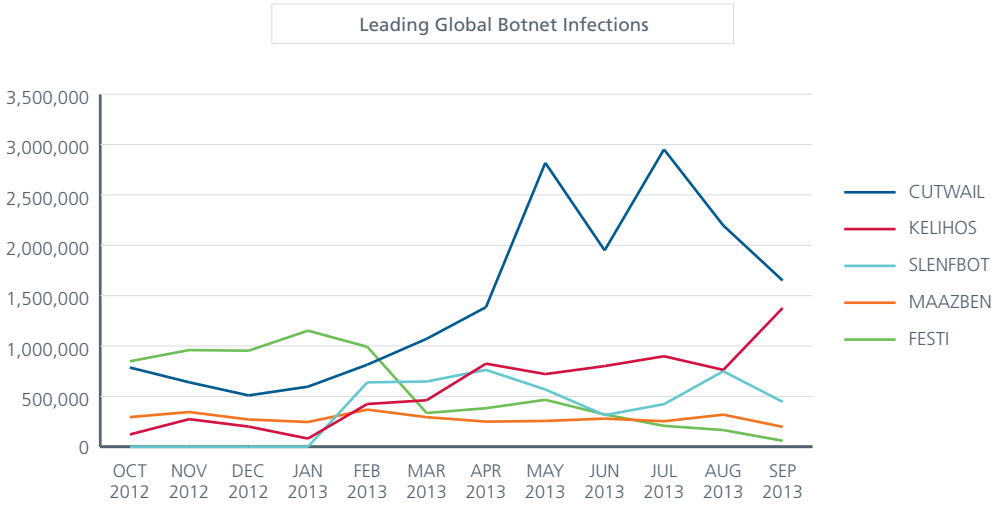
Botnet breakdowns

Infections from messaging botnets have showed an overall decline since May 2012. Quarter after quarter, however, we saw some ups and downs with a small general upward trend.



Cutwail remains in first place among botnets, while Kelihos, which was first seen at the end of 2012, is again number two. Slenfbot, which started in the first quarter of 2013, continues in third place.





Messaging botnet prevalence

Our breakdown of botnets shows how the five most widespread botnet families are represented in various countries around the globe. Cutwail is the global leader; Kelihos came close to the top spot in September.

About the Authors

This report was prepared and written by Benjamin Cruz, Paula Greve, François Paget, Craig Schmugar, Jimmy Shah, Dan Sommer, Bing Sun, Adam Wosotowsky, and Chong Xu 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 500 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. http://www.mcafee.com/us/threat-center.aspx

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com.

[1] http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf
[2] http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf
[3] http://info.tapjoy.com/wp-content/uploads/sites/4/2013/05/RedefiningVirtualCurrency_WhitePaper-1MAY2013-v1.pdf
[4] http://krebsonsecurity.com/2013/10/feds-take-down-online-fraud-bazaar-silk-road-arrest-alleged-mastermind/
[5] http://blogs.mcafee.com/consumer/android-malware-set-for-july-4-carries-political-message
[6] http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf
[7] http://www.infosecurity-magazine.com/view/33544/rex-mundi-hackers-post-data-stolen-from-numericable/
[8] http://news.softpedia.com/news/Rex-Mundi-Hackers-Blackmail-Italian-Hosting-Service-Websolutions-it-366685.shtml
[9] http://blogs.mcafee.com/mcafee-labs/the-dangers-of-a-royal-baby-scams-abound
[10] http://news.xinhuanet.com/english/world/2013-07/26/c_132577334.htm
[11] http://www.welivesecurity.com/2013/07/30/versatile-and-infectious-win64expiro-is-a-cross-platform-file-infector
[12] http://www.buzzfeed.com/michaelrusch/thompson-reuters-twitter-account-apparently-hacked
[13] http://www.dailydot.com/news/sea-syrian-electronic-army-white-house-staffers/
[14] http://blogs.mcafee.com/mcafee-labs/java-back-door-acts-as-bot
[15] http://www.ehackingnews.com/2013/08/exclusive-british-channel-4-blog-hacked.html
[16] https://blogs.rsa.com/thieves-reaching-for-linux-hand-of-thief-trojan-targets-linux-inth3wild
[17] http://blogs.mcafee.com/mcafee-labs/bitcoin-miners-use-autoit-complied-programs-with-antianalysis-code
[18] http://blogs.mcafee.com/mcafee-labs/andromeda-botnet-hides-behind-autoit
[19] http://blogs.mcafee.com/mcafee-labs/vertexnet-botnet-hides-behind-autoit
[20] http://blogs.mcafee.com/mcafee-labs/hesperus-evening-star-shines-as-latest-banker-trojan
[21] http://blogs.technet.com/b/srd/archive/2013/09/17/cve-2013-3893-fix-it-workaround-available.aspx
[22] McAfee MTIS13-154.pdf: https://community.mcafee.com/docs/DOC-5302
[23] http://www.escapistmagazine.com/news/view/123676-Rogue-Bitcoin-Code-Found-in-Competitive-Counter-Strike-Servers
[24] http://www.wired.com/wiredenterprise/2013/07/esea-2/
[25] http://www.theguardian.com/technology/2013/jul/24/bitcoin-alleged-ponzi-fraud
[26] http://www.irishmirror.ie/news/irish-news/extradition-case-child-porn-accused-2170785
[27] http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/
[28] https://community.rapid7.com/community/metasploit/blog/2013/08/07/heres-that-fbi-firefox-exploit-for-you-cve-2013-1690
[29] http://ia600904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf
[30] http://www.forbes.com/sites/kashmirhill/2013/08/12/every-important-person-in-bitcoin-just-got-subpoenaed-by-new-yorks-financial-regulator/
[31] http://thegenesisblock.com/security-vulnerability-in-all-android-bitcoin-wallets/
[32] http://www.welt.de/finanzen/geldanlage/article119086297/Deutschland-erkennt-Bitcoin-als-privates-Geld-an.html
[33] http://rt.com/business/bitcoin-atm-canada-vancouver-717/
[34] http://krebsonsecurity.com/2013/07/hacker-ring-stole-160-million-credit-cards/
[35] http://www.pokernewsdaily.com/poker-professional-masaaki-kagawa-arrested-for-malware-ring-24285/
[36] A KVM (keyboard, video, and mouse) switch is a hardware device that can allow users to remotely operate their work computer systems.
[37] http://www.dailymail.co.uk/news/article-2426519/Gang-arrested-1-3million-Barclays-hijack-plot-carbon-copy-Santander-scam.html
[38] http://www.huffingtonpost.com/2013/08/21/anonymous-arrests-fbi_n_3780980.html
[39] http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf
[40] http://hackread.com/egyptian-ministry-sites-hacked-anonymous-jordan/
[41] http://post.jagran.com/pakistan-launches-cyber-war-against-india-hacks-72-websites-1376474598
[42] http://news.softpedia.com/news/Indian-Hacker-Breaches-Pakistan-Army-s-Website-and-Facebook-Pages-374298.shtml
[43] http://www.stripes.com/news/hackistan-afghan-cyber-guerrillas-step-up-attacks-on-pakistani-websites-1.234947
[44] http://www.foxbusiness.com/industries/2013/08/15/chase-website-suffers-intermittent-outage/
[45] http://www.washingtonpost.com/blogs/ask-the-post/wp/2013/08/15/editors-note
[46] http://hackread.com/syrian-electronic-army-hacks-sharethis-godaddy-acc-and-redirects/
[47] http://qz.com/119245/how-the-syrian-electronic-army-hacked-the-new-york-times-twitter-and-the-huffington-post/
[48] http://hackread.com/sea-hacks-fox-tv-hootsuite-social-media-account/
[49] http://info.publicintelligence.net/FBI-SEA.pdf
[50] (Explicit content) http://reflets.info/opsyria-syrian-electronic-army-was-hacked-and-d0xed-warning-explicit-content/
[51] http://krebsonsecurity.com/2013/08/syrian-electronic-army-denies-new-data-leaks/
[52] http://www.theregister.co.uk/2013/09/18/honker_union_270_japan_targets_manchurian_incident/
[53] http://beijingcream.com/2013/09/hackers-post-anti-ccp-mooncakes-to-shaoxing-website/

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

60633rpt_qtr-q3_1113_fnl_ETMG