Report

McAfee Threats Report: First Quarter 2013

By McAfee® Labs

Table of Contents

Introduction

McAfee Labs researchers have analyzed the threats of the first quarter of 2013 and recognized several familiar trends: steady growth in mobile malware and a rapid increase in general malware, including AutoRun malware and stealth malware that attacks the master boot record (MBR). Worldwide spam doubled during the quarter—as it makes a comeback after more than a year of decline.

Narrowly targeted attacks focused on the financial sector, but one came with a twist. Our analysis of the Citadel Trojan shows that cybercriminals have found a way to turn this traditional bank-account threat into the broader theft of personal information from narrowly targeted victims in certain countries. Will the attackers use this data in the future?

Our count of mobile malware samples, just about exclusively for the Android OS, continues to skyrocket. Almost 30 percent of all mobile malware appeared this quarter. Malicious spyware and targeted attacks highlighted the latest assaults on mobile phones.

All malware that we track—affecting clients, servers, networks, mobiles—now stands at more than 128 million samples. That figure has climbed steadily for ages and quite rapidly during the last two quarters. AutoRun, ransomware, and MBR threats were the leaders this period. With ransomware, cybercriminals hold a system hostage and insist on payment to unlock a computer. But will they free the machine after the victim pays? There are no guarantees, and anonymous payment systems make it basically impossible to track their movements. MBR threats can remain on a system for a long time without the victim's knowledge and download other forms of malware.

The McAfee Global Threat Intelligence™ network tells us that IP addresses in the United States are again both the source and the target of most malicious network activity. Browser-based attacks, such as hidden iframes and malicious Java code, are the most common type.

Our analysis of web threats found that the number of new suspicious URLs, mostly in the United States, increased by 12 percent this quarter. New phishing attacks aimed primarily at online auctions and financial targets. One of the biggest stories this quarter is the increase in spam after more than a year of decline. We counted 1.9 trillion messages in March. That's lower than record levels but about twice the volume of December 2012.

Cybercriminals continue to develop and market crimeware tools, which make it easy for inexperienced scammers to join the ranks and exploit victims. The European Union's new European Cybercrime Centre was instrumental in aiding law enforcement to arrest and prosecute online criminals. Hacktivists raised the possibility of using denial-of-service attacks as lawful means to support their ends. We also examine the efforts of cyberarmies during the quarter. These groups usually arise in countries that limit personal liberties and claim to act on behalf of their governments.

The Citadel Trojan

Zeus "banking" malware and its variants have made headlines in recent months. One variant, the Citadel Trojan, took the spotlight in late 2012 with the news of its withdrawal from the open crimeware market. However, this withdrawal does not necessarily mean that Citadel will cease to be a significant global threat. The McAfee Labs report *Inside the World of the Citadel Trojan* has determined that Citadel's original developers and perhaps others are developing new variants that significantly extend Citadel's functionality and threat profile.[1] The primary trends observed in the second half of 2012 and this quarter include:

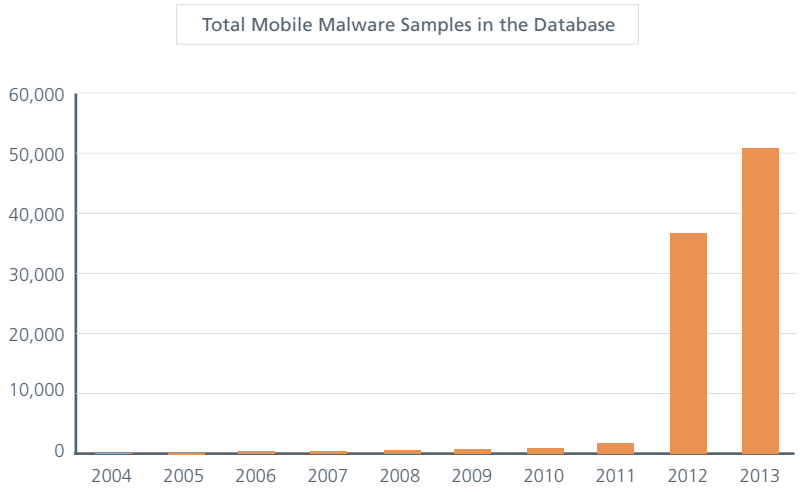
- Targeted attacks on public and private enterprises, primarily in Europe
- Functional enhancements used to steal information as well as currency
- Narrowing of targets to a few hundred as compared with tens of thousands of targets observed in previous uses of the Zeus malware family
- Harvesting credentials from internal applications, banking system applications, manufacturing systems, etc. that could be used in a later attack against those applications
- Emergence of the "Poetry Group" as the primary perpetrator of Citadel-based attacks

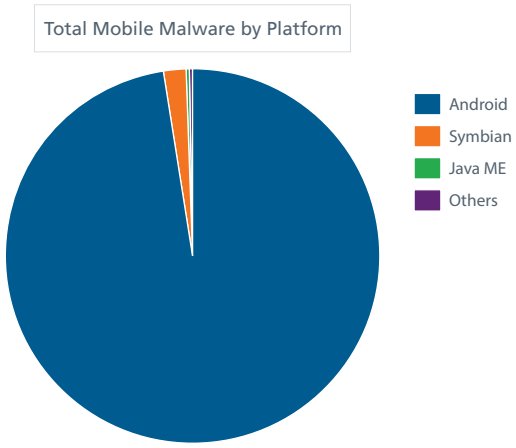
Citadel is considered an emerging threat to not only the financial services industry, but to other industries as well. Citadel gives cybercriminals advanced remote connectivity, and it also gives them the ability to dynamically decide which target to engage. While Citadel is being withdrawn from the open market, McAfee Labs believes that we will continue to see successor variants deployed throughout 2013. We also expect that its targets will expand as more cybercriminals realize that the potential capabilities of Citadel go well beyond financial fraud. There is a significant amount of recent activity to suggest that perpetrators will continue to use Citadel to attack businesses and government organizations around the world.

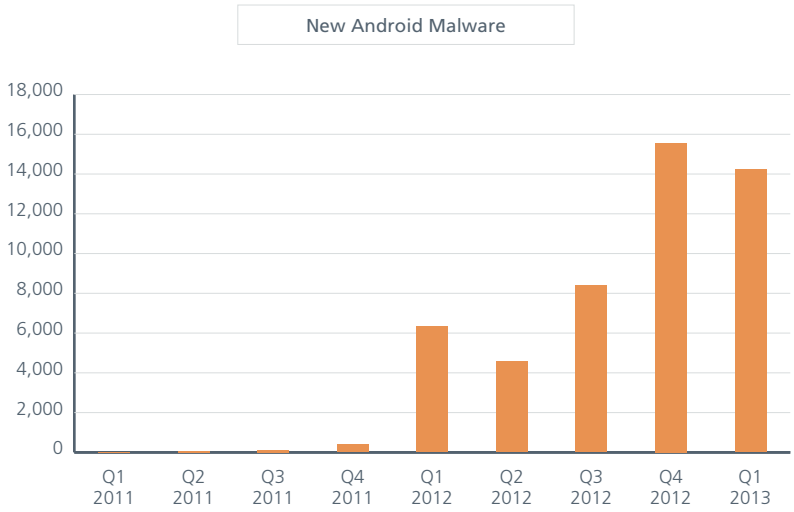
Mobile Threats

At the end of this quarter, the total number of samples in our mobile malware "zoo" reached 50,926, with 28 percent of that arriving in 2013. In all of 2011 we gathered only 792 samples. The growth of mobile malware declined slightly this quarter, but we're still on course for another eye-catching—and record—year.

Some researchers cite higher figures of new mobile malware, with predictions of up to one million binaries. But these numbers may include all files bundled in malicious Android apps and families that repackage APK files. At McAfee Labs, we count only unique malware families and variants and not, for example, common ad libraries and other redundant malicious files.







Although the threats of commercial spyware and adware are declining, we see that malicious spyware and targeted attacks are becoming more prominent. Malicious spyware combined with botnets are among the latest threats.

Android/Ssucl.A is a Trojan that pretends to be a system cleanup utility. In reality it's a botnet client that takes orders from a remote control server. Not only does this Trojan steal user and SMS information, but an attacker can use it to launch phishing attacks for Dropbox and Google logins. The malware does not stop there: Ssucl.A will also attempt to download and infect a PC using an autorun.inf attack.

Tibetan and Uyghur activists were targeted this quarter by a phishing attack and Android malware. Android/Chuli.A pretends to announce events and conferences of relevance to the targeted activists. Once the malware runs, it collects sensitive information that can help attackers locate infected users. After receiving the location and SMS information, the attacker can send further commands to each infected device.

Targeted Trojans expand geographically

As late as the end of last year, it was possible to say that the majority of mobile attacks were located in Russia and China. This quarter, however, we have seen criminals expand their activities to other parts of the world.

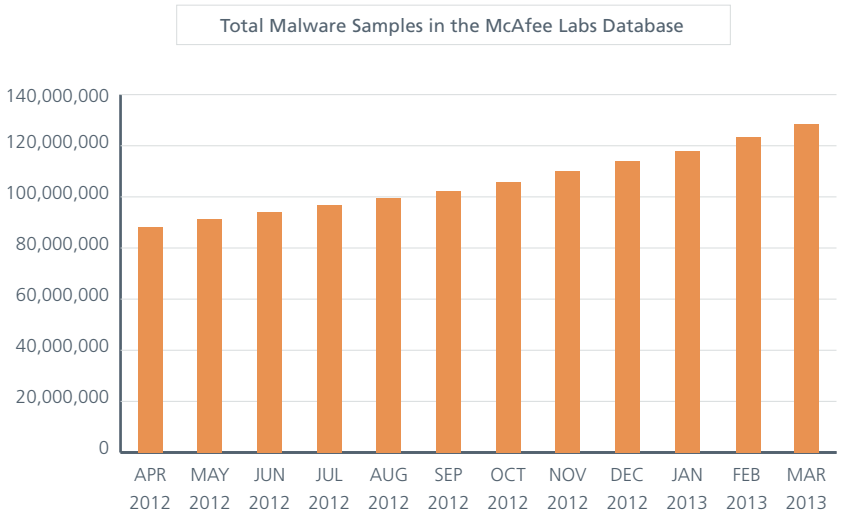
South Korea suffered a targeted attack from Android/Smsilence.A, which pretends to be a coupon app for a popular chain of coffee stores. When run, the malware pops up a message stating that there is a server error, while actually sending the user's phone number to the attacker. The malware is able to forward received SMS messages and delete other incoming texts. Smsilence.A checks the phone's country code to ensure it affects only South Koreans.

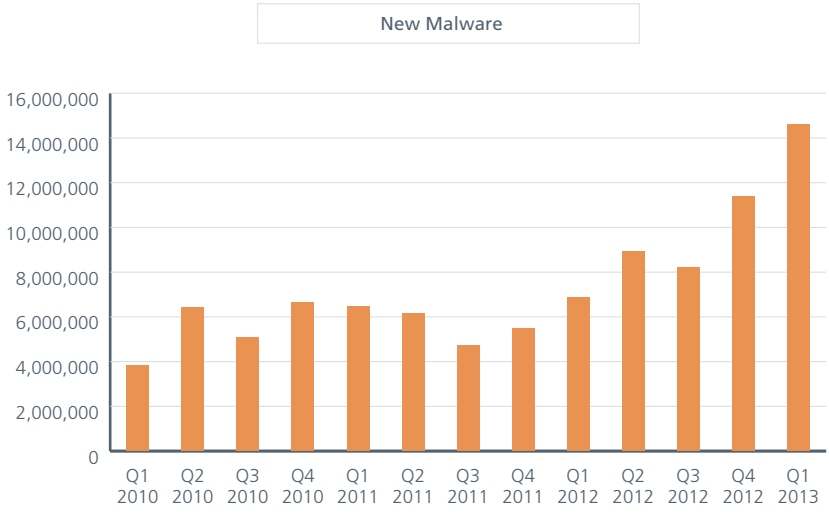
Indian users were affected by an advance-fee fraud facilitated by Android/Fakejoboffer.A. Advance-fee fraud convinces victims that they have won a prize or have received something of great value. Collecting this prize requires only that they pay a nominal fee. The victims lost this advance fee because the prize or item of value never existed. After the victims pay the "fee," Fakejoboffer.A displays a screen of a job interview letter, which informs victims that they have been selected for a job interview from a multitude of candidates and that they should pay for their travel expenses to get to the interview office. The victims are told that they will be reimbursed for their ticket costs when they arrive at the (nonexistent) interview.

Online banking users in Italy, Thailand, and Australia were also assailed by mobile criminals. Android/Fksite.A claims to be secure banking software but instead it forwards mobile transaction authorization numbers (mTANs) to attackers. These numbers have a limited lifespan after which they are useless for logging into a bank account. An attacker who intercepted an mTAN would need to make sure it was still active to steal money from an account. Android/FkSite.A ensures that the attacker gets fresh mTANs by checking whether they're still "alive" before forwarding them.

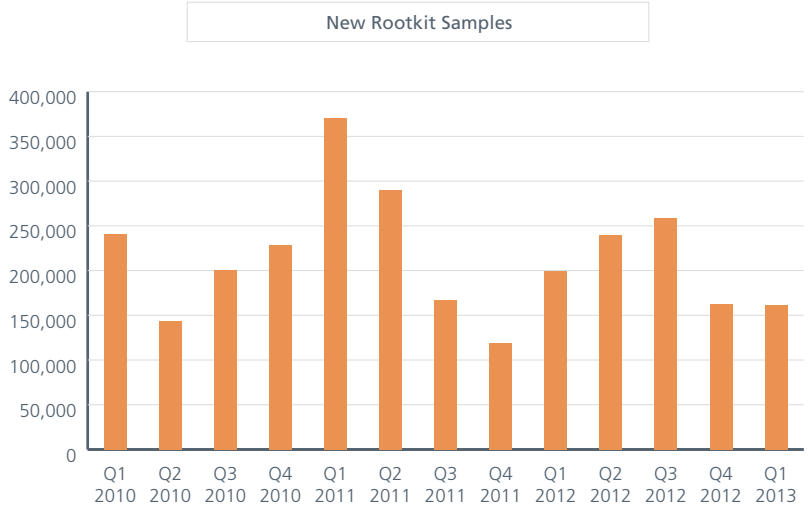
General Malware Threats

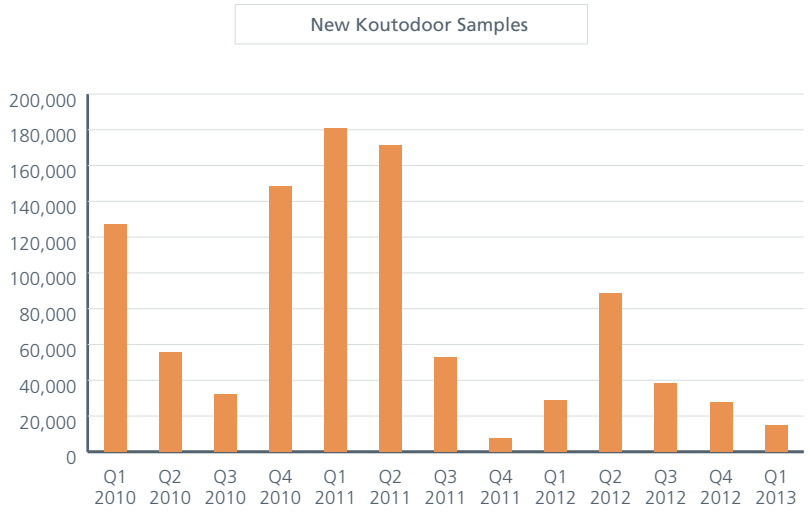
Malware shows no sign of changing its steady growth, which has risen steeply during the last two quarters. At the end of this quarter we now have more than 128 million samples in our malware "zoo."

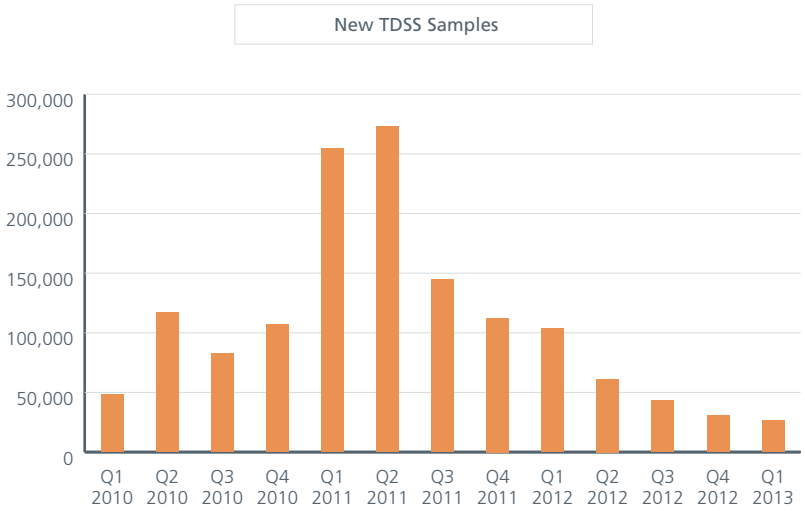


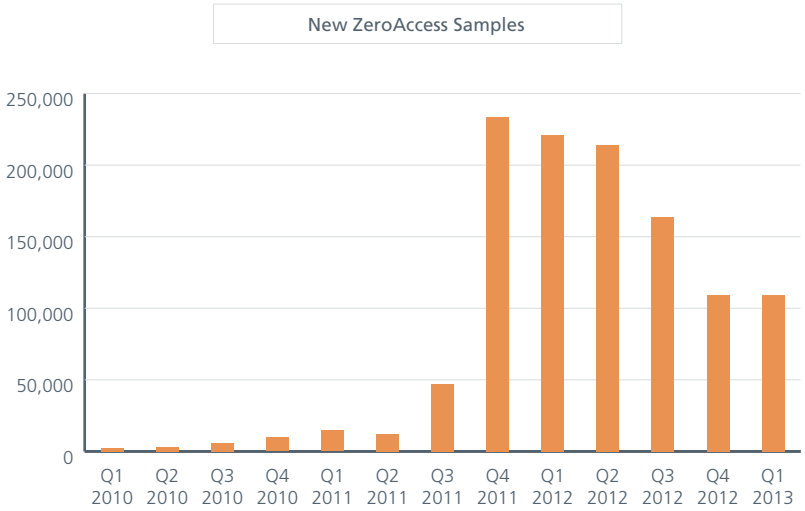


Rootkits, or stealth malware, are one of the nastiest classifications of malware we see. They are designed to evade detection and reside on a system for prolonged periods. After rising during most of the past year, growth in new rootkit samples has been flat for two quarters. All three of the rootkits types we track in this report matched this trend.

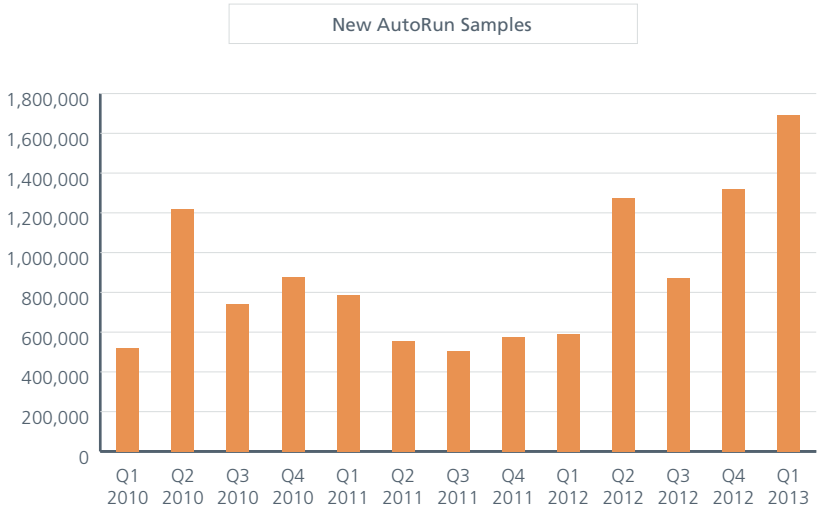


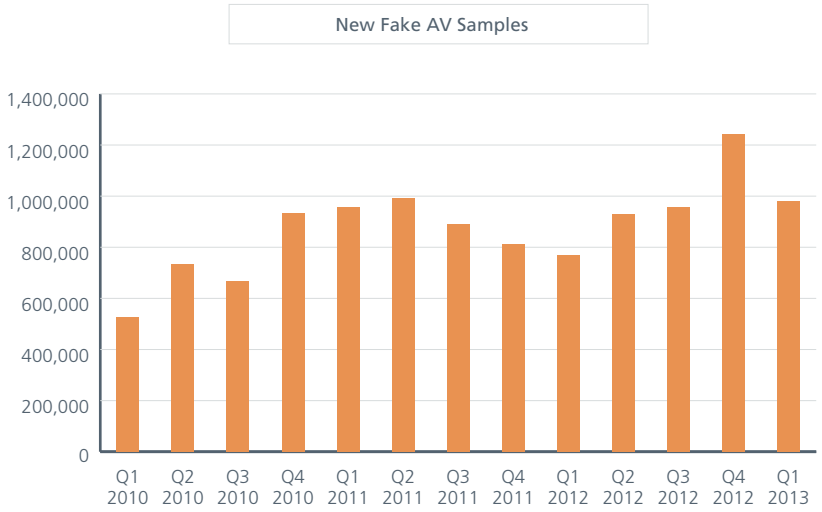


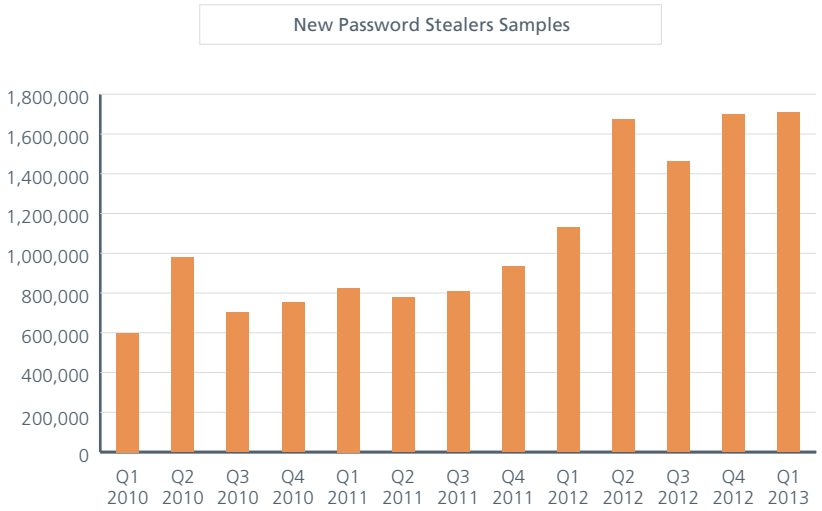




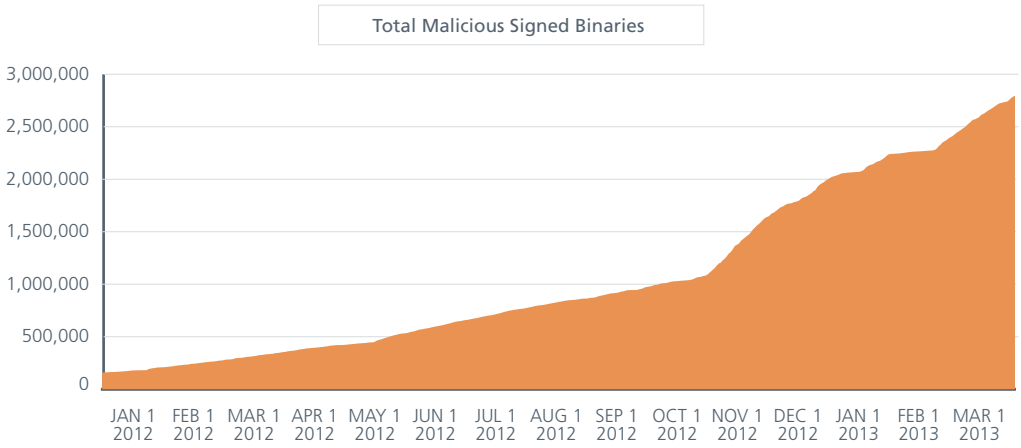
AutoRun malware, which often hides on USB drives and can allow an attacker to take control of a system, has risen rapidly for two quarters and reached a new high, with almost 1.7 million new threats. The number of fake antimalware products—which can behave as a form of ransomware, extorting money from victims to "clean" their computers—declined from its record level at the end of last year, but the overall numbers remain high. Password-stealing Trojans, which attempt to raid victims' bank accounts, were flat in growth yet established a new record.

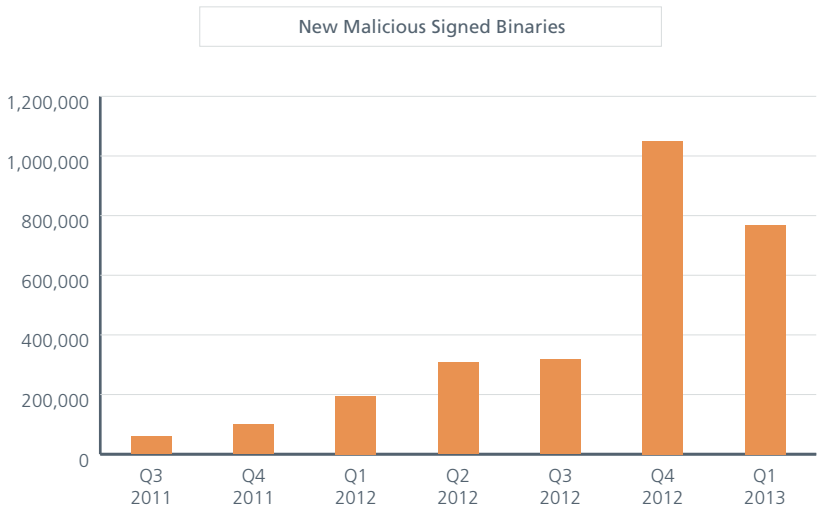

New AutoRun Samples
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
Q1 2010
Q2 2010
Q3 2010
Q4 2010
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013


New Fake AV Samples
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
Q1 2010
Q2 2010
Q3 2010
Q4 2010
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013

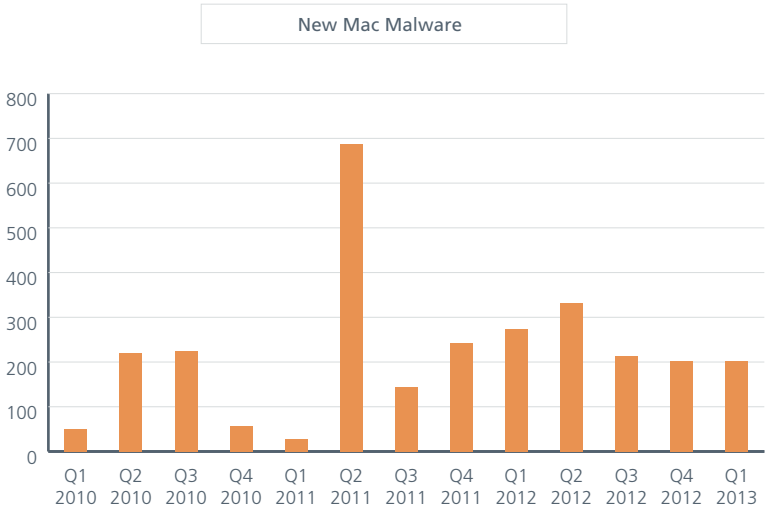


Signed malware dropped considerably from its immense leap in the fourth quarter, but still turned in the second highest period we've recorded.

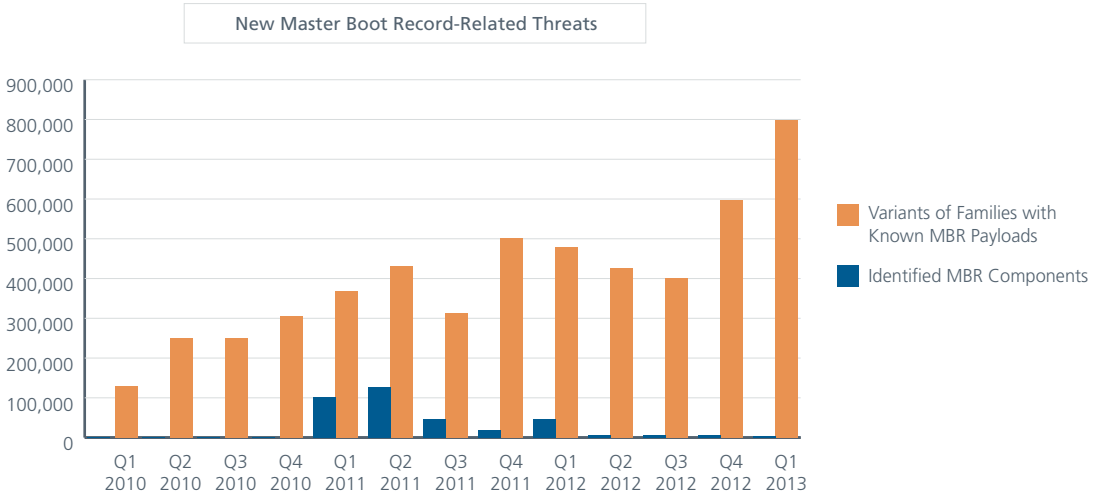




New malware that attacks the Mac has registered flat growth for three straight quarters. In spite of the small numbers compared with PC threats, Mac users also need protection.



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. These attacks, including mebroot, Tidserv, Cidox, and Shamoon, have rapidly increased their numbers and have set a new record high for two quarters running.

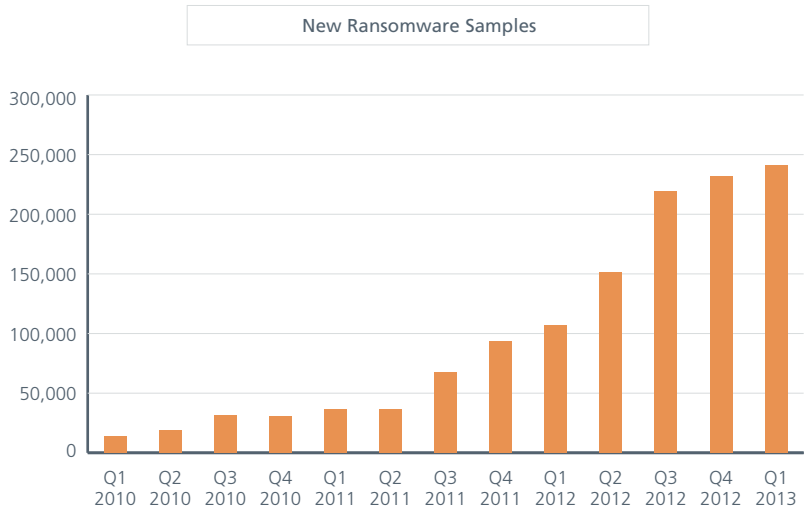


Ransomware

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 approaches 250,000, but the most worrying aspect is the number of reported infections. We have limited visibility into these figures because only our consumer products can share detection data with us. (We make that information public.[2]) This trend is also reflected by warnings from law enforcement and federal agencies around the globe.

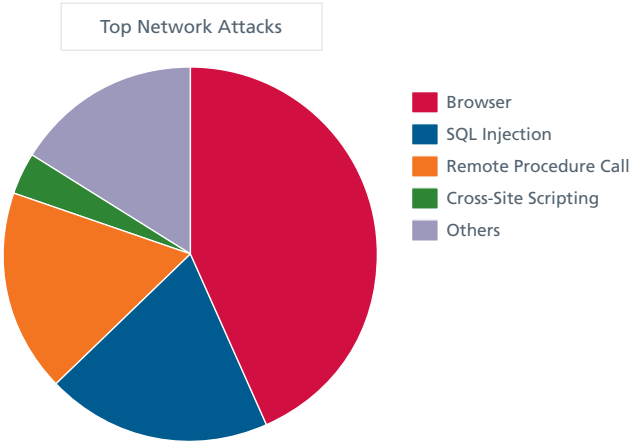
One reason for ransomware's growth is that it is a very efficient means for criminals to earn money because they use various anonymous payment services. This method of cash collection is superior to that used by fake AV products, for example, which must process credit card orders for the fake software. 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. Criminals can buy kits like Lyposit—whose malware pretends to come from a local law enforcement agency (based on the computer's regional settings) and instructs victims to use payment services in a specific country—for just a share of the profit instead of for a fixed amount.

These advantages mean that the problem of ransomware will not disappear anytime soon. You should always take precautions to back up your valuable data.

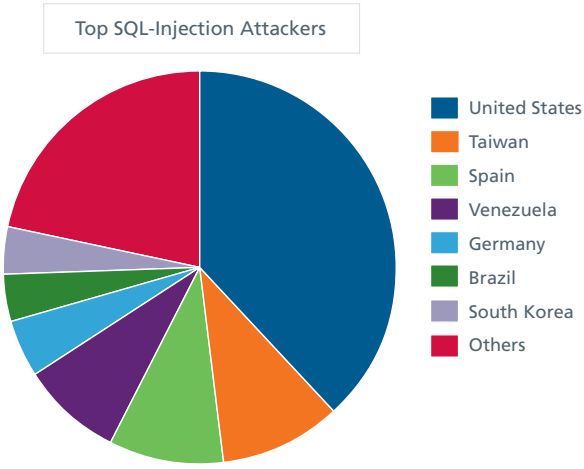


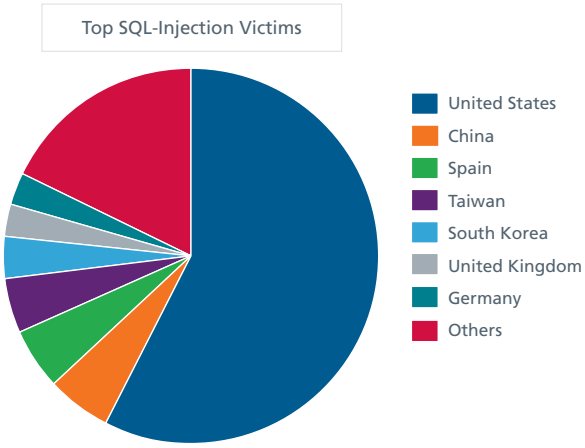
Network Threats

As usual the United States is both the source and the target of much of the Internet's malicious activity, according the McAfee Global Threat Intelligence™ network. Browser-based threats continue to lead all network attacks and have increased since last quarter. SQL injections and remote procedure calls are, respectively, the second and third most popular threats.

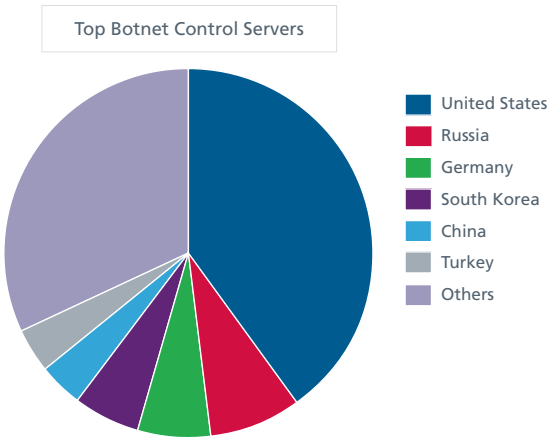


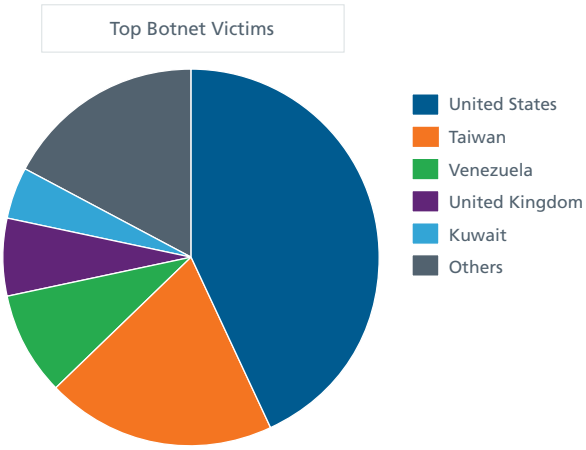
As the host of SQL-injection attacks, which poison legitimate websites, the United States' piece of the pie shrunk this quarter. Taiwan and Spain moved ahead of last quarter's second place, Venezuela. By far most victims of these attacks are in the United States.



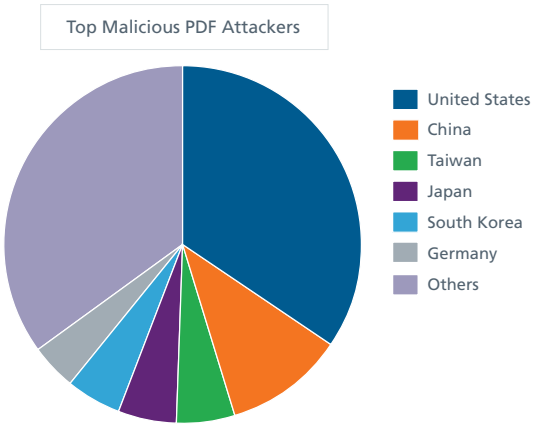


In our botnets tracking, the United States holds on to first place, with percentages mostly unchanged from last quarter. Russia and Germany again take the following places among control servers. Among victims, Taiwan moves into second place this time, pushing Venezuela to third.





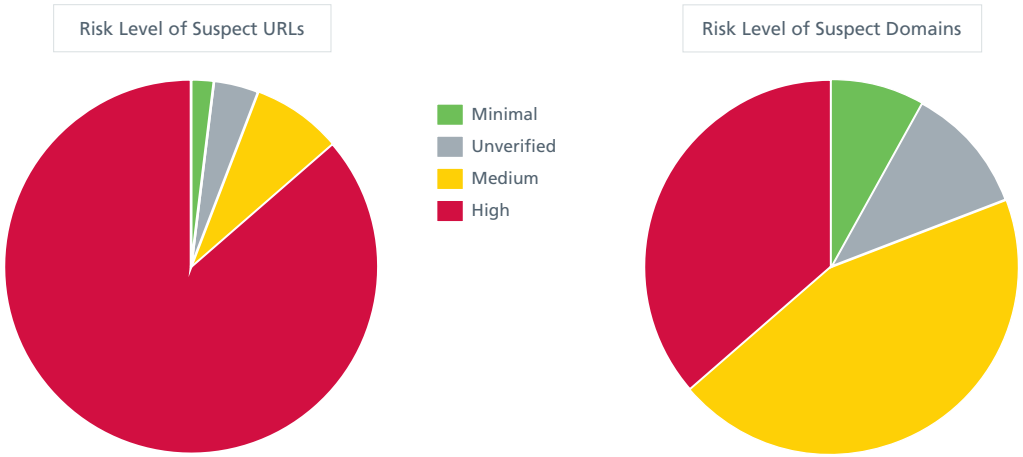
The United States regained the largest piece of the pie (35 percent) among countries hosting the most PDF exploits this quarter, as South Korea dropped from first place to fifth. China, with 11 percent, held onto second.



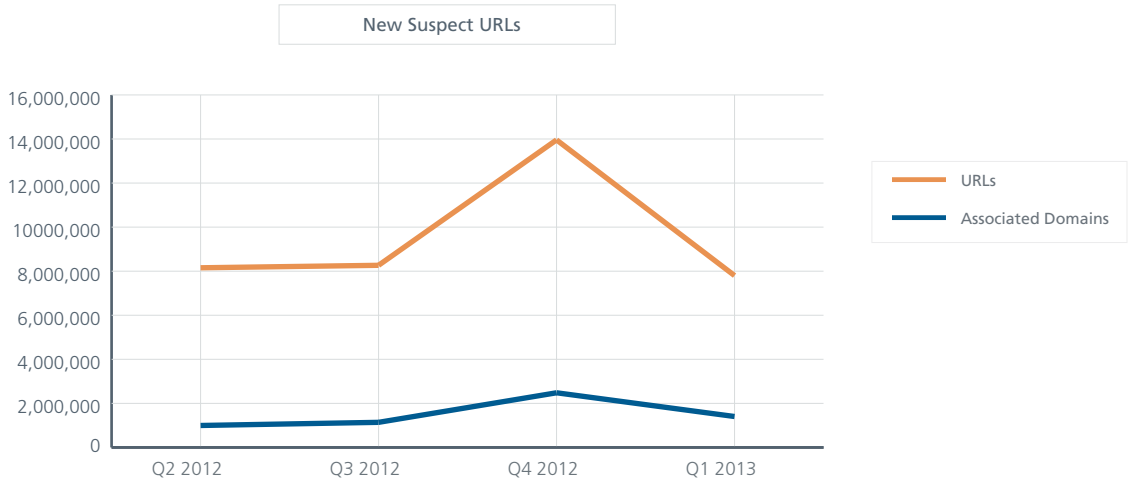
Web Threats

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 just a few of the factors that contribute to our rating of a site's reputation.

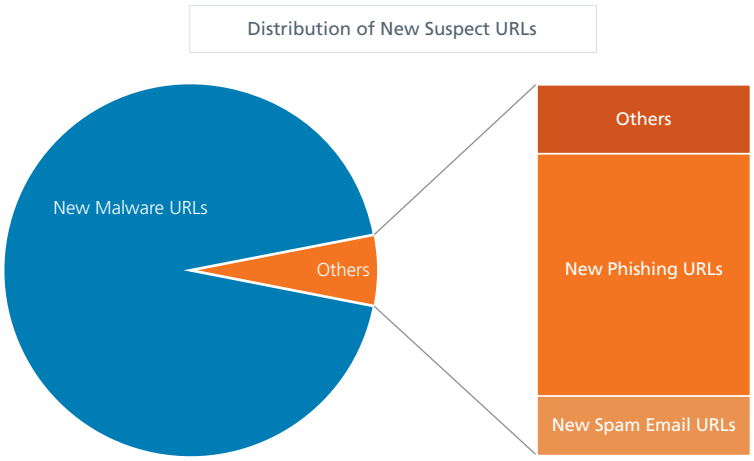
At the end of March, the total number of suspect URLs tallied by McAfee Labs overtook 64.3 million, which represents a 12 percent increase over the fourth quarter. These URLs refer to 27.7 million domain names, up 6 percent from the previous period. In our databases, we classify these URLs and domains according to their risk ratings.



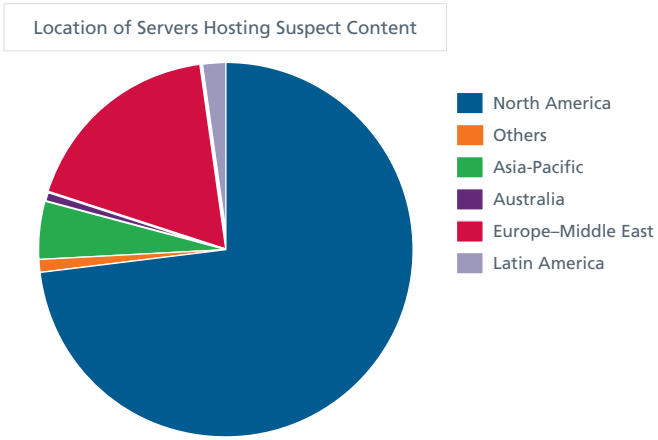
This quarter we recorded an average of 2.6 million new suspect URLs per month related to about 470,000 domains. These figures return to the levels we encountered in the second and third quarters of 2012.



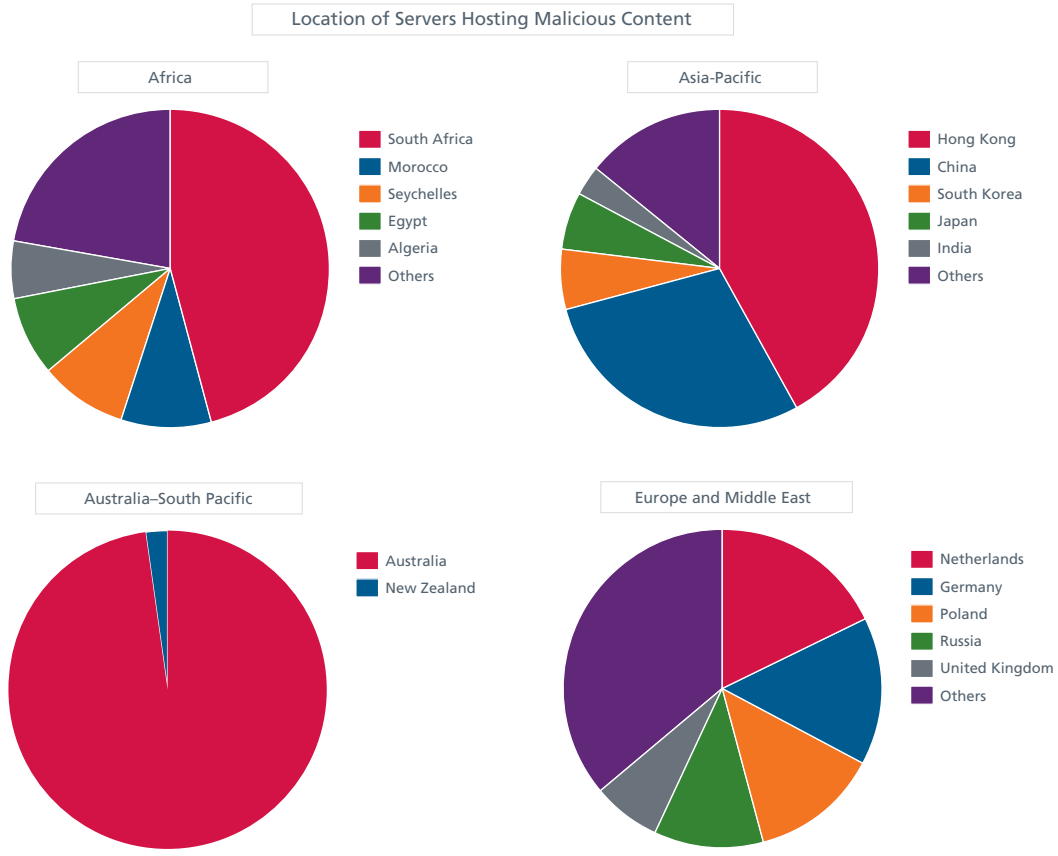
Most of these suspicious URLs (94 percent) host malware, exploits, or code that have been designed specifically to compromise computers. Phishing and spam represent 2.5 percent and 1.8 percent, respectively.

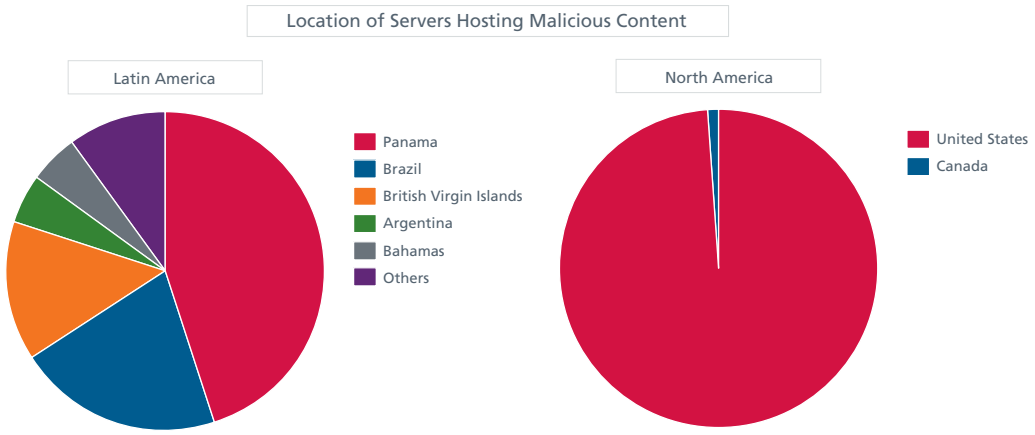


The domains associated with newly suspect URLs are mainly located in North America (chiefly the United States) and in Europe and the Middle East (chiefly the Netherlands). This trend is not new; North America historically hosts quite a bit of malware and suspect content.



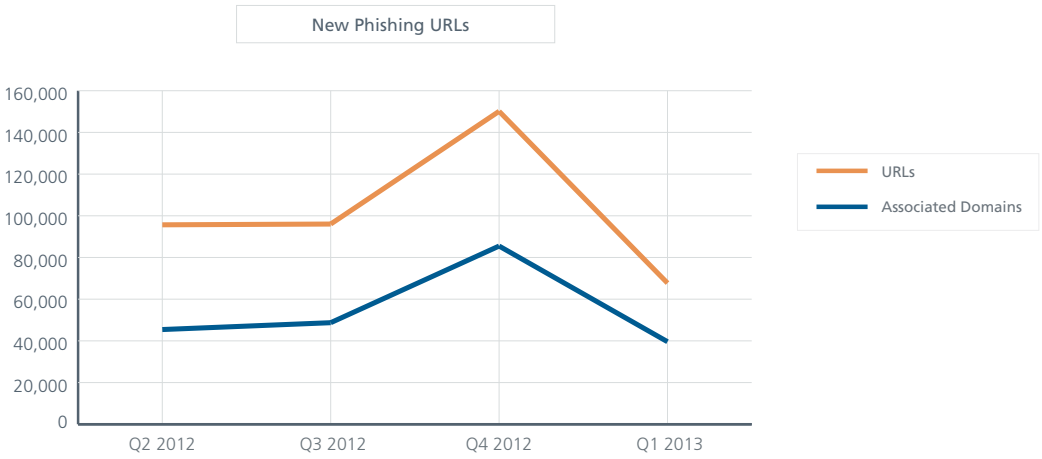
Digging into the location of servers hosting malicious content in other countries we see quite a global diversity. Each region has one or two clearly dominant players.



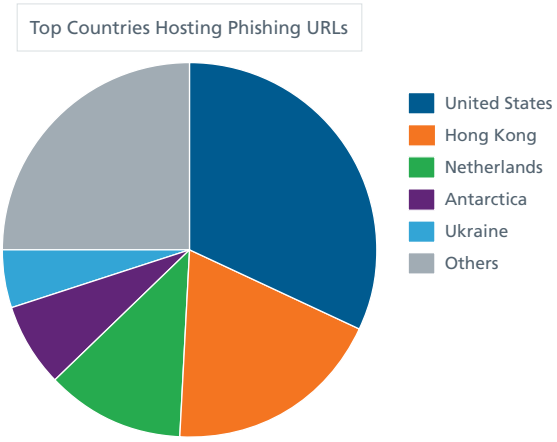


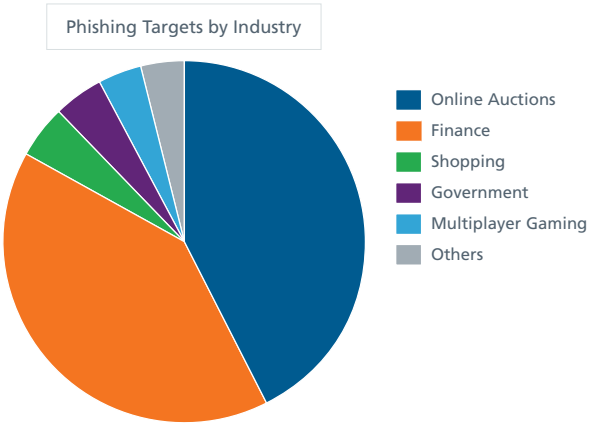
Phishing

After last quarter's 50 percent increase in the number of new phishing URLs, this quarter we saw the numbers drop below the level of previous quarters.



Most of these URLs are hosted in the United States. We were surprised this quarter to find Antarctica on this list!



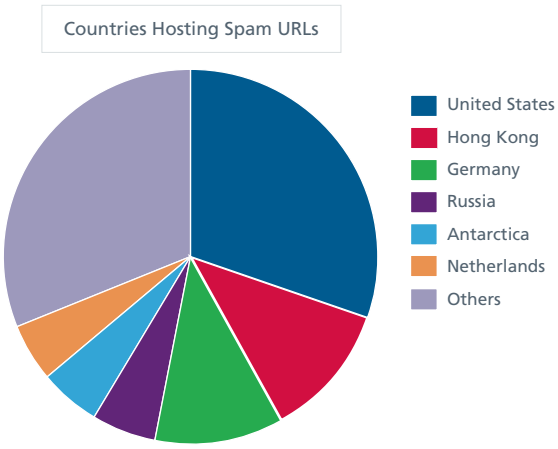


Companies from the United States are the most targeted, suffering 80 percent of all attacks. They are followed by United Kingdom and Brazil, with 5 percent and 3 percent, respectively. Phishers go after several key industries: finance, government, shopping, online auctions, and multiplayer gaming.

United States	United Kingdom	Brazil	Italy	Australia
Amazon	Barclays	Banco Bradesco	Intesa Sanpaolo	ANZ (Australia and New Zealand Banking Group)
Blizzard Entertainment	HM Revenue & Customs	Banco do Brasil	Posteitaliane	Westpac Bank
eBay	HSBC	Banco Itau	UniCredit	
Internal Revenue Service	Lloyds TSB			
J.P. Morgan Chase	Natwest			
PayPal	Royal Bank of Scotland			
Wells Fargo				

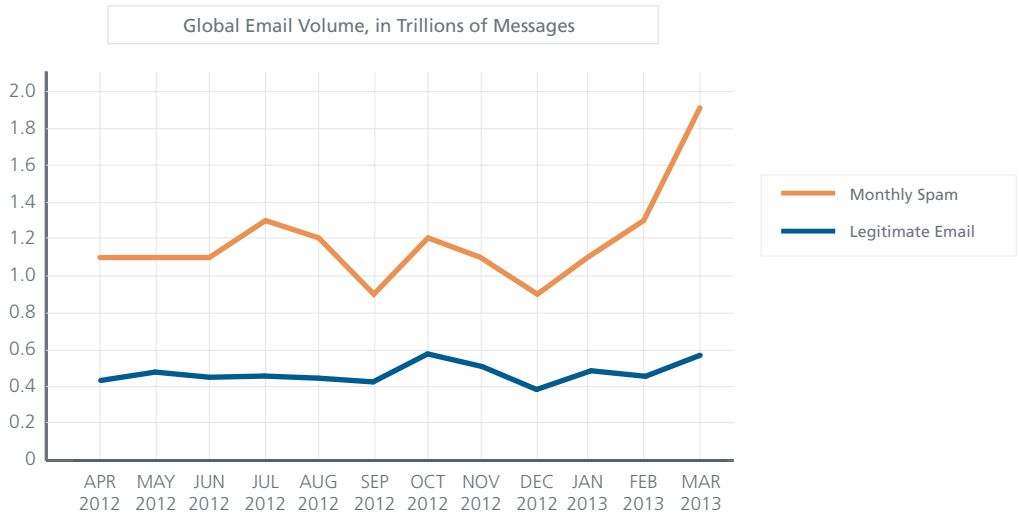
Spam URLs

Spam links are those that arrive in unsolicited spam emails. This family includes sites built only for spamming purposes, such as spam blogs or comment spam. New URLs jumped from about 30,000 last quarter to more than 45,000 this quarter. The primary countries hosting these URLs are the United States, Hong Kong, and Germany. Antarctica again joins the party.



Messaging Threats

After a long decline, spam levels were stable in 2012 despite some small upticks in July and October. This quarter, however, we saw a big increase that reached a volume not matched since May 2011.

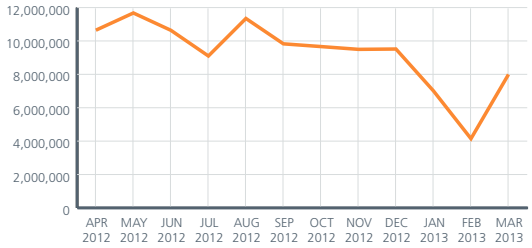


Spam volume

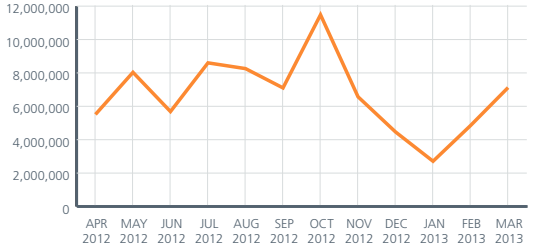
Although the global volume of spam is generally falling, our statistics by country show marked differences from quarter to quarter. Belarus is the most dramatic example, with a 540 percent increase this period. The next are Kazakhstan, at 150 percent growth, and Ukraine with 41 percent. Peru (58 percent), South Korea (54 percent), and Germany (53 percent) enjoyed large declines.

Spam Volume

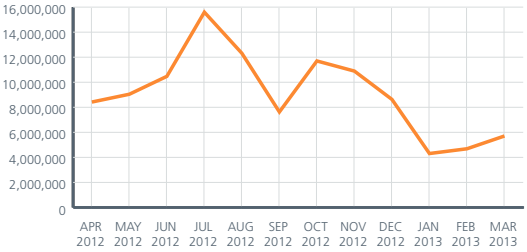
China



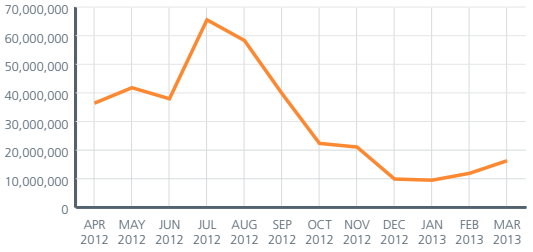
Columbia



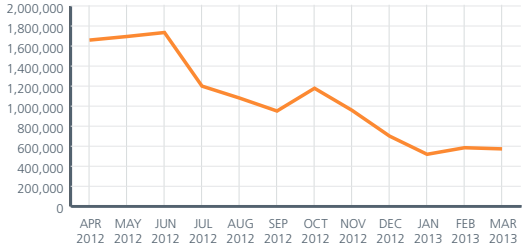
Germany



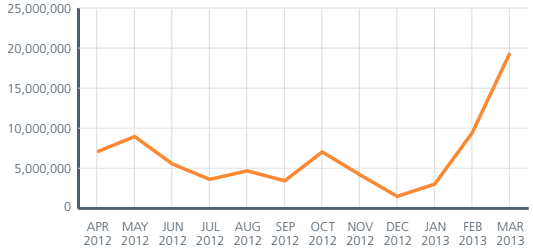
India



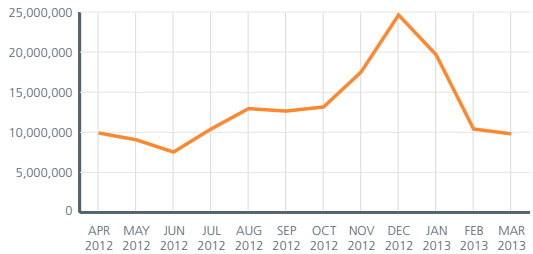
Japan



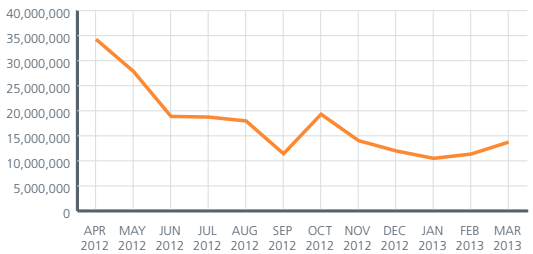
Kazakhstan



Romania

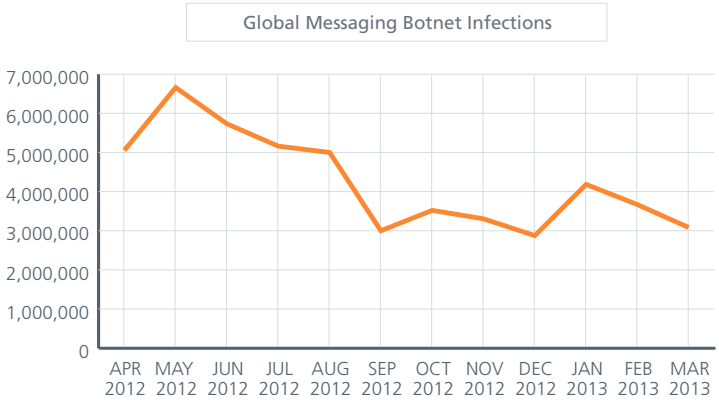


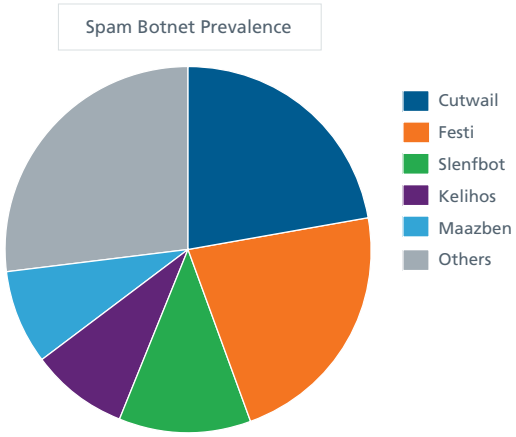
Russia



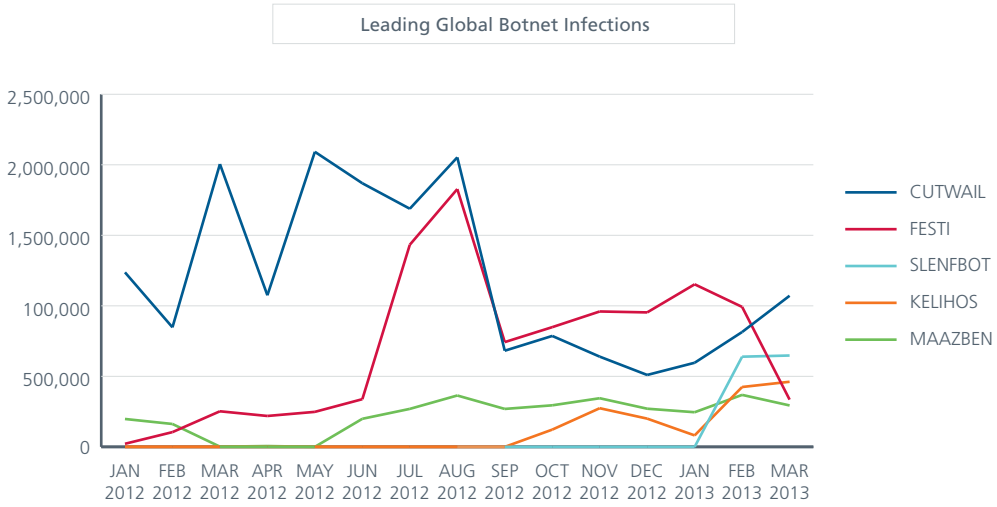
Botnet breakdowns

Infections from messaging botnets have showed an overall decline since May 2012. Last period, the level matched that of the fourth quarter 2011. This quarter we saw a rise in January, followed by a drop to the same level as three months ago.



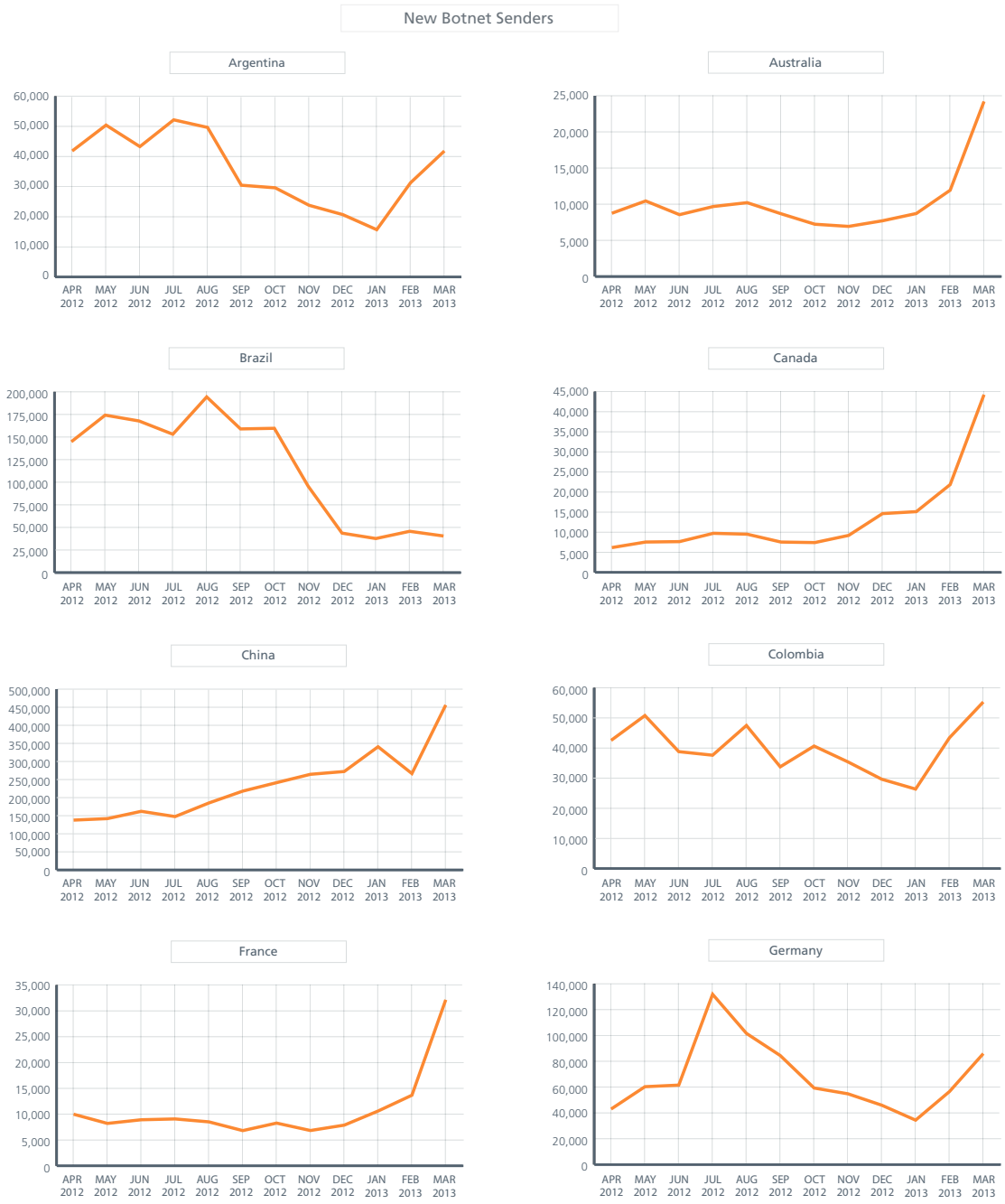


Waledac was shut down and dropped off our chart at the end of last year. This quarter, Lethic disappeared from our leaders' lineup. Kelihos was the new arrival last quarter; this period's rookie is Slenfbot. Cutwail is the current most prevalent botnet. Festi led just a few months ago, but has now fallen to fourth spot.



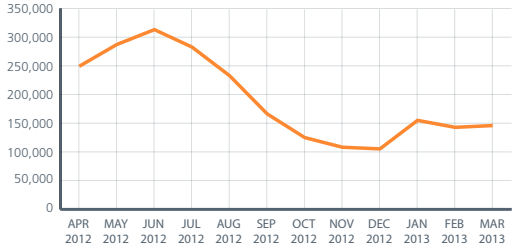
New botnet senders

Like country-specific spam, country-specific botnet statistics show big variances from last quarter to this quarter and among countries. In Japan the number of botnet senders increased by 420 percent, the Netherlands by 270 percent, Canada by 160 percent, and France by 145 percent. Meanwhile Brazil dropped by 60 percent and Peru by 50 percent.

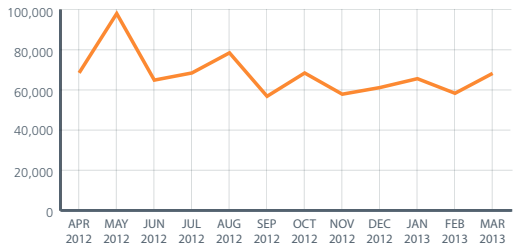


New Botnet Senders

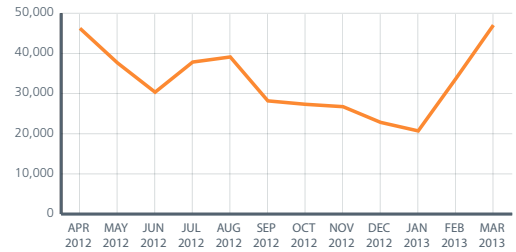
India



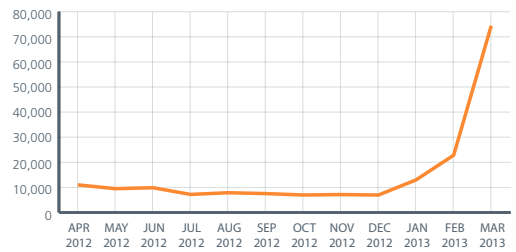
Iran



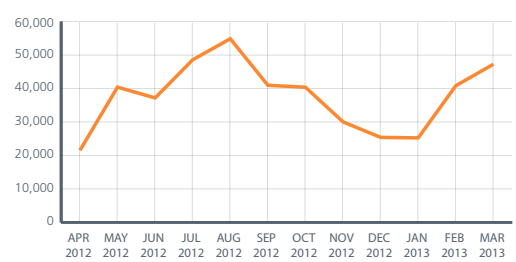
Italy



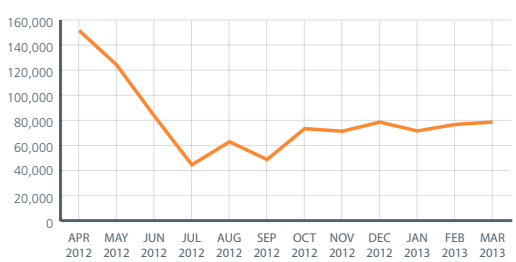
Japan



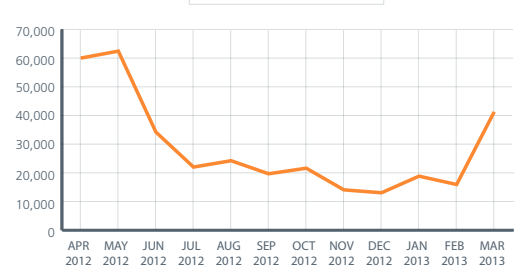
Mexico



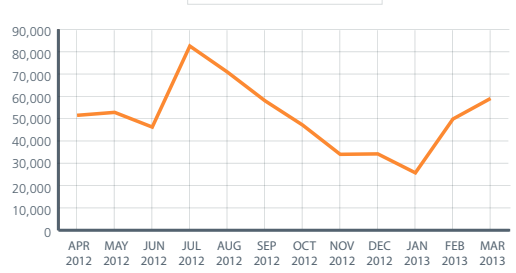
Russia



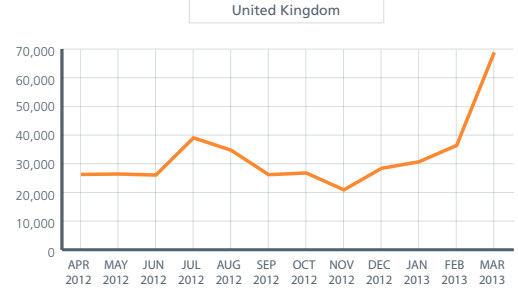
South Korea



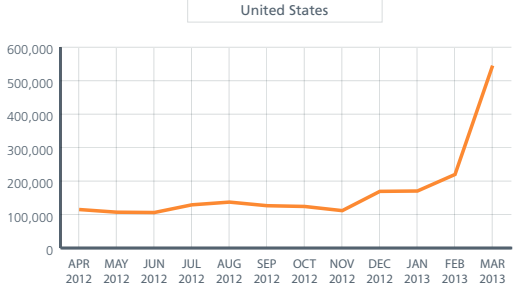
Spain



United Kingdom



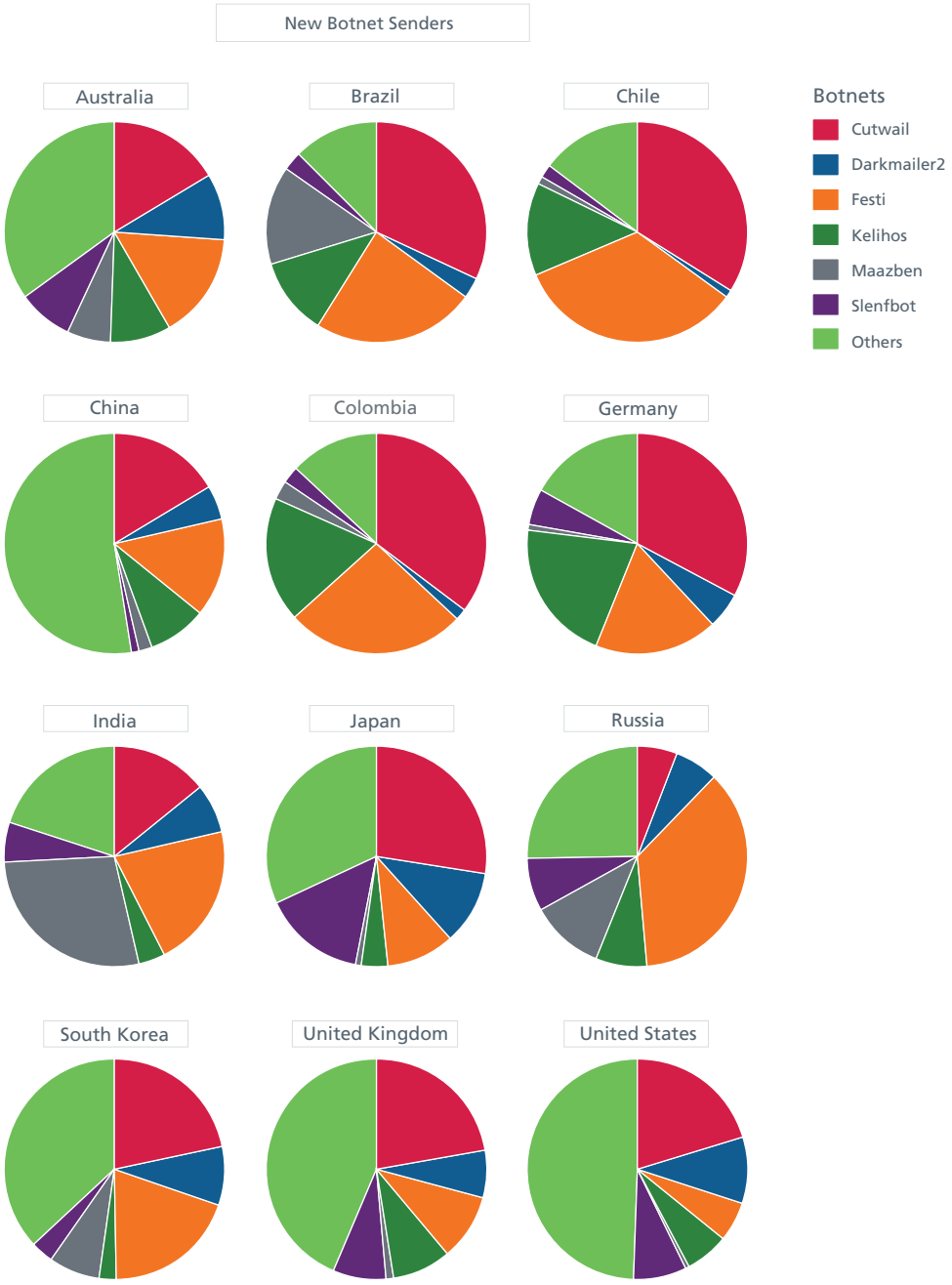
United States



Messaging botnet prevalence

Our breakdown of botnets shows the popularity of the five most widespread botnet families in various countries around the globe, with Cutwail and Festi the global leaders. Other notable prevalence:

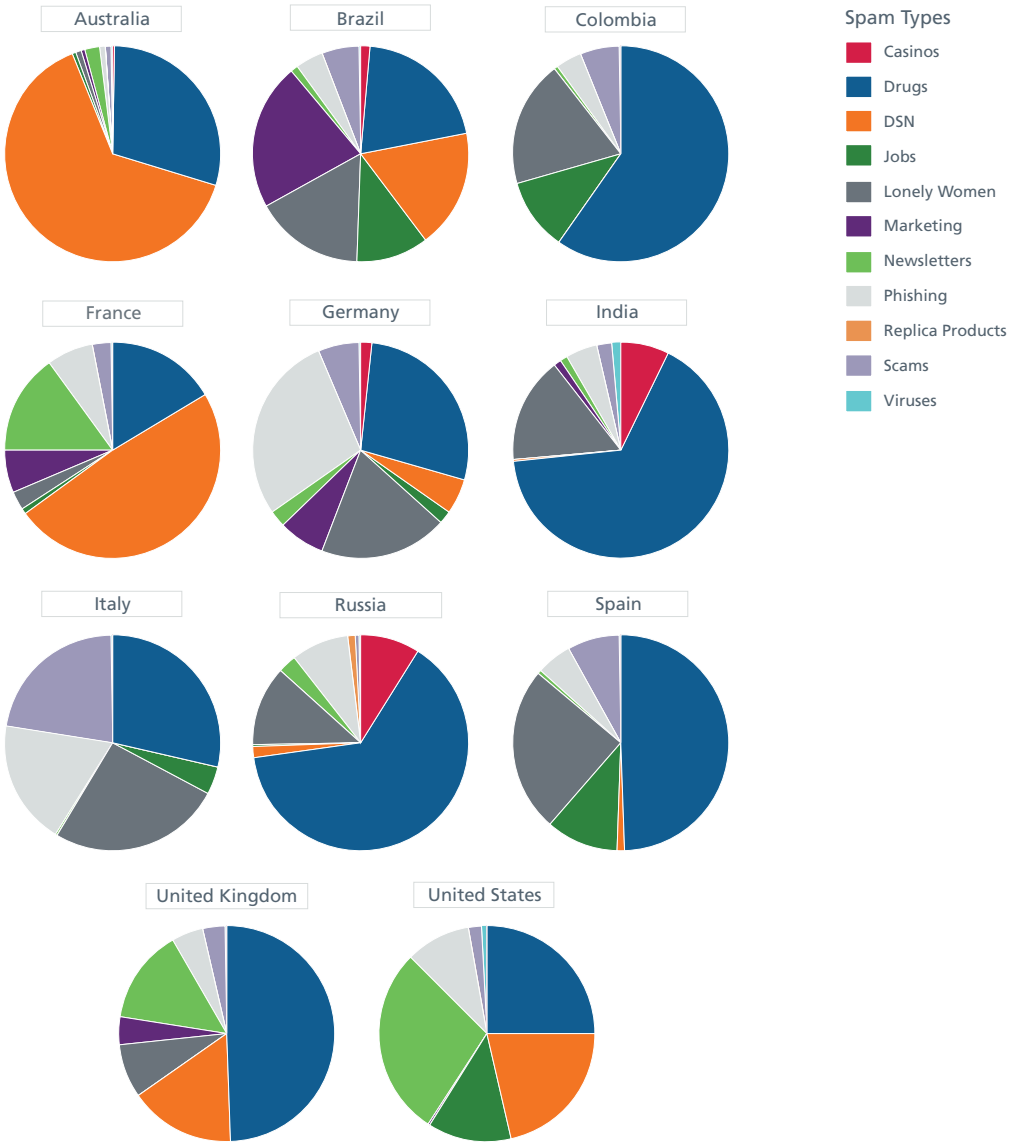
- Darkmailer in Belarus, Kazakhstan, Pakistan, and Indonesia
- Cutwail in Argentina, Spain, Greece, and Mexico
- Festi in Russia and Morocco
- Slenfbot in Belarus, Kazakhstan, and Ukraine



Drugs and DSN

As we look at spam subject lines around the world, we see that drugs and Delivery Service Notification teasers remain widely popular. Drug spam is generally associated with lots of infections because it is botnet based. The United Kingdom was an especially big target this quarter. In Germany phishing lures rank highly. In India, Italy, Poland, and Spain "lonely women" make frequent appeals for companionship, surpassing Russia as the usual top spot for unhappy potential brides. In the United States and France newsletters attempt to "subscribe" readers.

Argentina, Brazil, and Spain sent a lot of job spam in Polish. This could be a conspiracy to hire Polish workers, but it's probably just an indication that a Spanish-speaking "snowshoe" spammer was spreading the load across many IP addresses, to avoid rapid eviction by ISPs. Spam promoting pump-and-dump stock schemes was way up this quarter, no doubt riding the recent market wave to appeal to unwary investors seeking higher gains. But it's never a good move for traders to get involved with these types of stocks.



Cybercrime

Crimeware tools

Several vulnerabilities made headlines this quarter. Related exploits were incorporated into multiple popular exploit frameworks:

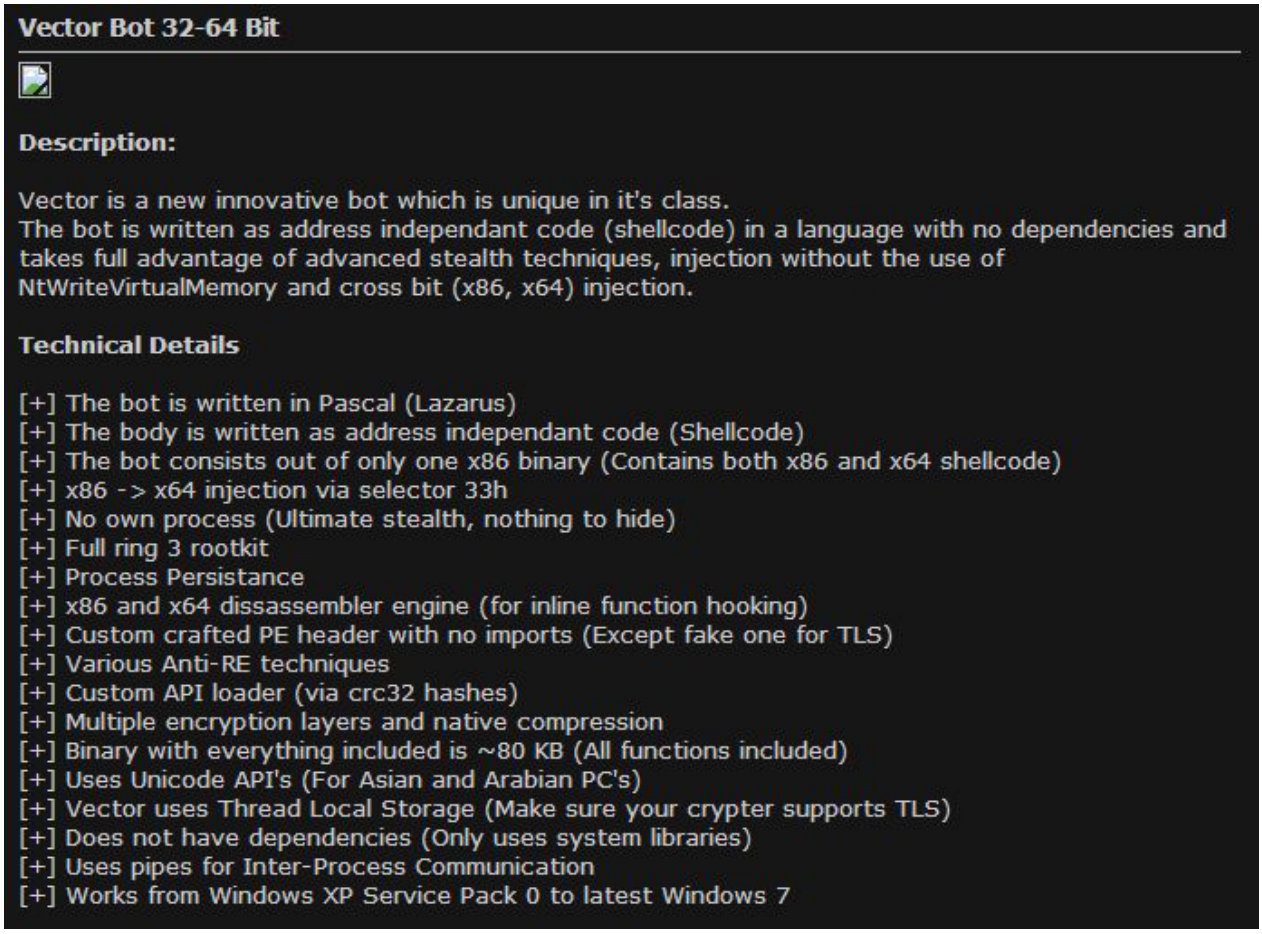
- CVE-2013-0422 (CButton): Oracle Java Runtime Environment setSecurityManager() Code Execution. Incorporated into Blackhole, Nuclear, Cool, Sakura, Sweet Orange, and others.
- CVE-2013-0431 (MBeanInstantiator): Oracle Java SE Java Runtime Environment JMX III Remote Code Execution. Incorporated into Blackhole, Nuclear, Cool, Sakura, Styx, Sweet Orange, and others.
- CVE-2013-0437: Oracle Java SE Java Runtime Environment 2D 1 Remote Code Execution
- CVE-2013-0634: Adobe Flash Player Malformed Regular Expressions Remote Code Execution. Incorporated into Gong Da, Fiesta, and others.
- CVE-2013-1493: Oracle Java JVM Process Remote Code Execution. Incorporated into Styx and others.

The following table summarizes some of the exploit packs researchers found available for sale this quarter.

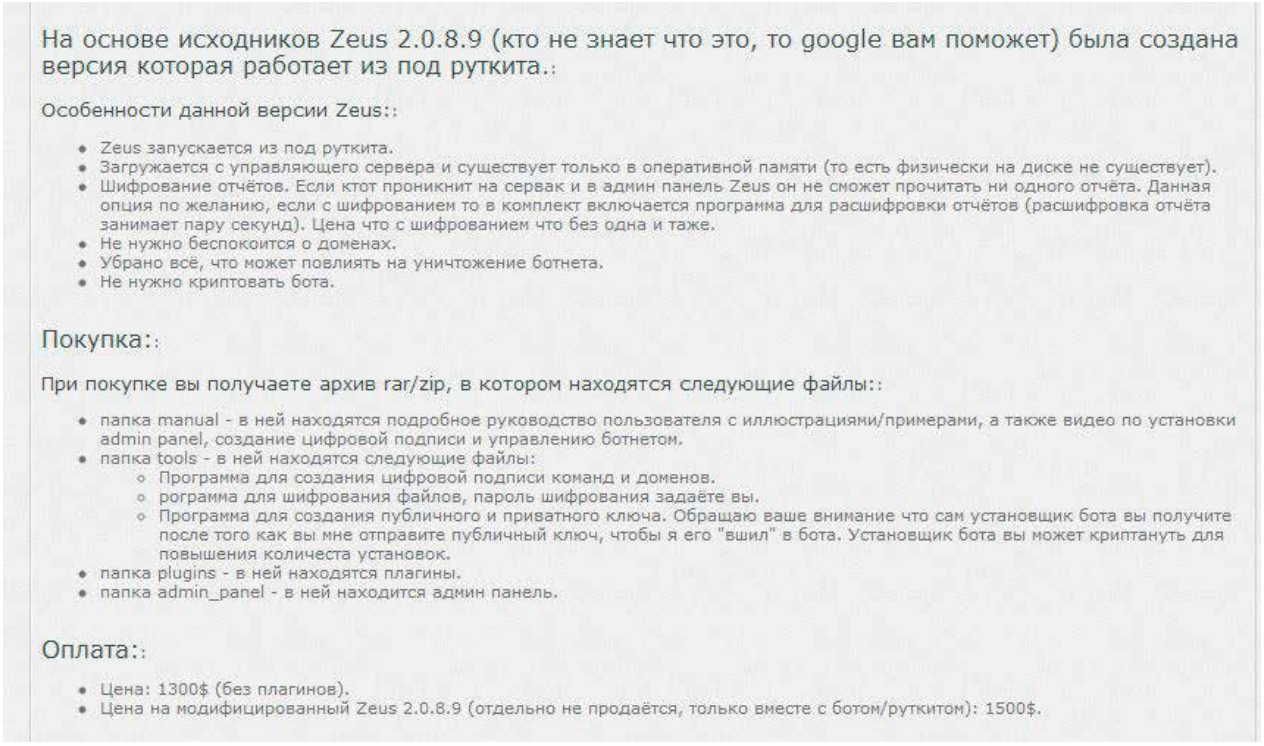
Exploit Pack	Vulnerabilities
Gong Da 1.3[3] (January)	• CVE-2011-3544: Java Rhino • CVE-2012-0507: Java Atomic • CVE-2012-1535 • CVE-2012-1723: Java Applet Field • CVE-2012-1889: MS XML Core • CVE-2012-4681: Java Gondvv • CVE-2012-5076: JAX-WS • CVE-2013-0422: CButton
Gong Da 1.4[4] (February)	• Same as Gong Da 1.3 with two exceptions: ° CVE-2012-1535 (Removed) ° CVE-2013-0634 (Added)
WhiteHole[5] (January)	• CVE-2011-3544: Java Rhino • CVE-2012-1723: Java Applet Field • CVE-2012-4681: Java Gondvv • CVE-2012-5076: JAX-WS • CVE-2013-0422: CButton
Neutrino[6] (March)	• CVE-2012-1723: Java Applet Field • CVE-2013-0431

We also saw some botnet-creating malware for sale this quarter.

- Vector Bot, for €1,000, payable via Liberty Reserve



- Namtar Bot 1.0, based on the Zeus 2.0.8.9 leaked source code, costs US$1,500. Includes a rootkit. Some other modules:
  - DDoS module: US$350
  - Socks module: US$120
  - HOSTS File Modifier module: US$50
  - Backconnect Socks module: US$380



На основе исходников Zeus 2.0.8.9 (кто не знает что это, то google вам поможет) была создана версия которая работает из под руткита.:

Особенности данной версии Zeus::

- Zeus запускается из под руткита.
- Загружается с управляющего сервера и существует только в оперативной памяти (то есть физически на диске не существует).
- Шифрование отчётов. Если ктот проникнит на сервак и в админ панель Zeus он не сможет прочитать ни одного отчёта. Данная опция по желанию, если с шифрованием то в комплект включается программа для расшифровки отчётов (расшифровка отчёта занимает пару секунд). Цена что с шифрованием что без одна и таже.
- Не нужно беспокоится о доменах.
- Убрано всё, что может повлиять на уничтожение ботнета.
- Не нужно криптовать бота.

Покупка::

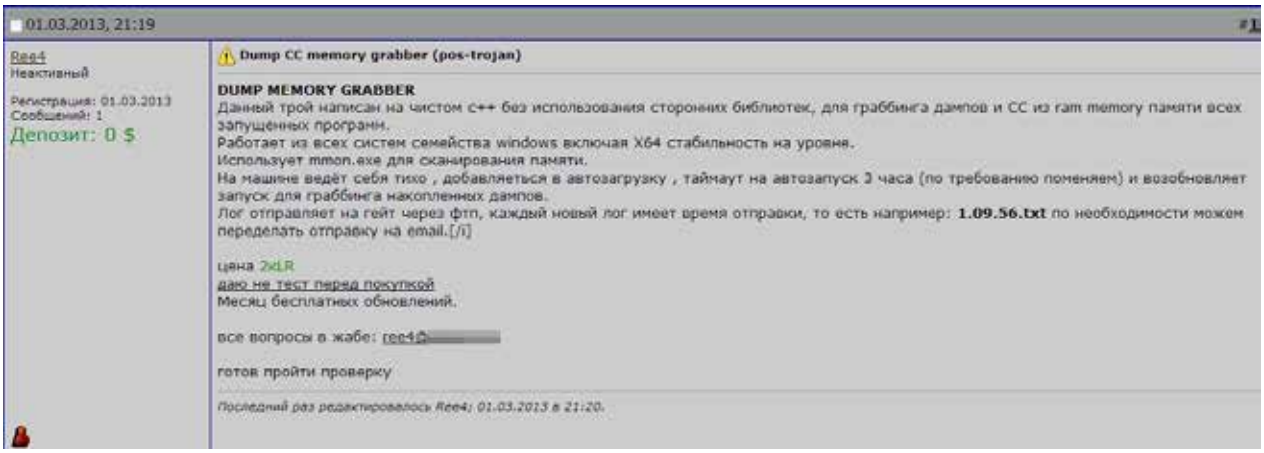
При покупке вы получаете архив rar/zip, в котором находятся следующие файлы::

- папка manual - в ней находятся подробное руководство пользователя с иллюстрациями/примерами, а также видео по установки admin panel, создание цифровой подписи и управлению ботнетом.
- папка tools - в ней находятся следующие файлы:
  - Программа для создания цифровой подписи команд и доменов.
  - рограмма для шифрования файлов, пароль шифрования задаёте вы.
  - Программа для создания публичного и приватного ключа. Обращаю ваше внимание что сам установщик бота вы получите после того как вы мне отправите публичный ключ, чтобы я его "вшил" в бота. Установщик бота вы может криптануть для повышения количеста установок.
- папка plugins - в ней находятся плагины.
- папка admin_panel - в ней находится админ панель.

Оплата::

- Цена: 1300$ (без плагинов).
- Цена на модифицированный Zeus 2.0.8.9 (отдельно не продаётся, только вместе с ботом/руткитом): 1500$.

- Dump Memory Grabber, discovered by Groupe-IB and CERT-GIB, is malware that steals payment card information from several US banks, including Chase, Capital One, Citibank, and Union Bank of California.[7] Installed in point-of-sale systems and ATMs, it collects Track 1 and Track 2 data and transfers the resulting log file to a remote server. The malware's author, who appears to have links to a Russian cybercrime gang, asks for US$2,000.



01.03.2013, 21:19 #1

Ree4
Неактивный

Регистрация: 01.03.2013
Сообщений: 1
Депозит: 0 $

Dump CC memory grabber (pos-trojan)

DUMP MEMORY GRABBER
Данный трой написан на чистом c++ без использования сторонних библиотек, для граббинга дампов и CC из ram memory памяти всех запущенных програмн.
Работает из всех систем семейства windows включая X64 стабильность на уровня.
Использует mmon.exe для сканирования памяти.
На машине ведёт себя тихо , добавляеться в автозагрузку , таймаут на автозапуск 3 часа (по требованию поменяем) и возобновляет запуск для граббинга накопленных дампов.
Лог отправляет на гейт через фтп, каждый новый лог имеет время отправки, то есть например: **1.09.56.txt** по необходимости можем переделать отправку на email.[/i]

цена 2кLR
даю на тест перед покупкой
Месяц бесплатных обновлений.

все вопросы в жабе: ree4[redacted]

готов пройти проверку

Последний раз редактировалось Ree4; 01.03.2013 в 21:20.

- VSkimmer is another financial malware. It can steal credit card information from Windows machines running financial transactions and credit card payments. The malware detects the card readers, grabs all the information from the Windows machines attached to these readers, and sends that data to a control server.[8] In March, a cybercriminal claiming to have purchased vSkimmer in 2012 for US$6,000, offered a cracked version with builder and web panel for €600.

Actions against cybercriminals

The European Union's new European Cybercrime Centre (EC3) was inaugurated in The Hague on January 11. Cooperating closely with the US Federal Bureau of Investigation and the US Secret Service, in addition to other foreign agencies, the Centre will facilitate research and development among law enforcement, judges, and prosecutors. It will produce threat assessments, including trend analyses, forecasts, and early warnings. The Centre will also offer operational support to EU countries (for example, against intrusion, fraud, online child sexual abuse, etc.) and deliver high-level technical, analytical, and forensic expertise in EU joint investigations.[9]

Most of the police successes we noted during the quarter involved EC3:

- In January, the FBI, on the trail for three years, arrested a 24-year-old Algerian in Thailand for allegedly hacking into banks. The US authorities accuse him of breaking into private accounts in more than 200 banks and financial institutions worldwide, allegedly causing millions of dollars in losses. Authorities asked that he be extradited to the United States, where a district court has issued an arrest warrant.[10] According to security analyst Brian Krebs, who actively monitors the cybercriminal underground, the hacker fits the profile of "bx1," a well-known cybercriminal suspected of being a major operator of Zeus-powered botnets.[11]
- In January, the FBI announced the unsealing of indictments against three individuals (one Russian, one Latvian, and one Romanian) who allegedly played critical roles in creating and distributing the Gozi malware.[12] This malware is known for infecting more than one million computers worldwide, among them at least 40,000 computers in the United States, including computers belonging to the National Aeronautics and Space Administration, as well as computers in Germany, Great Britain, Poland, France, Finland, Italy, Turkey, and other countries. Gozi has caused tens of millions of dollars in losses to the individuals, businesses, and government entities.
- In February, Spanish police, working closely with the EC3, announced the results of Operation Ransom, which dismantled a large and complex cybercrime network that spread "police" ransomware.[13] It was estimated that the criminals affected tens of thousands of computers worldwide, bringing in profits in excess of €1 million per year. The operation resulted in 11 arrests: The first was a 27-year-old Russian allegedly responsible for the creation, development, and international distribution of the various versions of the malware. He was arrested in the United Arab Emirates in December 2012. Another 10 individuals linked to the financial cell—six Russians, two Ukrainians, and two Georgians—were arrested in Spain's Costa del Sol.
- In March, Finnish law enforcement authorities and the EC3 dismantled an Asian criminal network responsible for illegal Internet transactions and the purchase of airline tickets. As a result of this successful operation, two members of the criminal gang traveling on false documents were arrested at Helsinki airport. In addition, around 15,000 compromised credit card numbers were found on the criminals' computers. The criminal network had misused credit card details stolen from cardholders. In Europe alone, cardholders and banks lost more than €70,000. There is evidence of further criminal activities in large-scale international payment fraud and illegal immigration.[14]

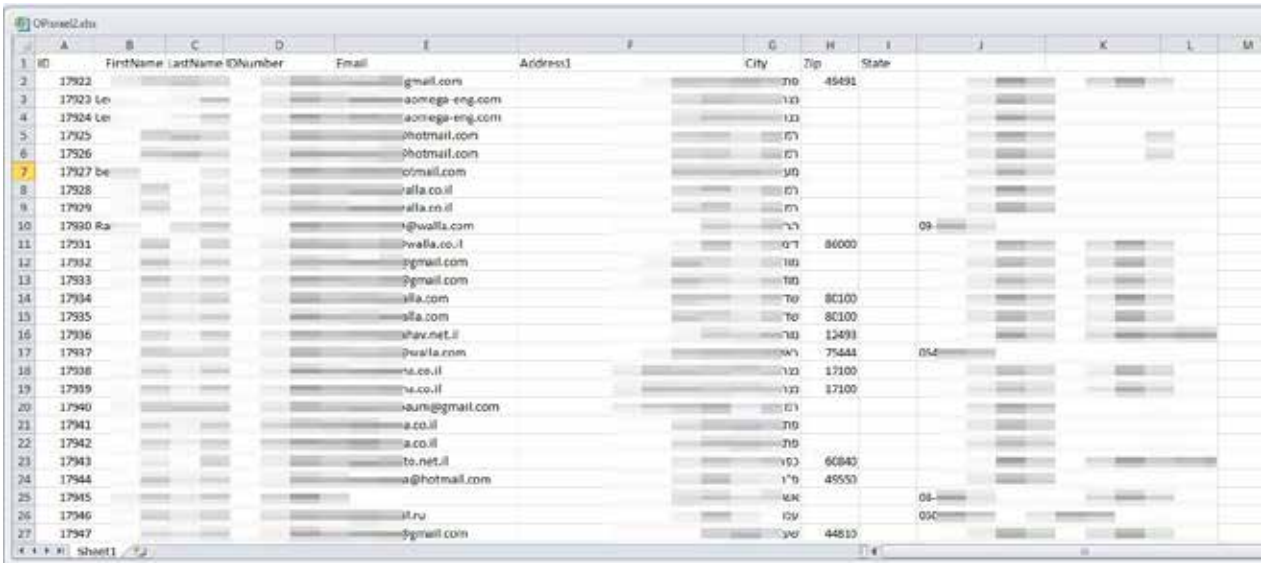
- In March, the Slovenian police detained five Slovenian citizens in a coordinated action that concludes the investigation of a series of attacks that started in mid-2012 against small companies. These attacks involved malware that upon infecting the victims computers logged passwords and installed components which allowed the attackers to observe activities on the infected systems. The attacks usually happened on Fridays or the day before national holidays in case the victims did not shut down the computer or remove the smart card containing the bank-issued certificate from the card reader. This left enough time for the attackers to queue bank transfer orders unobserved during weekends and holidays. The criminal group used 25 money mules to transfer around €2 million. Money mules were recruited with a work-at-home scam in the name of a fictitious British insurance company.[15]
- In March, Europol, EC3, and Romanian police arrested 44 alleged members of a global fraud ring believed to have tampered with payment terminals throughout Europe, stealing the details of tens of thousands of cards. The police operation Pandora-Storm saw more than 400 officers search 82 houses in Romania and the United Kingdom, arresting 44 and seizing illegal electronic equipment, financial data, cloned cards, and cash. The crooks had reportedly stolen the card numbers and PINs of around 36,000 people in 16 European countries before making counterfeits and carrying out transactions in Argentina, Colombia, the Dominican Republic, Japan, Mexico, South Korea, Sri Lanka, Thailand, and the United States.

Hacktivism

In the recent McAfee Labs white paper *Hacktivism: Cyberspace has become the new medium for political voices*, we discussed the issue of legalizing some forms of DDoS attacks to support activism.[16] That notion was put into play this quarter. In January, a petition was posted on the White House's "We the People" website that sought to have distributed denial-of-service actions against computer systems recognized as a legitimate form of protest.[17] To trigger a White House response, the petition needed 25,000 signatures, but it obtained only 6,000.[18]

On January 11, the tragic suicide of the young hacker and digital rights activist Aaron Swartz disrupted the activist world and prompted Anonymous to launch Operation Last Resort, which demands the reform of US computer crime laws. Among the hacks associated with this operation were Anonymous-published logins, hashed passwords (not in plain text), and private information such as contact data and cell phone numbers from more than 4,000 individuals. Anonymous claimed its victims included American bank executives: presidents, vice presidents, COOs, branch managers, VPs, and more. A spreadsheet was placed on a .gov website and Pastebin, and was publicized via various Anonymous accounts on Twitter and Facebook.[19]

#OpIsrael, launched in November 2012 in retaliation for Israeli attacks on the Gaza Strip, coordinated a spate of attacks this quarter. Various hacker teams close to Anonymous said they targeted official Israeli web domains, stealing data and causing intermittent disruption to the official website of spy agency Mossad via a self-described "sophisticated DDoS" attack. In this case, two Excel files were released by the Turkish group "The Red Hack," while "Sektor 404" claimed responsibility for the denial-of-service attack on Mossad.

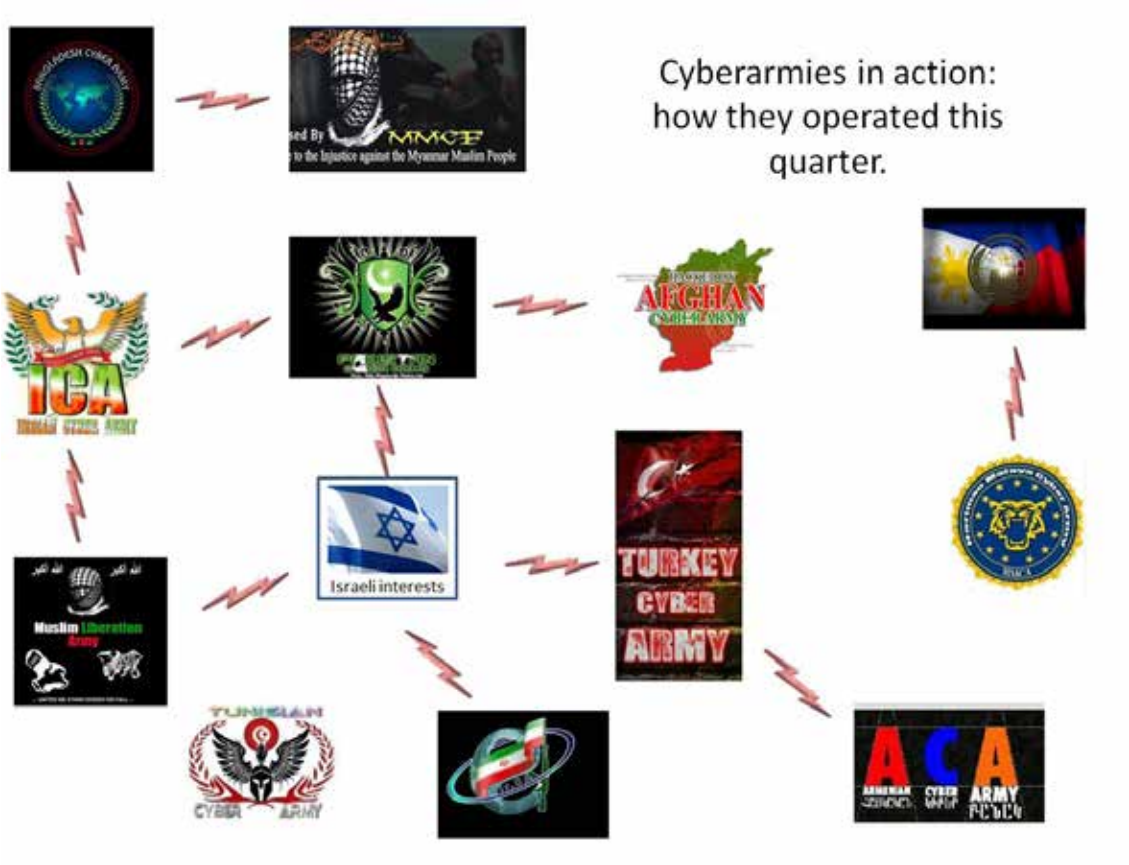


"There is no doubt that [the attackers] got some identification information about Israelis," said Middle East Internet expert Dr. Tal Pavel. "But the claims that they hacked the Mossad site and got a list of Mossad agents is most likely psychological warfare, and not a hack into an important database."[20] Anti-Israeli actions are expected to continue during the second quarter.

Cyberarmies

In *Hacktivism: Cyberspace has become the new medium for political voices*, we defined cyberarmies as formed by patriots in countries with totalitarian tendencies who claim, rightly or wrongly, to act on behalf of their governments by supporting national and extremist movements. Some readers asked McAfee Labs for further illustrations. Here are some of the most active during the quarter:

- 3xp1r3 Cyber Army: Bangladeshi hackers known for their mass defacing. In January, one member defaced more than 600 Indian websites.[21]
- Afghan Cyber Army: In January, they breached and defaced 34 Pakistani sites[22]
- Alarakai Cyber Army: Recently, they signed a site defacement with a picture of Osama Bin Laden and the message "We Mujahideen of al-Qaeda Internet want to stop fighting Muslims in Arakan in Myanmar (Burma)"[23]
- Armenian Cyber Army: The Turks failure to admit the 1915 Armenian genocide is the main motive for the attacks launched by this group. In February they defaced some Azerbaijani web sites.[24]
- Bangladesh Cyber Army: Another Bangladeshi group involved in Indian/Bangladesh hacker cyberattacks linked with conflicting events at the Bangladesh-India border[25]
- Brazilian Cyber Army: In February, the group claimed to have hacked the official website of Sierra Leone Police[26]
- Indian Cyber Army: Nationalist group known for its clashes with the Pakistan Cyber Army. In 2012, it joined with Anonymous on certain operations.
- Iranian Cyber Army: Supports the Iranian regime. Its opponents say it operates under the Intelligence Unit of the Revolutionary Guard.[27] In March, they defaced numerous websites.[28]
- Muslim Liberation Army: Pakistani group known to attack Indian websites in 2012 to protest its presence in Kashmir. In February, a member of this group hacked and defaced more than 25 Israeli sites to deliver a message supporting Palestinians.[29]
- Pakistan Cyber Army: Claim not to be a hacking or cracking group or anything illegal, but a symbol of all the Pakistani security experts who want to safeguard Pakistani cyberspace from hacking attacks. In February, the group hacked various Indian websites.[30]
- Philippine Cyber Army: In March, the group attacked 175 Malaysian sites (including state-owned pages), in response to Malaysian hackers asking people to send a message to the Philippine government to keep away from the region of Sabah.[31] They are close to Anonymous.
- Syrian Electronic Army: Known to support Syrian President Bashar Assad, who saluted the youth of the Electronic Army in a speech in June 2011, when they first emerged.[32] In February, they took over the Agence France-Presse photo department's Twitter feed.[33] In March, they gained access to an administrator's account for Human Right Watch, calling the organization's report that Assad is using cluster munitions "false."[34]
- Tunisian Cyber Army: In March, they assaulted US government websites (as part of #opBlackSummer).[35] They jointly signed the attack with the Al-Qaeda Electronic Cyber Army.
- Turkey Cyber Army: Announced various defacements via their Facebook account.



One person's view of totalitarianism varies from another's, just as one view of democracy varies from another. So let's choose a standard: If we use the Reporters Without Borders World Press Freedom Index, we find that the freest country is Finland, at No. 1, and the least free, Eritrea, is ranked No. 179.[36] With the exception of Armenia, all of the countries hosting cyberarmies are ranked above 100, and nine of 13 fall between numbers 138 and 176. Nations that offer many freedoms to their citizens are not "represented" by cyberarmies.

About the Authors

This report was prepared and written by Xiaobo Chen, Toralv Dirro, Paula Greve, Haifei Li, François Paget, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Dan Sommer, Bing Sun, 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 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. www.mcafee.com/labs

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-citadel-trojan.pdf
[2] http://home.mcafee.com/virusinfo/global-virus-map
[3] http://eromang.zataz.com/2013/01/13/gong-da-gondad-exploit-pack-add-java-cve-2013-0422-support/
[4] http://eromang.zataz.com/2012/12/02/cool-exploit-kit-remove-support-of-java-cve-2012-1723/
[5] http://malware.dontneedcoffee.com/2013/02/briefly-wave-whitehole-exploit-kit-hello.html
[6] http://malware.dontneedcoffee.com/2013/03/hello-neutrino-just-one-more-exploit-kit.html
[7] http://www.securityweek.com/exclusive-new-malware-targeting-pos-systems-atms-hits-major-us-banks
[8] https://blogs.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals
[9] http://europa.eu/rapid/press-release_IP-13-13_en.htm
[10] http://www.security-faqs.com/alleged-algerian-bank-hacker-arrested-by-fbi-in-thailand.html
[11] http://krebsonsecurity.com/2013/01/police-arrest-alleged-zeus-botmaster-bx1/
[12] http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusPR.php
[13] https://www.europol.europa.eu/content/police-dismantle-prolific-ransomware-cybercriminal-network
[14] https://www.europol.europa.eu/content/international-network-line-card-fraudsters-dismantled-newsletter
[15] http://www.cert.si/obvestila/obvestilo/article/slovenian-police-cracks-down-on-a-gang-netting-almost-2-million-EUR-from-companies-via-e-banking-hac.html
[16] Page 32. http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf
[17] http://news.cnet.com/8301-1009_3-57563188-83/anonymous-petitions-u.s-to-see-ddos-attacks-as-legal-protest/
[18] http://njtoday.net/2013/02/06/petition-to-have-white-house-recognize-ddos-as-legitimate-protest-unlikely-to-draw-response/
[19] http://www.zdnet.com/anonymous-posts-over-4000-u-s-bank-executive-credentials-7000010740/
[20] http://www.timesofisrael.com/dont-believe-hack-claims-against-mossads-website-expert-says/
[21] http://news.softpedia.com/news/Over-600-Indian-Websites-Defaced-by-3xp1r3-Cyber-Army-Hacker-318967.shtml
[22] http://www.thehackerspost.com/2013/01/34-pakistan-sites-hacked-defaced-by.html
[23] http://www.cyber-expertz.net/2013/01/68-italy-sites-include-3-govt-hacked-by.html
[24] http://www.armenews.com/article.php3?id_article=87754
[25] http://news.softpedia.com/news/Bangladesh-Cyber-Army-Attacks-Indian-Sites-in-Memory-of-15-Year-Old-Girl-Video-319234.shtml
[26] http://www.ehackingnews.com/2013/02/sierra-leone-police-website-hacked-by.html
[27] http://www.popsci.com/technology/article/2013-03/how-iran-censors-internet-infographic
[28] http://www.innsalzach24.de/innsalzach/waldkraiburg/waldkraiburg/waldkraiburg-homepage-realschule-ziel-eines-hacker-angriffs-innsalzach24-2783344.html
[29] http://www.thehackerspost.com/2013/02/israeli-server-hacked-by-hitcher-from.html
[30] http://hackread.com/bangalore-city-police-website-hacked-defaced-by-pakistan-cyber-army/
[31] http://www.malaysia-chronicle.com/index.php?option=com_k2&view=item&id=64242:sabah-crisis-sparks-cyberwar&Itemid=2
[32] http://www.npr.org/2011/09/25/140746510/pro-assad-army-wages-cyberwar-in-syria
[33] http://www.esecurityplanet.com/hackers/afp-twitter-feed-hacked-by-syrian-electronic-army.html
[34] http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/syria-rebel-hackers-syrian-electronic-army-anonymous-support
[35] http://hackread.com/tunisian-cyber-army-founds-xss-vulnerability-on-pentagon-website/
[36] http://fr.rsf.org/IMG/pdf/classement_2013_gb-bd.pdf

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

60244rpt_qtr-q1_0513_ETMG