

# McAfee Threats Report: Second Quarter 2012

By McAfee Labs

## Table of Contents

Mobile Threats	4
Malware Threats	6
Signed malware	10
Ransomware holds data hostage	12
Messaging Threats	12
Botnet Breakdowns	15
Spam Seeks to Deceive via social engineering	19
Network Threats	20
Web Threats	23
Cybercrime	27
Bulletproof hosting	27
Actions against cybercriminals	29
Hackivism	30
About the Authors	31
About McAfee Labs	31
About McAfee	31

Laozi, often called Lao Tzu, was a philosopher of ancient China. Author of the *Tao Te Ching*, according to tradition he lived in the sixth century BCE yet his insights remain valuable today. Looking at the ever-evolving threats landscape, he might say “My mind tells me to give up, but my heart won’t let me.” The threat landscape is indeed a battlefield. Maybe Sunzi, also known as Sun Tzu and another philosopher of ancient China, said it best with “Invincibility lies in defense; the possibility of victory in the attack.” We have learned much about malware and various threats over the years but they seem to grow and reach new heights each quarter. Whether malware and other cyberthreats are successful depends on many interconnected factors. Sunzi also noted “He who is prudent and lies in wait for an enemy who is not will be victorious.” Sounds like the answer lies in preparedness.

Looking at the second quarter of 2012, the key things that stood out were the emergence of mobile (Android) “drive-by downloads” as a new attack vector, the use of Twitter for control of mobile botnets, and the appearance of mobile “ransomware” as the newest way of extracting funds from unsuspecting victims. Much of the growth and rebound in malware and threats we saw last quarter has continued strongly. Last quarter PC malware had its busiest period in recent history, but this quarter has been even busier. We saw significant growth in established rootkits but a slowdown in others. Almost all of the families of malware we examine continue to reach new levels, with activity among password-stealing Trojans particularly strong. We continue our breakouts of the rootkit ZeroAccess, which has declined a bit, and signed malware, which increased slightly. There was also steady, continued growth in malware targeting the Mac. It’s not extreme, but the trend is upward nonetheless.

Spam showed some small increases in certain parts of the world, but the long-term trend is still on the decline. Of the countries we highlight in this report, only Colombia, Japan, South Korea, and Venezuela showed an increase greater than 10 percent. Botnet infections spiked sharply in May but then dropped off moving into June.

The United States again hosts the most new malicious web content of any country in the world. This dynamic appears in several other sections of this report. The United States is often the biggest originator and victim of a variety of threats. The web is a dangerous place for the uninformed and unprotected. Make sure you are trained and aware.

We present for the second time our new section on network-based attacks. We offer detailed geographical breakdowns of cross-site scripting and SQL-injection attacks—as well as others—from a variety of perspectives.

Looking into cybercrime we review “crimeware-as-a-service” from bulletproof hosting services and we explore some notable cybercrime takedowns, arrests, and indictments during the quarter. We also examine some recent shifts in the Anonymous hacktivist collective and hacktivism in general.

We find cybercriminals engaged in a long-term battle to separate us from our money. While we ponder new operating systems and other defensive technologies, let’s finish with some inspiration related to our battlefield analogy.

*You should not have any special fondness for a particular weapon, or anything else, for that matter. Too much is the same as not enough. Without imitating anyone else, you should have as much weaponry as suits you.*

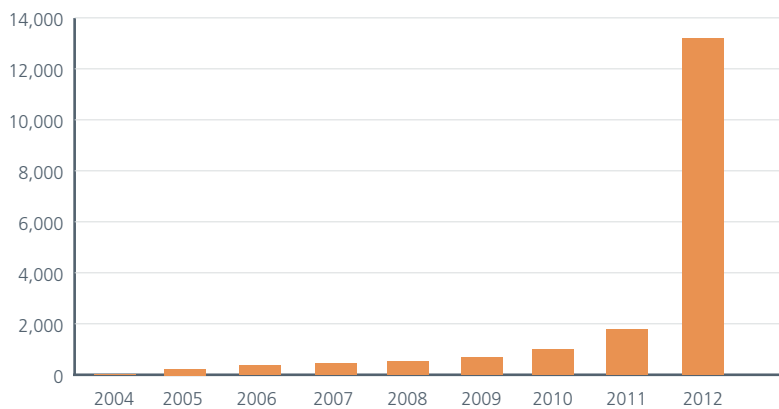
—Miyamoto Musashi, *The Book of Five Rings*

### Mobile Threats

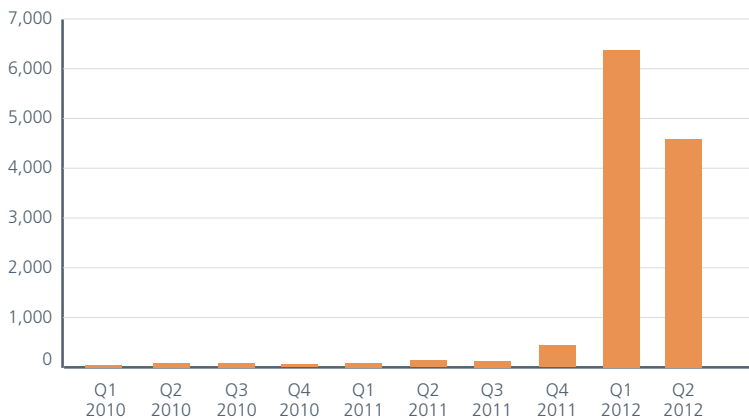
During the past few quarters we've seen that the Android OS is the most popular target for writers of mobile malware. This quarter was no different; practically all new mobile malware was directed at the Android platform. The mix included SMS-sending malware, mobile botnets, spyware, and destructive Trojans.

Although in sheer numbers this quarter was not as explosive as the last, growth this year remains unprecedented.

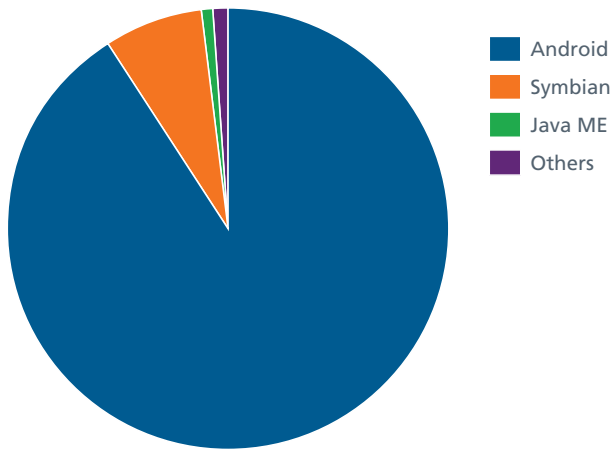
Total Mobile Malware Samples in the Database



New Mobile Malware by Quarter



Total Mobile Malware by Platform



Drive-by downloads arrived for Android this quarter with Android/NotCompatible.A. Similar to drive-by installs on the PC—simply visiting a site infects your computer—mobile drive-by downloads drop malware on your phone when you visit a site. A victim still needs to install the downloaded malware, but when an attacker names the file Android System Update 4.0.apk, most suspicions vanish.

A new botnet client, Android/Twikabot.A, uses Twitter for control. Instead of connecting to a web server, the malware searches for commands from specific attacker-controlled Twitter accounts. The attacker can tweet commands and all infected devices will follow them. Using a service such as Twitter allows an attacker to leverage the resources of others without paying for a dedicated server or stealing one that belongs to a victim. Internet relay chat servers have been exploited in the past for similar reasons, but using the web service gives attackers a small measure of anonymity.

Last quarter we saw an Android Trojan horse program, Android/Moghava.A, that corrupts all photos on an SD card. This quarter it appears malware authors have created a new variant, Android/Stamper.A, which uses a different picture and targets fans of a popular Japanese singing group. The image is from a “What would your baby look like?” competition from last year. This variant doesn’t change anything except the image and a few strings in the image-stamping code from Android/Moghava.A, meaning that it also has the same bug that corrupts photos. Fans expecting to get results from the pop group’s fan elections instead have all their pictures photo-bombed by a baby.

If much of Android malware seems familiar to PC malware, it should come as no surprise. Malware writers leverage the expertise they honed during the years of writing malware for other platforms. Mobile malware is certainly not proof-of-concept or early code. It is fully functional and mature, and mobile malware writers know what they are looking for: consumer and business data.

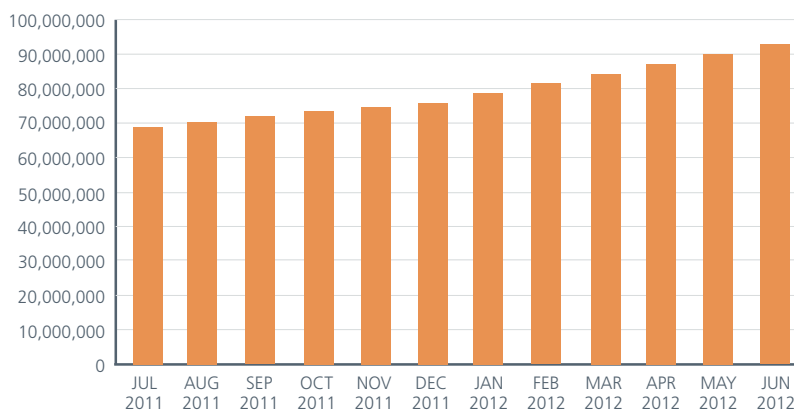
## Malware Threats

In his famous essay *The Myth of Sisyphus*, Albert Camus introduces his philosophy of the absurd: our futile search for meaning and clarity in the face of an unintelligible world devoid of truths or values. The final chapter compares the absurdity of human life with the punishment of *Sisyphus*, a figure in Greek mythology who was condemned to repeat forever the same meaningless task of pushing a boulder up a mountain, only to see it roll down again.

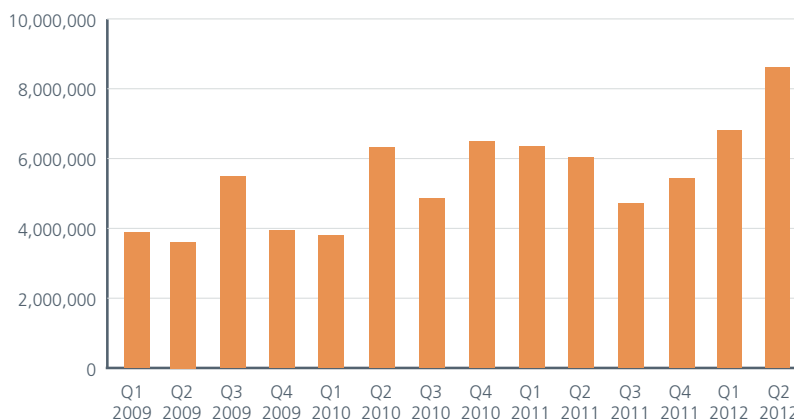
When we look back over the last decade of malware growth, we appear to see the same mountain that caused Sisyphus so much futile toil. In fact, in recent years the mountain seems to be getting higher and steeper. Last time we had detected the largest number of malware per quarter in the last four years—until we look at this quarter! Unique malware samples in our “zoo” collection number 1.5 million more this quarter than last. At this rate we will almost certainly see 100 million samples by next quarter and possibly the first 10-million-sample quarter. Do those numbers actually matter in some way? What do they tell us about the way we conduct defensive information security?

At the least, they tell us that the boulder is getting heavy. With very few exceptions, almost all areas of malware are up this quarter from last (and last quarter had record growth in some areas). One thing is certain: To continue to take the same steps is absurd to the Sisyphian extreme. Perhaps we need to do what Camus suggested in his essay. We may be required to revolt—with innovation.

Total Malware Samples in the Database

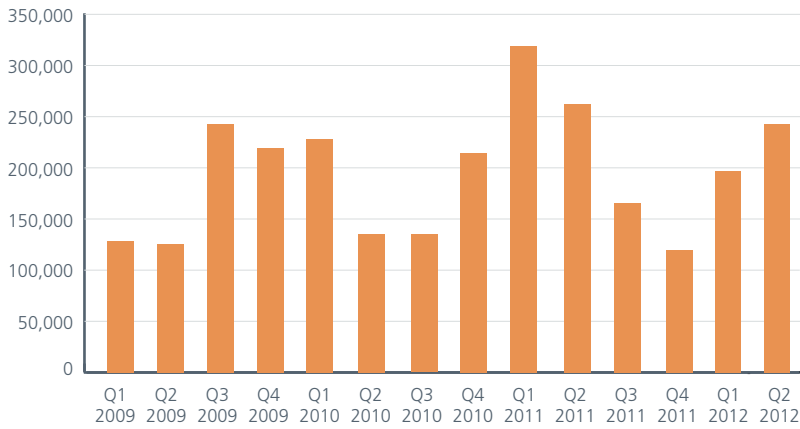


New Malware

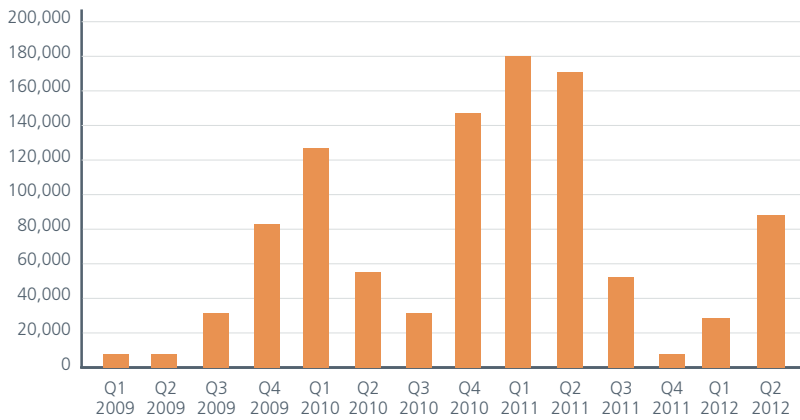


Rootkits rose slightly overall this quarter, with Koutodor showing tremendous growth. ZeroAccess and TDSS declined a bit from last quarter but their influence in other classes of malware can clearly be felt. Rootkits, or stealth malware, are one of the nastiest classifications of malware we see; they have a heavy influence on almost all other areas of malware. They are designed to evade detection and “live” on a system for a prolonged period.

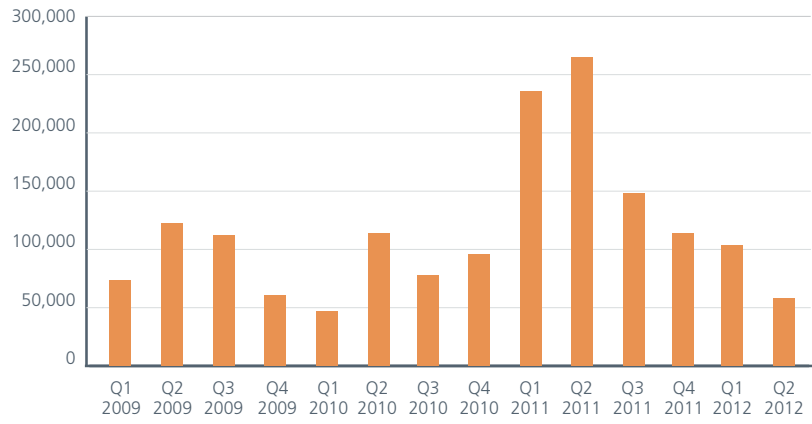
Unique Rootkit Samples Discovered



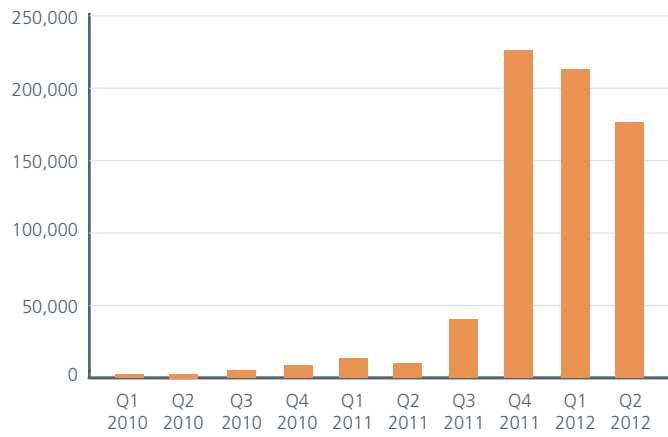
New Koutodor Samples



New TDSS Samples

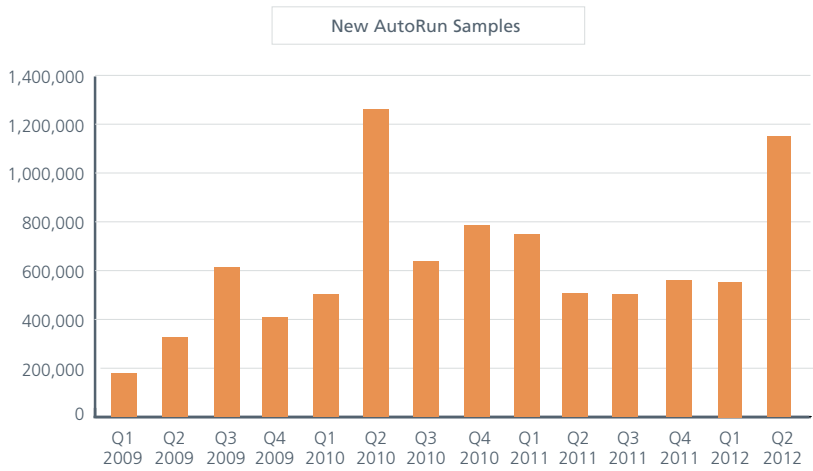
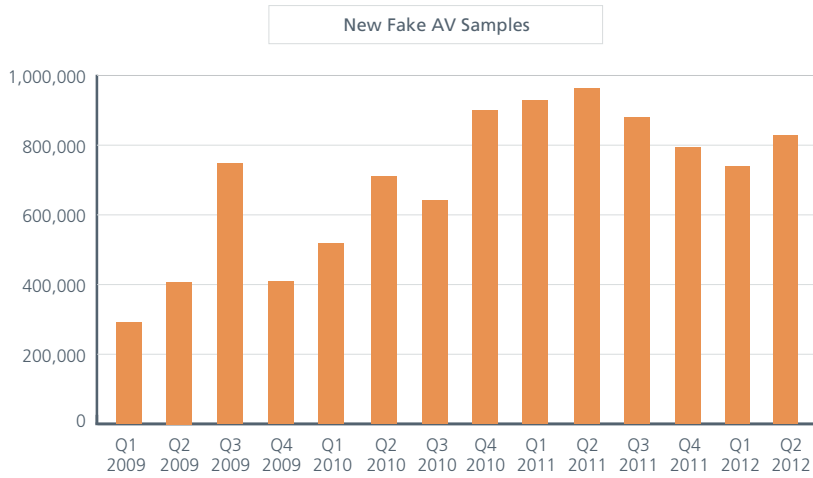


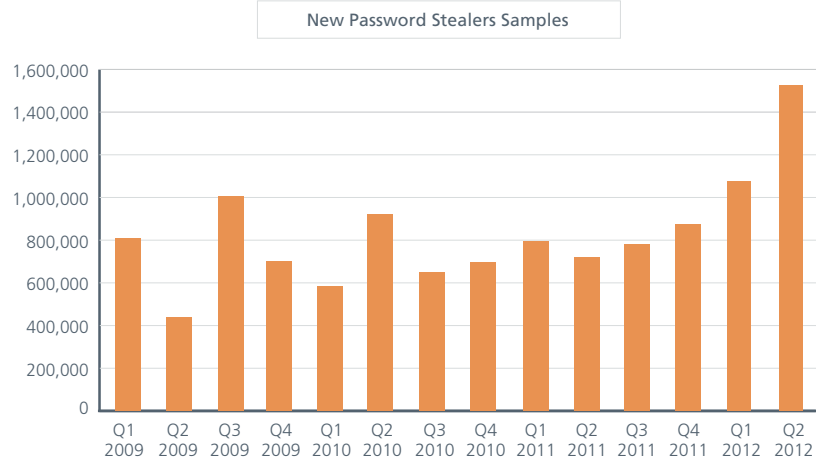
New ZeroAccess Samples





Fake AV (bogus security software), AutoRun, and password-stealing Trojans are still alive and with us. Fake AV actually showed a small amount of growth but the overall trend is still down, while both AutoRun and password-stealing malware showed significant growth this quarter.



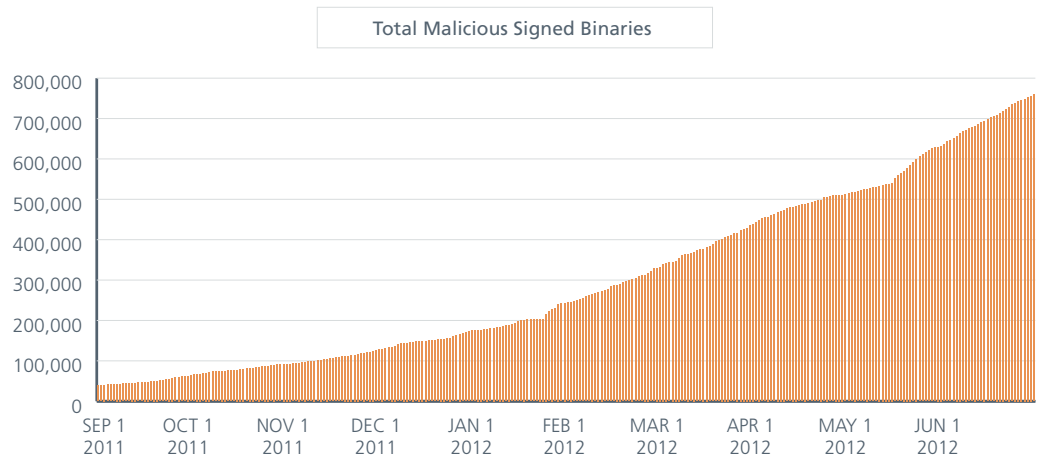


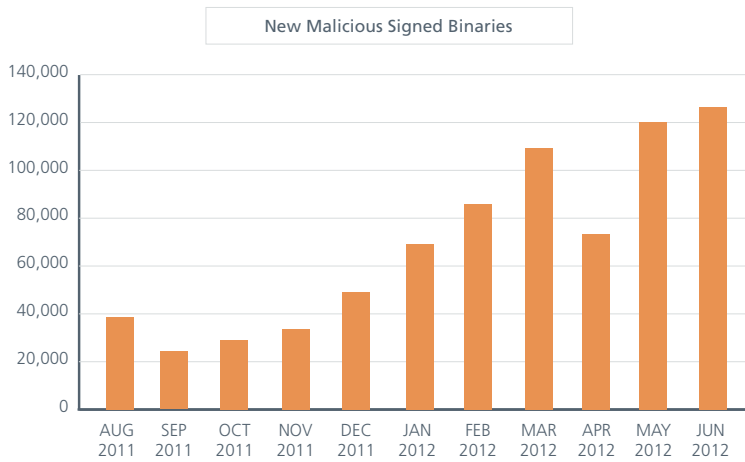
### Signed malware

Because a good blog by McAfee Labs senior researcher Craig Schmugar cannot be shared enough, let us recall why malware writers use digital signatures with their malware:

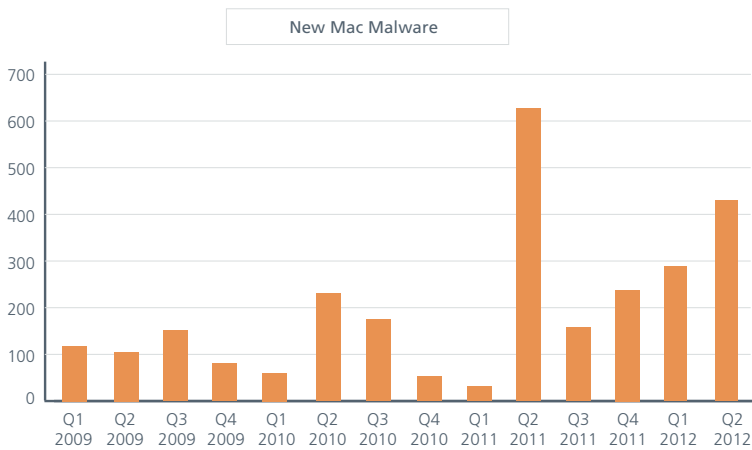
*Attackers sign malware in an attempt to trick users and admins into trusting the file, but also in an effort to evade detection by security software and circumvent system policies. Much of this malware is signed with stolen certificates, while other binaries are self-signed or "test signed." Test signing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

We saw growth in this advanced method of attack during the quarter. In our *2012 Threats Predictions* we predicted that this technique, likely inspired by the success of Duqu and Stuxnet, would rise in 2012.<sup>2</sup> That opinion seems to be a successful example of crystal-ball gazing.

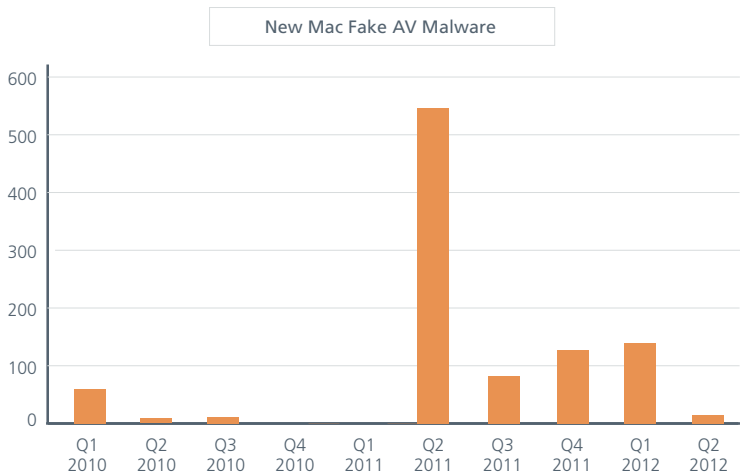




All Mac fanboys and -girls are hereby on notice: Mac malware is showing steady, continued growth. We grant that when compared numerically to Windows malware the numbers are small, but these threats should be taken seriously and Mac users should take precautions. It's simple: Malware can be written for *any* operating system and platform:



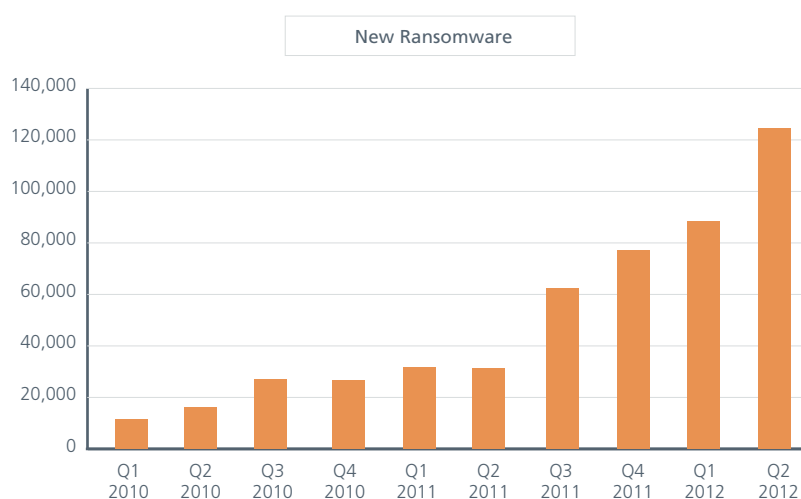
Following a midyear spike in 2011, Fake AV malware for the Mac has significantly declined this quarter:



## Ransomware holds data hostage

The popularity of certain types of malware rises and falls. Fake-alert/fake-AV software has been on the decline since 2011, in total unique samples and the number of machines reporting detections. Declines can come about for several reasons, including both increasing law enforcement efforts as well as cybercriminals finding it more difficult to process victims credit card payments. Unfortunately, cybercriminals do not pack up shop when one business model stops working; they invent other ways to make money. Recently malware developers have turned their attention toward “ransomware.”

Ransomware hold parts or all of a victim’s computer or data hostage. The malware encrypts data or the entire computer and then, using anonymous payment methods, demands money to restore it. The cybercriminal need not find a processor for credit card payments. The rip-off is nothing new. One of the first Trojans seen on the PC, the AIDS-Trojan in 1989, worked exactly this way, but for many years such attacks were rare. Now they have become much more common.



Ransomware has increased during the last several quarters. This quarter we saw ransomware at its busiest ever.

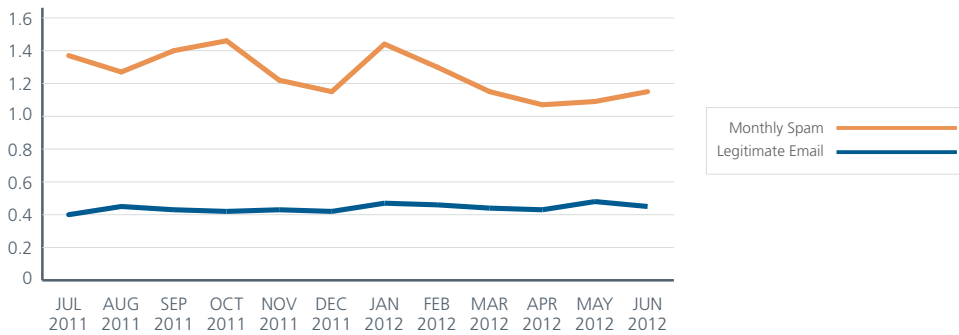
Ransomware is particularly problematic because the damage is instant and commonly a machine is rendered completely unusable. So not only is the victim’s data destroyed, but some of the victim’s money is also gone if he or she attempts to pay the attacker’s ransom. And although it is a personal disaster for a home user to lose years’ worth of data, pictures, and memories, the situation can be much worse in an enterprise if the malware encrypts all the data that a victim has write-access to on a corporate network.

How can we defend ourselves? On top of being really careful with file attachments or links in email and online, back up your systems on a regular basis. Corporate administrators should consider using access-protection rules in their security products to prevent infections.

## Messaging Threats

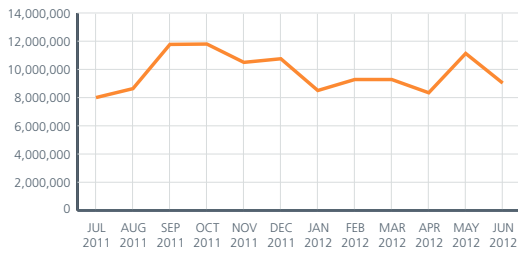
Despite spikes in October 2011 and January 2012, spam levels are still on the decline. We saw a small increase this quarter, but we don’t think it will change the downward trend. In spam rates per country we observed stability in some and decreases in others. Only Colombia, Japan, South Korea, and Venezuela showed an increase in volume of greater than 10 percent. But don’t be fooled: Spam is still dangerous and targeted spearphishing attacks are even more so.

Global Email Volume, in Trillions of Messages

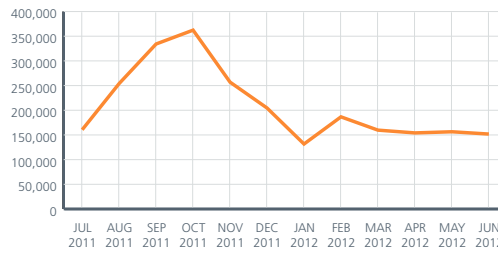


Spam Volume

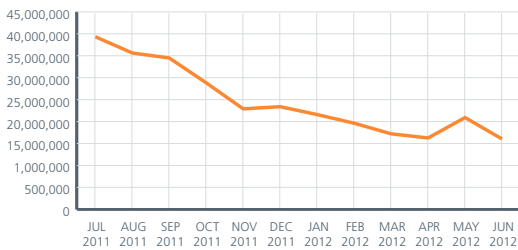
Argentina



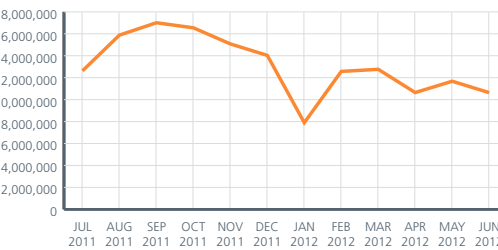
Australia



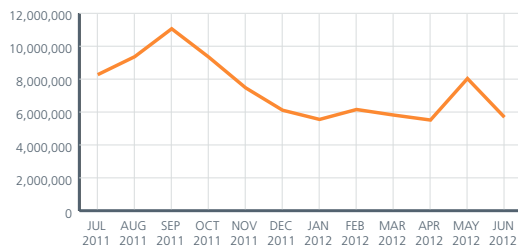
Brazil



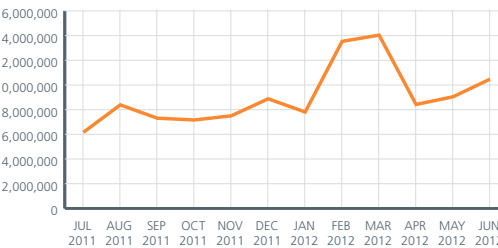
China



Colombia

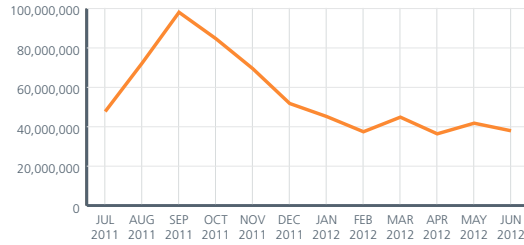


Germany

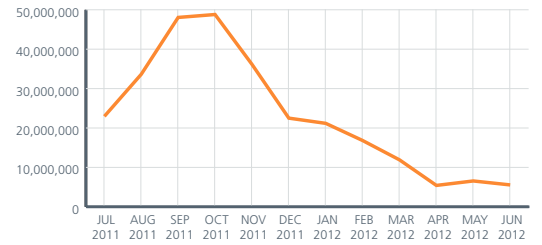


### Spam Volume

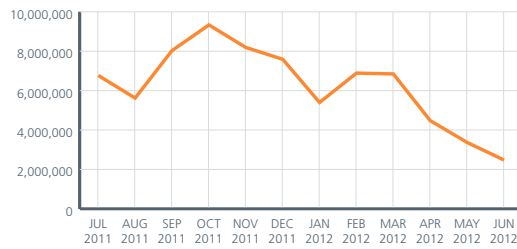
India



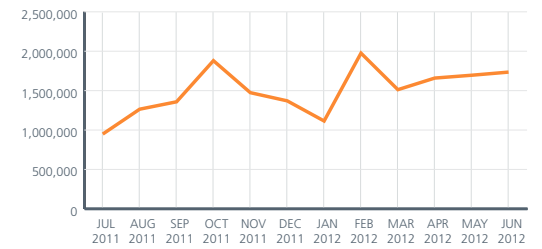
Indonesia



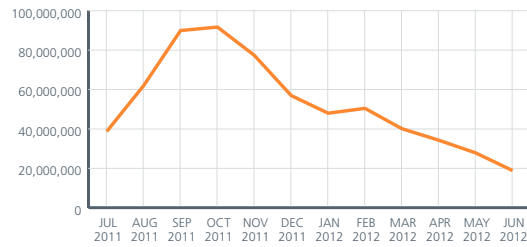
Italy



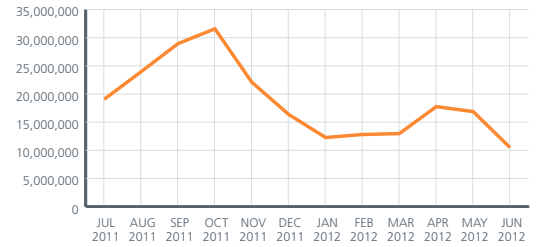
Japan



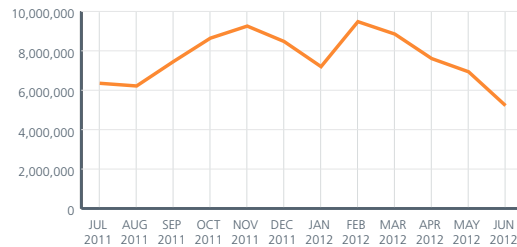
Russia



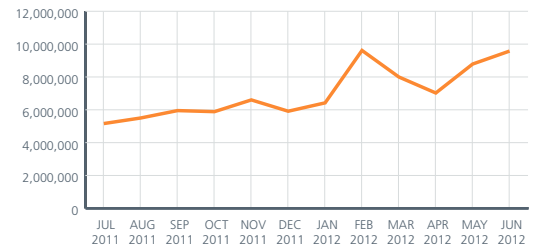
South Korea



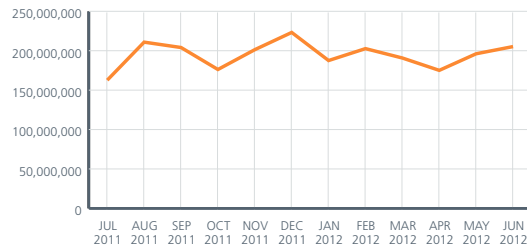
Spain



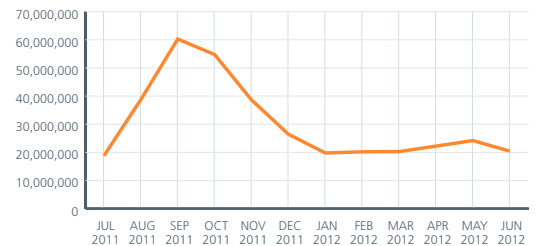
United Kingdom



United States

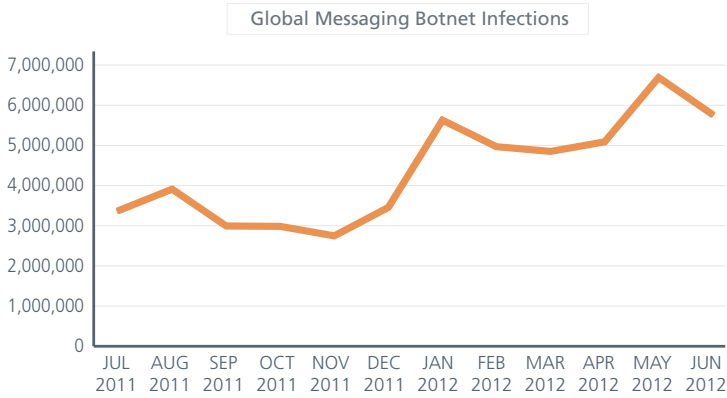


Venezuela

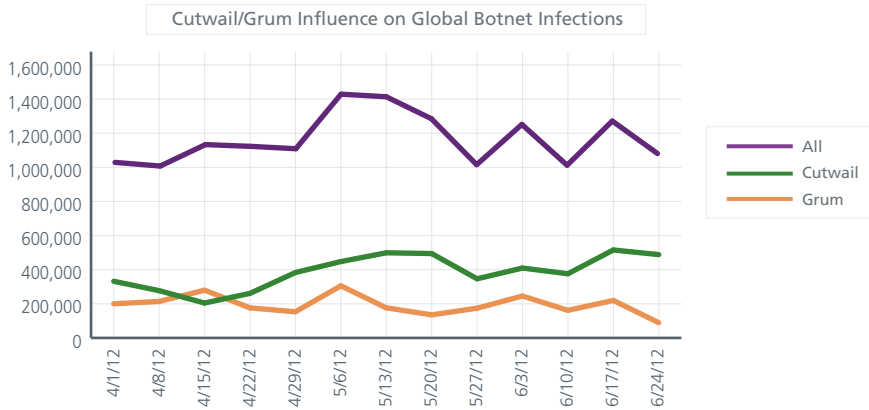


### Botnet Breakdowns

Last quarter we noticed that growth in messaging botnets had flattened. This quarter, however, infections reached a 12-month high. At approximately the same time we saw spikes in the volume of global spam. This correspondence demonstrates the prevalence of botnets in spam activities. It also shows that to maintain spam activity, botnet workloads must increase.

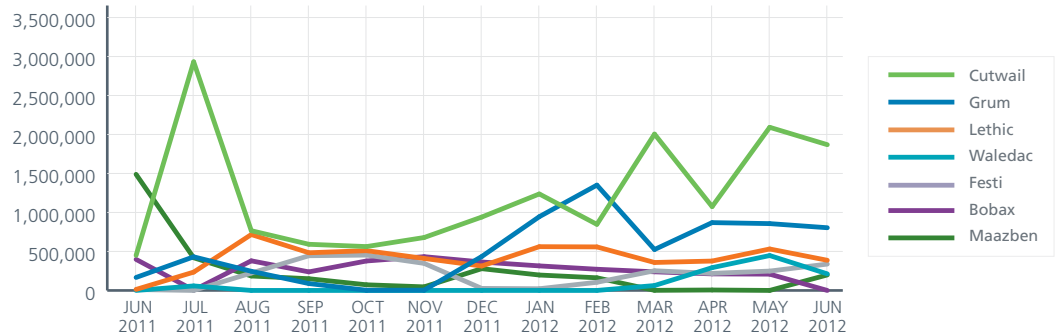


The quarter's spam volume is mostly due to the intense activity of the Cutwail and Grum botnets.



The overall ranking of messaging botnets changed little from last quarter to this one. Grum and Lethic remain numbers 2 and 3, respectively, while Cutwail as usual holds on to the top spot.

Leading Global Botnet Infections



Most of the other leading messaging botnets showed flat growth or even a decline in new infections this quarter. One exception was Bobax, which disappeared in June when Maazben came alive again.

Countries that reported an increase of greater than 10 percent in new botnet senders included China, India, South Korea, and United States. The Koreans suffered the greatest increase, at more than 50 percent.

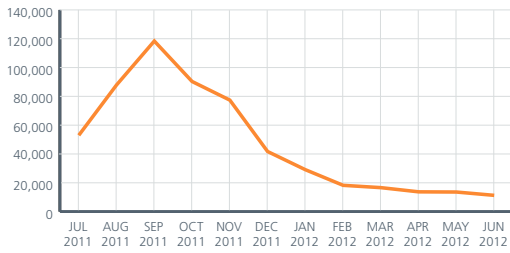
New Botnet Senders



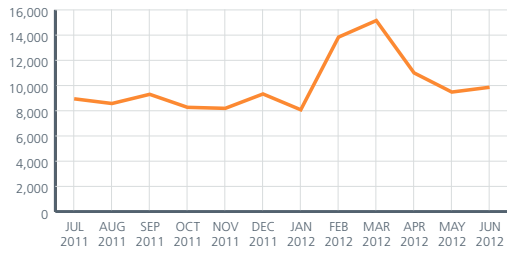


### New Botnet Senders

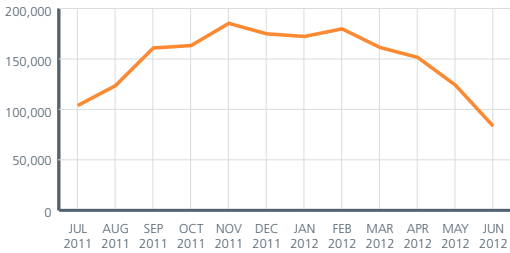
Indonesia



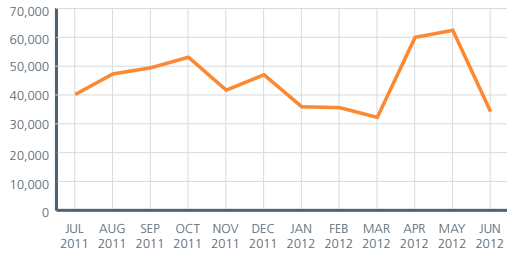
Japan



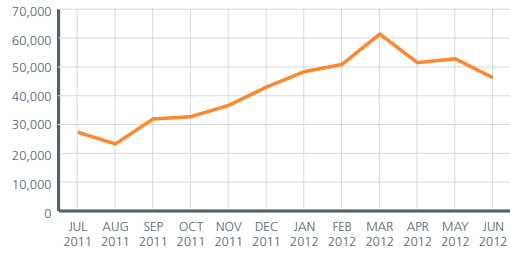
Russia



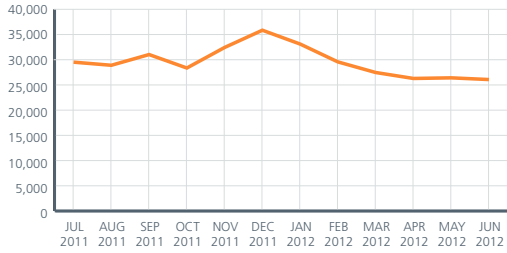
South Korea



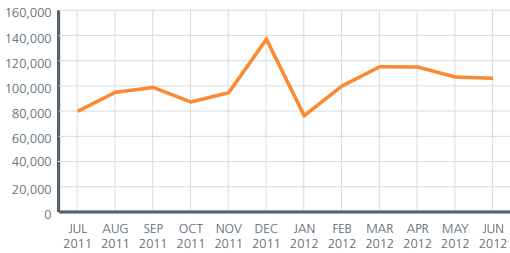
Spain



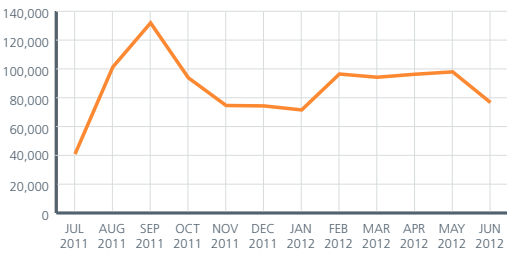
United Kingdom



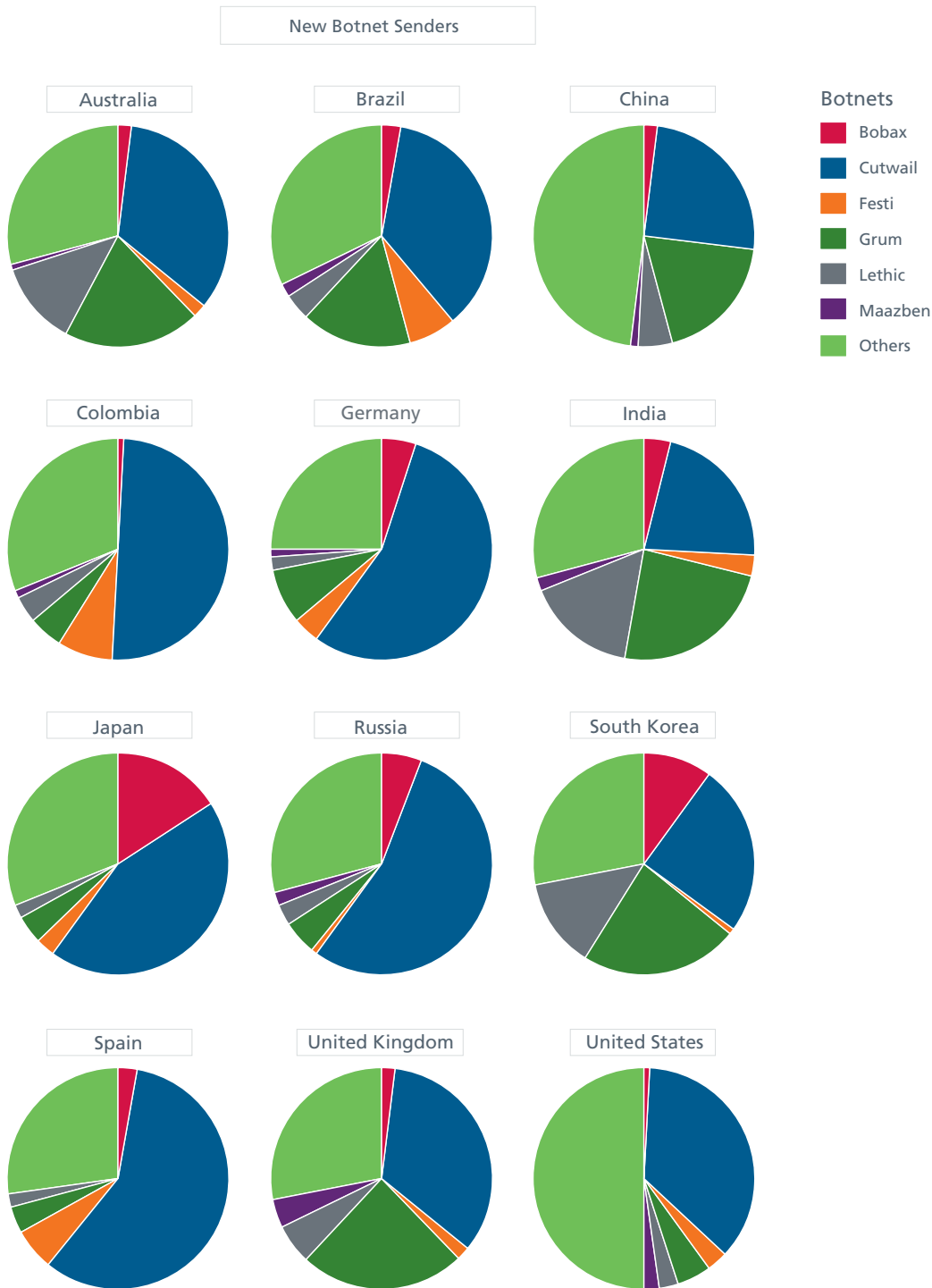
United States



Venezuela



The rate of new infections does not affect the state of current infections. Our breakdown of botnets by country shows that many of these botnets are still quite active around the world, even though the rate of new infections may be on the decline. Cutwail is the global leader in new infections and in current infections except in India, Pakistan, and Venezuela, where Grum is most prevalent.

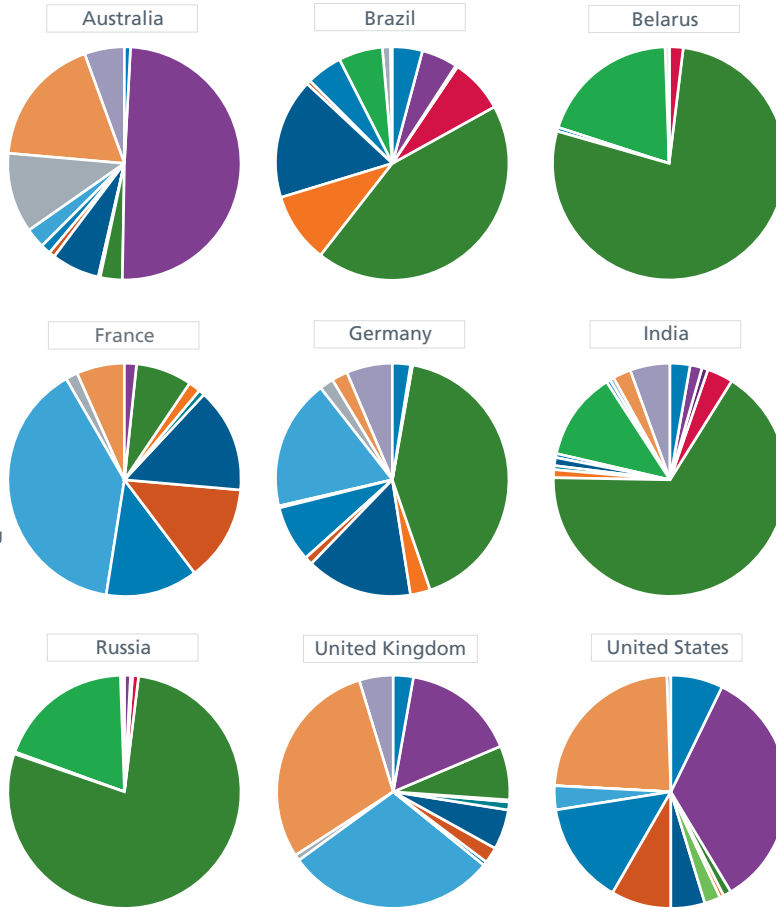


## Spam seeks to deceive via social engineering

Spam subject lines vary greatly depending on the part of the world one is in. Spammers find the effectiveness of social engineering lures differs depending on countries, cultures, religions, and other factors. The world “leader” was delivery status notification (DSN), an old favorite, and drug-related lures were also very popular.

### Spam Types

- 419 Scams
- DSN
- Adult Products
- Casinos
- Drugs
- Jobs
- Lonely Women
- Lottos
- Marketing
- Newsletters
- Phishing
- Replica Products
- Travel
- Unsolicited Advertising
- Viruses
- Webinars



## Network Threats

As we discussed last quarter, we have significantly expanded our network-based analysis. Examining this data shows that attack origination and attribution is a complex business. It is hard to answer the questions “Where did this attack come from?” or “Who is responsible for this attack?” with any certainty. Analyzing code does not often provide insights into who wrote it. Analyzing network attacks for indicators and markers of attribution is equally difficult. We have made a good start toward attribution, but we are only at the beginning stages of concluding who the actors are. Sometimes all we can say is “this is how the code behaves,” “this is what the attack does,” or “this is where we believe it originated.” Anything deeper than that risks Oscar Wilde’s art criticism:

*All art is at once surface and symbol.*

*Those who go beneath the surface do so at their peril.*

*Those who read the symbol do so at their peril.*

*It is the spectator, and not life, that art really mirrors.*

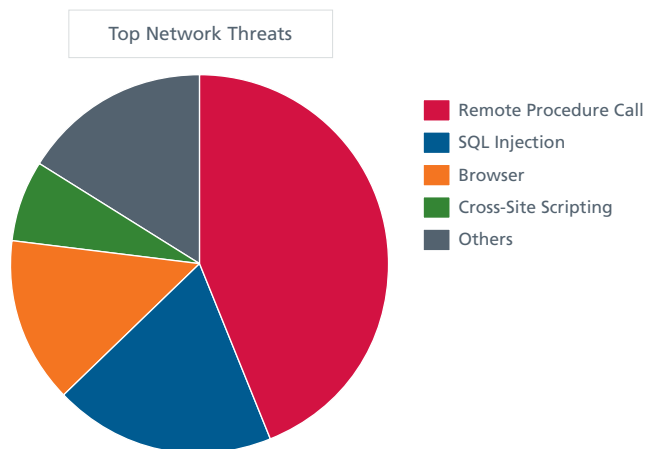
*Diversity of opinion about a work of art shows that the work is new, complex, and vital.*

—From *The Picture of Dorian Gray*

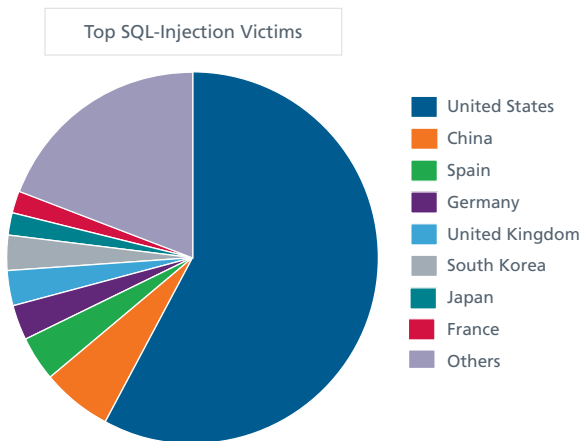
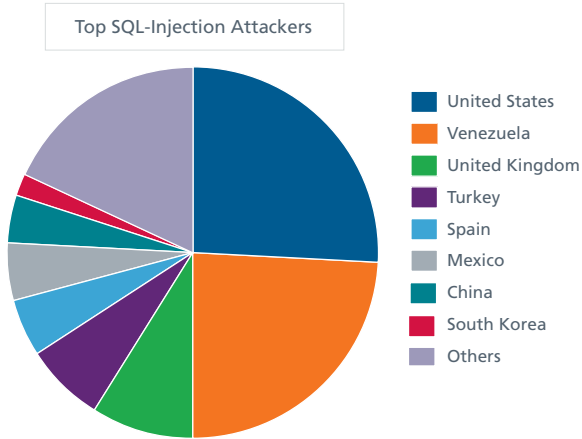
The security world has many diverse opinions on attribution. Most simply reflect the preconceived opinions of the analyst. This diversity shows we are at the very beginning of research into attribution. Sometimes you have to look at the data and just say “It is what it is.”

We can say with confidence that the United States again appears to be the biggest overall source and target of cyberattacks. Let’s dig into a few areas as collected and analyzed by the McAfee Global Threat Intelligence™ network.

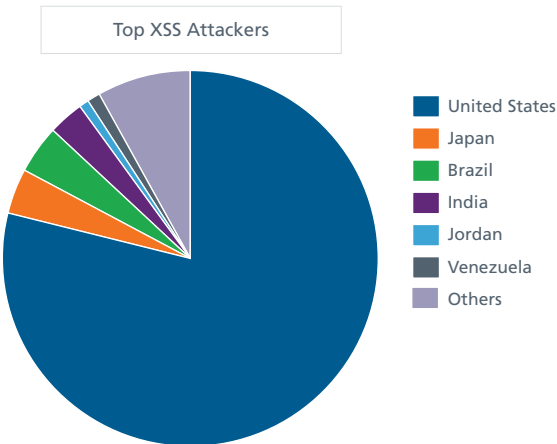
Threats by type are identical in name to last quarter’s, but the pie slices have changed in size due to a greater amount of remote procedure call activity this time. All other areas declined as a result of this shift, but the categories kept their order.



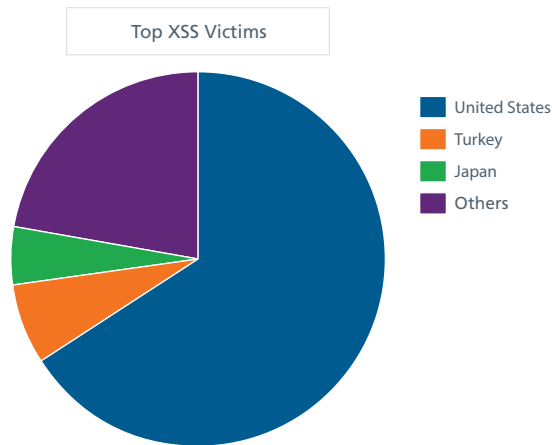
The United States barely edged out Venezuela for the top spot among attackers but **clearly** leads in the victims category.



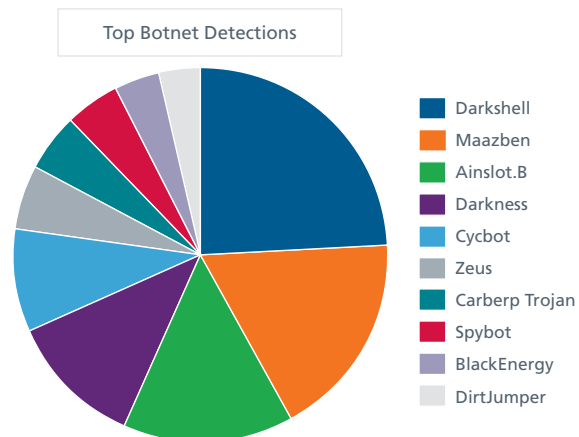
The United States, like last quarter, was by far the most popular origin of cross-site scripting (XSS) attacks.



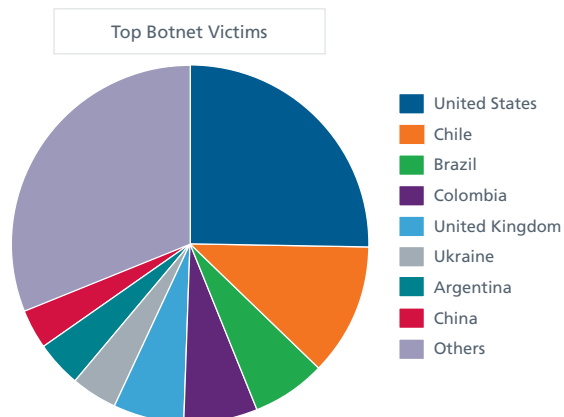
Among XSS victims the United States again topped the list as the biggest target, with Turkey coming in a very distant second.



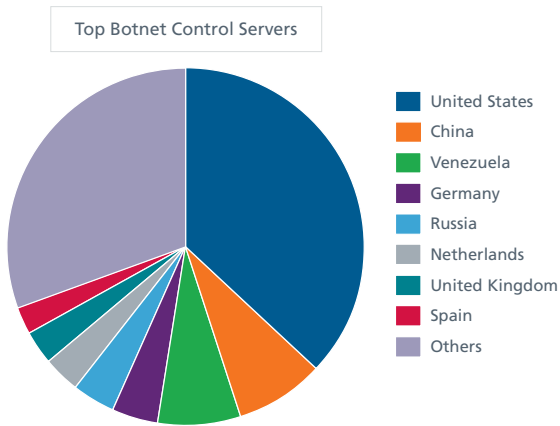
While last quarter we saw the Mariposa and Pushdo (Cutwail) botnets in the top two positions, this time Darkshell and Maazben take those spots.



Among victims, the United States took over the top spot from Venezuela. Chile was a second, with just half as many infections.



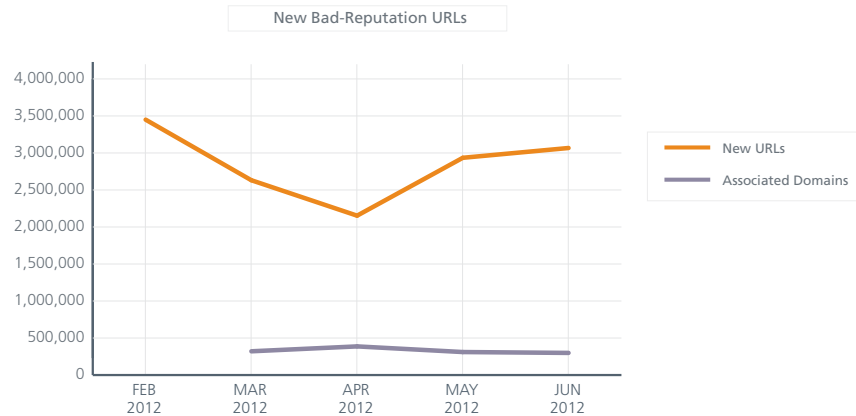
The United States remains number one in hosting botnet control servers, though that figure declined 10 percent this quarter. China and Venezuela were the largest of the remainder.



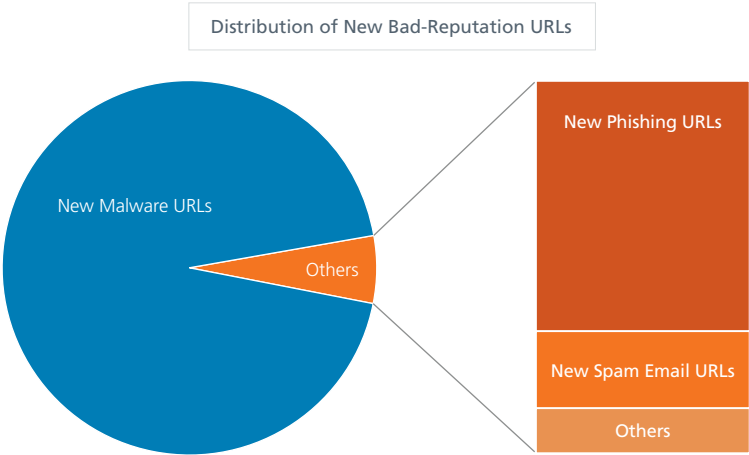
### Web Threats

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

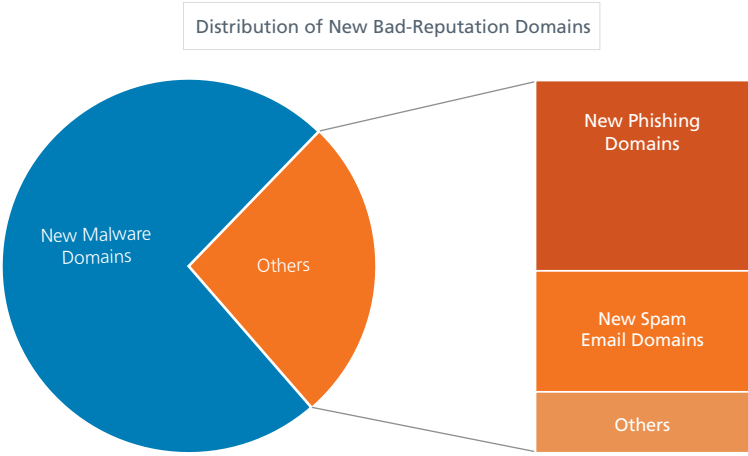
By the end of June, the total number of bad URLs referenced by our labs overtook 36 million! This is equivalent to 22.6 million domain names. This quarter we recorded an average of 2.7 million new bad URLs per month. In June, these new URLs were related to about 300,000 bad domains, which is equivalent to 10,000 new malicious domains every day, up slightly from last quarter. It is interesting to note that this figure is comparable with the 9,500 new malicious websites Google announced in a June blog.<sup>3</sup>



Most (94.2 percent) of these URLs host malware, exploits, or code that have been designed specifically to hijack computers. Phishing and spam represent about 4 percent and 1 percent, respectively.

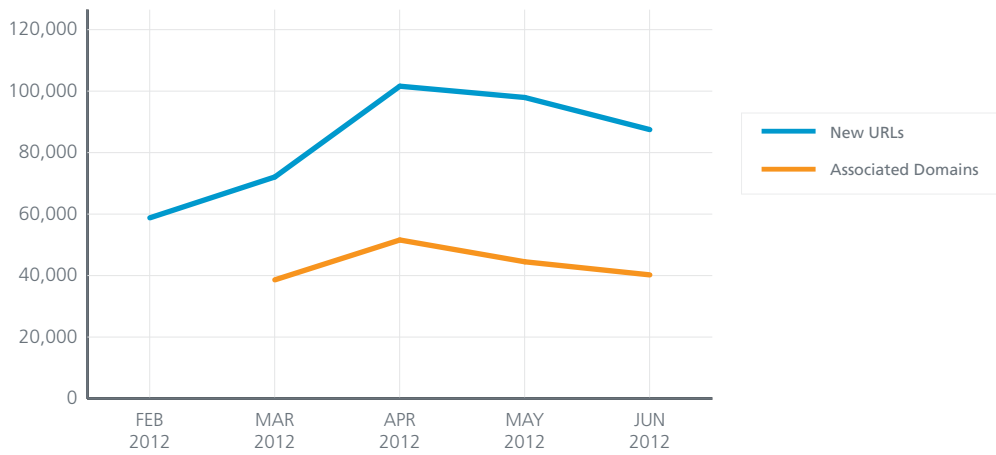


The distribution of domains shows a slightly different breakdown:

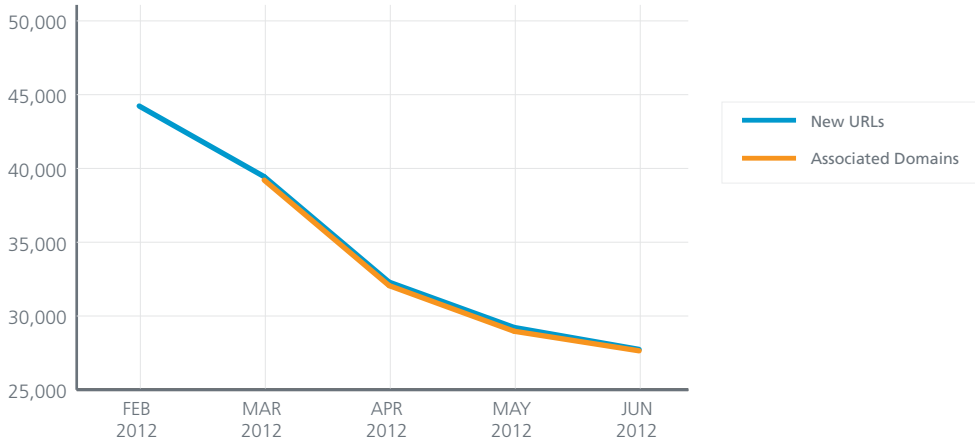




New Phishing URLs

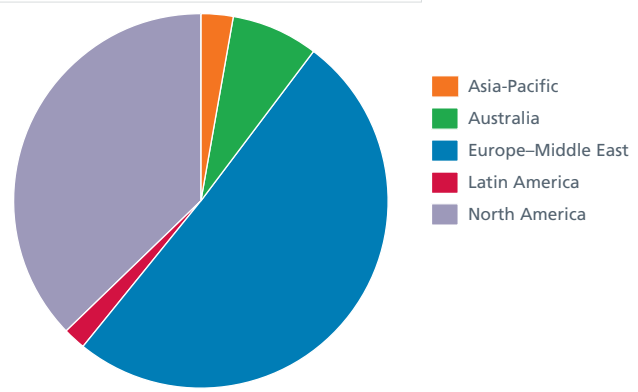


New Spam URLs

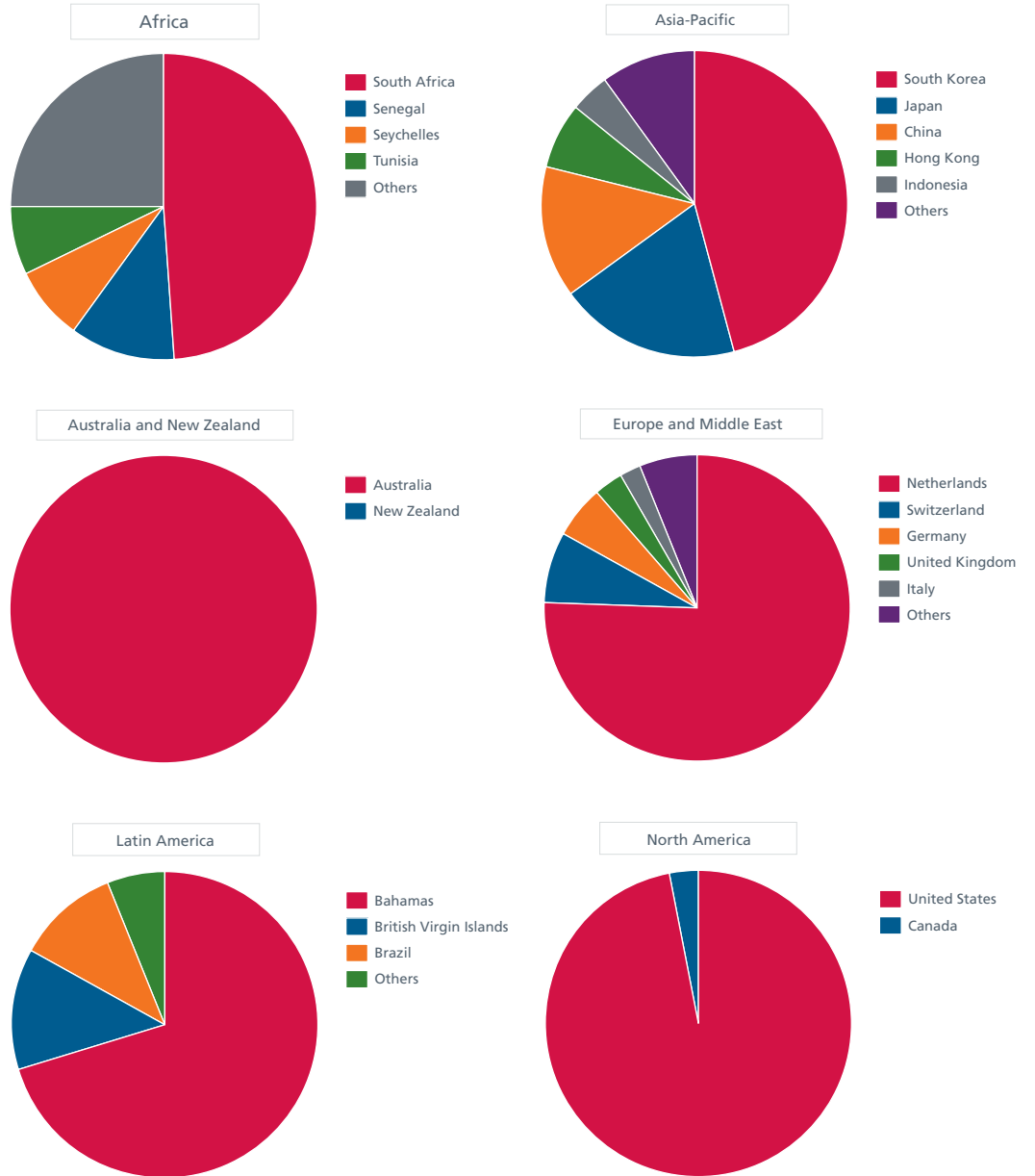


We did see a significant shift in the location of these bad servers during this period. Whereas last quarter almost 92 percent were based in North America, this quarter the biggest piece of the malicious web content pie moved to Europe and the Middle East. As we look deeper into each region we also observe further diversity, with the Netherlands as the chief hosting nation.

Location of Servers Hosting Malicious Content



Location of Servers Hosting Malicious Content

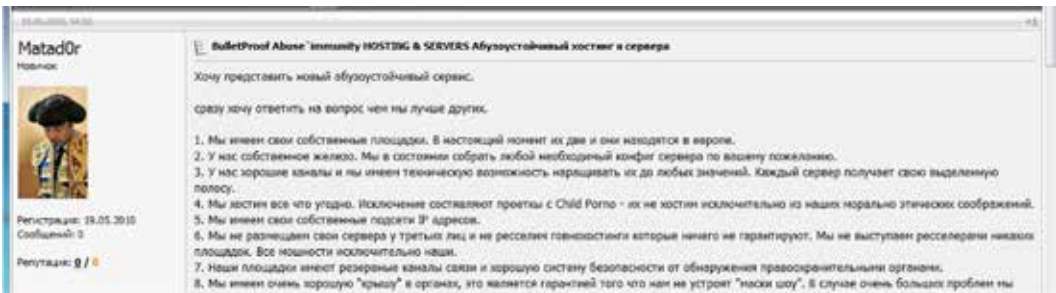


## Cybercrime

### Bulletproof hosting

This quarter, we continue our review of “crimeware as a service” with a look at bulletproof hosting. Last quarter, we highlighted “Operation Open Market,” an effort by the United States Secret Service against 50 individuals who were members, associates, or employees of the criminal organization Carder.su.

One defendant, known as Dorbik and Matad0r, was a vendor of such facilities. In 2010, he discussed his services in variety of specialized forums:



Matad0r's prices:

Hosting	Virtual Private or Dedicated Servers	Dedicated Servers
<ul style="list-style-type: none"> <li>• 2GB on the server</li> <li>• Up to 10 parked domains</li> <li>• Dedicated DNS servers</li> <li>• Hosting control panels</li> <li>• Unlimited traffic</li> <li>• Necessary modules and software for free</li> <li>• US\$50 per month</li> </ul>	<ul style="list-style-type: none"> <li>• VMware technology</li> <li>• Full root access to servers</li> <li>• Up to 25% of Xeon CPU</li> <li>• From 1GB RAM</li> <li>• From 30GB storage</li> <li>• Unlimited traffic</li> <li>• Free setup/re-setup</li> <li>• Full software set</li> <li>• Additional IP addresses if necessary</li> <li>• US\$150 per month</li> </ul>	<ul style="list-style-type: none"> <li>• Different configurations</li> <li>• 24-hour setup</li> <li>• Unlimited traffic</li> <li>• Free setup/re-setup</li> <li>• Any OS (including Windows) for free</li> <li>• Additional IP addresses if necessary</li> <li>• US\$400 per month</li> </ul>

Today, offers like these are numerous on the Internet, and there is no doubt who the customers are. The following examples are in Russian:



Заказать	Заказать	Заказать	
----------	----------	----------	--

**Дополнительные услуги:**

- Доп. 1 IP-адрес: (3\$ - Ежемесячно)
- Услуги администрирования вне регламента тех. подд

**Панели управления:**

- ISPmanager Lite: (5ye - Ежемесячно)
- ISPmanager Lite: (25ye - Вечная)
- ISPmanager Pro: (9ye - Ежемесячно)
- ISPmanager Pro: (47ye - Вечная)

**Разрешено:**

- Торрент трекеры
- Хитмер
- Фишинг
- Фейки
- Фарма
- Любые злоупотребления/abuse

**Запрещено:**

- Детское порно
- Зоофильное порно
- Фашизм
- Разжигание межнациональной розни
- Спам (SMTP)

**Allowed**

- Torrent
- Xrumer (spam)
- Phishing
- Fakes
- Pharma
- Abuse

**Forbidden**

- Child porn
- Zoophile porn
- Fascism
- Incitement of ethnic hatred
- Spam (SMTP)

In the next offer we can see loss-leader prices for dedicated servers (at top) and for virtual private/dedicated servers.

Dedicated Servers			
<p>AMD Athlon 64 3200+ @ 2.2 GHz            Ram: 1 GB            HDD: 2x 160 GB            IP: 1 pcc.            Traffic: Unlimited</p> <p><b>Germany</b></p> <p>Price: 70\$</p>	<p>AMD Athlon 3400 @ 1.8 GHz            Ram: 2 GB            HDD: 320 GB            IP: 1 pcc.            Traffic: Unlimited</p> <p><b>Romania</b></p> <p>Price: 60\$</p>	<p>Pentium G640 2x 2.8 GHz            Ram: 4 GB            HDD: 60 GB (SSD)            IP: 1 pcc.            Traffic: 3 TB</p> <p><b>Poland</b></p> <p>Price: 90\$</p>	<p>Intel Pentium Dual Core 2.5 GHz            Ram: 2 GB            HDD: 300 GB            IP: 2 pcc.            Traffic: Unlimited</p> <p><b>Malaysia</b></p> <p>Price: 130\$</p>
VPS/Clouds			
<p>Amm: 512 MB            HDD: 10 GB            IP: 1 pcc.            Traffic: Unlimited</p> <p><b>Czech Republic</b></p> <p>Price: 20\$</p>	<p>Amm: 512 MB            HDD: 20 GB            IP: 1 pcc.            Traffic: Unlimited</p> <p><b>Germany</b></p> <p>Price: 25\$</p>	<p>Amm: 512 MB            HDD: 20 GB            IP: 1 pcc.            Traffic: Unlimited</p> <p><b>USA</b></p> <p>Price: 25\$</p>	<p>Amm: 512 MB            HDD: 20 GB            IP: 1 pcc.            Traffic: Unlimited</p> <p><b>Russia</b></p> <p>Price: 21\$</p>

Сервера под спам и серый контент:

- Turkey - любой контент.
- France - любой контент.
- Germany - Любой контент.
- Russia - Серые и белые проекты, детская порнография.

The Russian comments say:

For spam and gray designs

~ Turkey ~

Allowed: Any content.

~ France ~

Allowed: Any content.

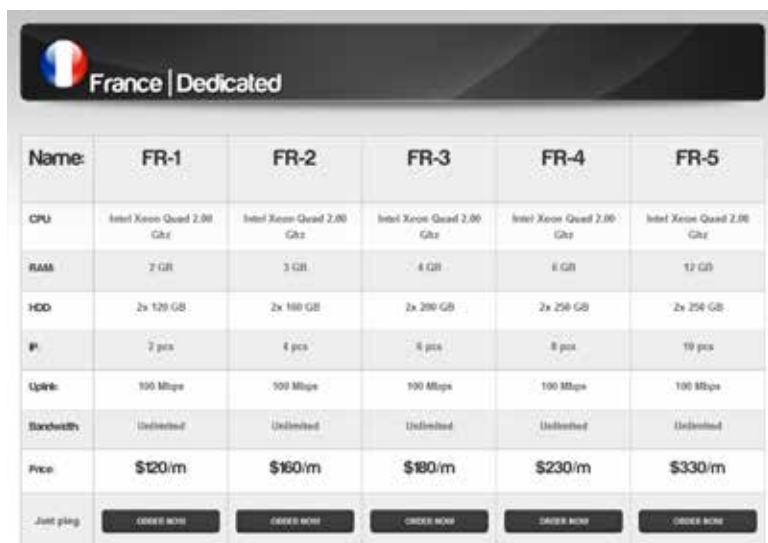
~ Germany ~

Allowed: Any content.

~ Romania ~

Allowed: Gray and white projects. Prohibited: child pornography.

When we browse the website linked to this shop, we find many other offers. Here is an example targeted at French customers:



Name	FR-1	FR-2	FR-3	FR-4	FR-5
CPU	Intel Xeon Quad 2.00 GHz	Intel Xeon Quad 2.00 GHz	Intel Xeon Quad 2.00 GHz	Intel Xeon Quad 2.00 GHz	Intel Xeon Quad 2.00 GHz
RAM	7 GB	3 GB	4 GB	6 GB	12 GB
HDD	2x 120 GB	2x 160 GB	2x 200 GB	2x 250 GB	2x 250 GB
IP	7 pcs	4 pcs	4 pcs	8 pcs	10 pcs
Uplink	100 Mbps	500 Mbps	100 Mbps	100 Mbps	100 Mbps
Bandwidth	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Price	\$120/m	\$160/m	\$180/m	\$230/m	\$330/m
Just plug	ORDER NOW	ORDER NOW	ORDER NOW	ORDER NOW	ORDER NOW



The means of payment visible on this screenshot speak for themselves.

### Actions against cybercriminals

Several police actions this quarter have been successful:

- Eight suspects in the United States and elsewhere were arrested and indicted for their involvement in an online drug market accessible only through the Tor anonymizing network. The suspects ran a website called The Farmer's Market, which offered LSD, ecstasy, marijuana, and other drugs for sale. Between January 2007 and October 2009 they processed about 5,256 online orders to some 3,000 customers in 34 countries for a value at more than US\$1 million.<sup>4</sup> Before moving to Tor in 2010, The Farmer's Market processed orders through Hushmail, an encrypted email service.
- On April 26, the Serious Organised Crime Agency (SOCA) in the United Kingdom announced the completion of a joint operation with the (U.S.) Federal Bureau of Investigation and U.S. Department of Justice, targeting 36 criminal websites dealing with stolen credit card and online bank account information.<sup>5</sup> These sites used ecommerce platforms known as Automated Vending Carts (AVCs) to allow criminals to quickly and easily sell large quantities of stolen data.
- On May 3 a U.S. attorney in New Jersey announced that several men, arrested in December 2011, admitted their roles in an Internet fraud ring that stole more than US\$1.3 million after phishing confidential account information from Internet users. Creating fake drivers licenses made with photos of money mules, they impersonated real customers to make unauthorized withdrawals from victims' accounts.<sup>6</sup>

- In May, police in Canadian province Québec arrested 45 people from an international fraud ring active in Britain, Australia, New Zealand, Malaysia, and Tunisia. The authorities seized more than 12,000 counterfeit bank cards. It is said the fraud ring drained some US\$100 million from the accounts of unsuspecting bank card holders. Fraudsters specialized in filming and modifying ATM machines, tried to steal PIN numbers or hack into computer terminals in stores, or forged counterfeit cards for illegal withdrawals. In some cases, they modified point-of-sale machines from businesses and restaurants, rigging them using Bluetooth technology to read the credit and debit card information contained on the computer.<sup>7</sup>
- In June, another Carberp group was neutralized by Russian law enforcement agents. Nicknamed The Hodprot Group (the name of a malware they previously used), it had been active for more than four years while engaged in the theft of funds from online banking systems via the use of banking malware. The group's activity yielded damages of over 125 million rubles (approximately US\$3.7 million) from the online banking customers.<sup>8</sup>
- The United Kingdom's SOCA announced that two fraudsters, known by their online pseudonyms as tOpp8uzz and GM, have been sentenced to jail after investigators accused them of running a fraud website worth an estimated £26.9 million (US\$41 million or €33.2 million). Arrested in 2011, they managed Freshshop, a site that resold stolen financial information.<sup>9</sup>
- Federal authorities arrested 24 people in the United States and a dozen other countries in what they say is the largest-ever undercover operation targeting the global online trade of stolen credit card numbers. This operation started in June 2010 when the FBI established an undercover forum called Carder Profit, enabling the agents to monitor carding activity. During the course of the operation the FBI supplied credit card providers with details on 411,000 compromised cards, leading to an estimated savings of US\$205 million in unrealized card fraud.<sup>10</sup> Among those arrested was the leader of UGNazi, a hacking group that has claimed responsibility for a flood of recent attacks on Twitter and Google.

### Hactivism

Several arrests were made of hactivists this quarter:

- In April, we learned of the arrest of the CabinCr3w members, a hacker group affiliated with Anonymous. Kahuna and w0rmer were suspected of hacking various police department– or law enforcement–related websites in February.<sup>11</sup>
- Half-hactivist, half-cyberarmy, the TeaMp0isoN group again got its name in the papers. On April 11, it launched a 24-hour phone-based denial-of-service (DoS) attack against the United Kingdom's foreign intelligence organization, MI6. The day after, TriCk, a possible leader of the group, called the MI6 offices in London to claim the attack and make fun of them. He explained it was prompted by a recent decision by the European Court of Human Rights that allowed U.K.-linked terror suspects to be extradited to America.<sup>12</sup> Undoubtedly too confident, TriCk, 17, was arrested by Scotland Yard two days later.<sup>13</sup> This capture seemed to portend the end of the group. By May TeaMp0isoN members MLT, also 17, and Phantom, 28, were arrested in the United Kingdom and Russia, respectively.
- Although little covered by the media, suspected Anonymous members were also arrested in June in France, Belgium, and Québec.

The Anonymous movement seems to be in flux. The number of operations may still be high but, with a few exceptions, their impact and consequences appear to have declined. But it would be premature to say the movement is finished. Anonymous highlights of the quarter:

- In April as part as Operation Defense, Anonymous launched DDoS attacks against several U.S. government and industrial interests known for supporting the Cyber Intelligence Sharing and Protection Act.<sup>14</sup>

- In May, Anonymous launched Operation Québec in reaction to the adoption of Bill 78 by the Canadian government. The act limited student protests.<sup>15</sup> As part of its campaign, the group hacked the Montreal Formula One race and posted names, phone numbers, and email addresses of individuals who bought tickets for the race. Ten or so government and police websites in Québec were pulled down, including websites for the public safety ministry, the Liberal Party, the coroner's office, and the police ethics commission.
- In June, Anonymous launched #Oplndia, which criticized growing government censorship of the Internet and particularly the recent court ban on sites such as Torrent and Vimeo. On June 9, Indian Internet activists, heeding the call of Anonymous, held protests in several Indian cities. The turnout was low, but young activists wearing Anonymous masks demonstrated in 16 cities including Mumbai, Pune, and Bangalore. Anonymous also attacked the websites of cert-in.org.in and india.gov.in. These were down most of the day.<sup>16</sup>
- In Japan, a new amendment establishing extremely severe penalties for people downloading pirated material such as DVDs and Blu-Ray discs was added to copyright laws. In response, several posts invoked the #OpJapan tag while attacking various Japanese targets.<sup>17</sup>

A favorite Anonymous target remains police forces around the world:

- In April as part of the F\*\*K FBI Friday initiative, hackers from Anonymous attacked the Lake County, Florida, Sheriff's Office website. They also defaced the International Police Association site.<sup>18</sup>
- In Québec, Anonymous supporters stole and published data from the SPVM (Montreal Police Service) website, including thousands of usernames, names, emails, addresses, and other personal information.<sup>19</sup> As part of opQuebec, they also targeted the Desjardins Credit Union police site. The usual welcome page was replaced with a simple black template with links to Anonymous resources. The names and emails of what appear to be the bank's clients and employees were also displayed.<sup>20</sup>

#### About the Authors

This report was prepared and written by Zheng Bu, Toralv Dirro, Paula Greve, Yichong Lin, David Marcus, François Paget, Vadim Pogulievsky, Craig Schmugar, Jimmy Shah, Dan Sommer, Peter Szor, and Adam Wosotowsky of McAfee Labs.

#### About McAfee Labs

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

#### About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on finding new ways to keep our customers safe. [www.mcafee.com](http://www.mcafee.com)



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

- <sup>1</sup> <http://blogs.mcafee.com/mcafee-labs/signed-malware-you-can-runbut-you-cant-hide>
- <sup>2</sup> <http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf>
- <sup>3</sup> <http://googleonlinesecurity.blogspot.co.uk/2012/06/safe-browsing-protecting-web-users-for.html>
- <sup>4</sup> <http://www.wired.com/threatlevel/2012/04/online-drug-market-takedown/>
- <sup>5</sup> <http://www.soca.gov.uk/news/446-web-domains-seized-in-international-operation-to-target-online-fraudsters>
- <sup>6</sup> <http://www.ahherald.com/newsbrief-mainmenu-2/law-and-order/13094-man-admits-role-in-13-million-phishing-fraud-scheme>
- <sup>7</sup> <http://www.cbc.ca/news/canada/montreal/story/2012/05/09/international-fraud-ring-montreal.html>
- <sup>8</sup> <http://www.group-ib.com/index.php/7-novosti/633-group-ib-aided-russian-law-enforcement-agents-in-arresting-yet-another-cybercriminal-group%22>
- <sup>9</sup> <http://www.infosecurity-magazine.com/view/26219/soca-announces-jailing-of-two-uk-credit-card-crooks/>
- <sup>10</sup> <http://www.infosecurity-magazine.com/view/26608/fbi-arrests-was-ughazi-a-target-or-an-instrument/>
- <sup>11</sup> <http://blogs.mcafee.com/mcafee-labs/hacker-leaves-online-trail-loses-anonymity>
- <sup>12</sup> <http://news.softpedia.com/news/TeaMp0isoN-Phone-Bombs-UK-Foreign-Intelligence-Agency-MI6-264125.shtml>
- <sup>13</sup> <http://news.softpedia.com/news/TeaMp0isoN-Confirm-TriCk-s-Arrest-Operation-Retaliatio-Starts-264663.shtml>
- <sup>14</sup> <http://www.securityweek.com/anonymous-launches-attacks-against-trade-associations-and-boeing>
- <sup>15</sup> [http://www.msnbc.msn.com/id/47620087/ns/technology\\_and\\_science-security/t/anonymous-threatens-montreal-grand-prix-over-anti-protest-law/#.T-r5\\_8XnNhw](http://www.msnbc.msn.com/id/47620087/ns/technology_and_science-security/t/anonymous-threatens-montreal-grand-prix-over-anti-protest-law/#.T-r5_8XnNhw)
- <sup>16</sup> <http://globalvoicesonline.org/2012/06/09/india-netizens-respond-to-anonymous-indias-protests/>
- <sup>17</sup> <http://securityaffairs.co/wordpress/6829/hacking/opjapan-anonymous-against-japan-and-its-war-to-piracy.html>
- <sup>18</sup> <http://news.softpedia.com/news/AntiSec-Hackers-Leak-40-GB-of-Data-from-Lake-County-Sheriff-s-Office-266784.shtml>
- <sup>19</sup> <http://www.cyberwarnews.info/2012/06/02/canadian-police-server-hacked-lots-of-personal-information-leaked-by-anonymous/>
- <sup>20</sup> <http://www.canada.com/health/Police+credit+union+site+hacked+Anonymous/6765994/story.html>

McAfee, the McAfee logo, and McAfee Global Threat Intelligence are registered trademarks or trademarks of McAfee or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2012 McAfee  
48400rpt\_quarterly-threat-q2\_0812\_fnl\_ETMG