Report

McAfee Threats Report: Fourth Quarter 2012

By McAfee Labs

Table of Contents

As McAfee Labs analyzed threats during the fourth quarter of 2012, we saw a number of familiar trends: terrifically rapid growth in mobile malware and a steady increase in general malware, including fake antivirus and signed malware. Spam rose at first but then returned to the level that it began the quarter. New botnet infections followed a similar path, with growth in October that eventually cooled, resulting in an end point that was lower than the prior quarter's.

Narrowly targeted attacks continue. Our on-going analysis of Operation High Roller and Project Blitzkrieg shows that cybercriminals can be patient when playing for high stakes. Our count of mobile malware samples has surpassed 36,000, with almost all of it aimed at the Android OS and having arrived in the past year. Spyware, exploits, and backdoor Trojans highlighted this quarter's assaults on mobile phones.

Our analysis of web threats found that the number of new suspicious URLs increased by 70 percent this quarter. Most of those servers are, as you may have guessed, in the United States. Most phishing attacks aim for financial targets, but we saw a rise in those against online auctions and multiplayer online gaming.

The number of new rootkits declined this quarter. That's a welcome change from prior quarters, but is this just a hiccup in a growing trend? AutoRun malware, fake AV "security" software, and signed malware (for targeted attacks) rose steeply during the quarter.

Malware that attacks deeper in a system, at the master boot record, climbed for the second straight quarter. These threats can remain on a system for a long time without the victim's knowledge and download other forms of malware. We expect to see further growth in attacks on the system stack.

New ransomware samples declined slightly this quarter, but the overall number is very high. Cybercriminals hold a system hostage and insist on payment to unlock a computer. But will they free the machine after you pay? There are no guarantees, and anonymous payment systems make it basically impossible to track their movements.

The McAfee Global Threat Intelligence™ network tells us that IP addresses in the United States are again both the source and the target of most malicious network activity. Browser and remote procedure call attacks are the most frequent.

Publicly reported database breaches were modest compared with last quarter, but the year was up about 20 percent over 2011. Oracle products suffered from more vulnerabilities than other leading databases.

Spam and new botnet infections continued their downward trend, though both rose in October. They're now at their lowest levels in more than a year.

In looking into cybercrime this quarter, we saw several sites offering fake IDs and other papers, including passports, for sale. Of course, these are only "souvenir" documents, not for real use. (That should mollify the authorities.) However, we also read of buyers who complained of being ripped off after paying for false papers that didn't arrive. After all, whom can you complain to when the sale goes bad?

We also update the most popular crimeware tools of the quarter, and highlight successes in law enforcement efforts to arrest crooks and break up cybercrime rings. Anonymous was in the news again, with varied success, as the group appears to be at a crossroads. Will it maintain its focus, or break into smaller groups with a smaller impact? We also look at a group that promotes terrorist actions and offer training and other resources online.

Operation High Roller Expands

Operation High Roller was a big story last year and we thoroughly analyzed the threat and its components in two papers.[1] This quarter we saw a shift in fraudulent activity using SpyEye and Zeus, which are typically used to steal money from bank accounts. Although active development of SpyEye has ceased, some groups still use this malware to target financial institutions. We continue to actively monitor further developments in the cybercrime underground.

This quarter we observed some notable activity:

- Automated transfer system (ATS) code has been deployed to target Europe's SEPA payment channel. We observed in November a specialized attack developed using SpyEye against a couple of German banks using an ATS in attempts to steal €61,000.
- Activity has expanded outside of the typical target countries to now pursue users in the Asia-Pacific region. The attack we observed targeted commercial accounts of customers who banked in Singapore.

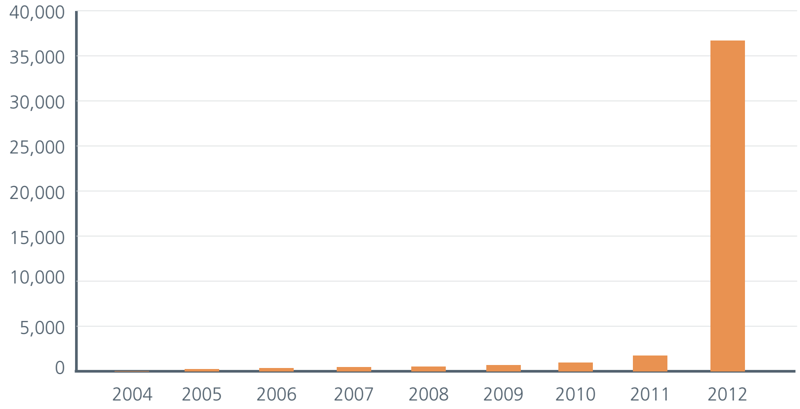
Project Blitzkrieg

Project Blitzkrieg, which we have also analyzed in a separate paper, is a current attack on US financial institutions.[2] The operation is run by a Russian and uses malware from the Gozi family called Prinimalka. If the impact of Project Blitzkrieg matches the claims of its author, the financial industry needs to be prepared. This mass fraud campaign planned against 30 US banks is supposed to occur by spring 2013, and was announced in September 2012. Our investigation shows the threat is real and that the Trojan has been in action as early as 2008 and as recently as October 2012.

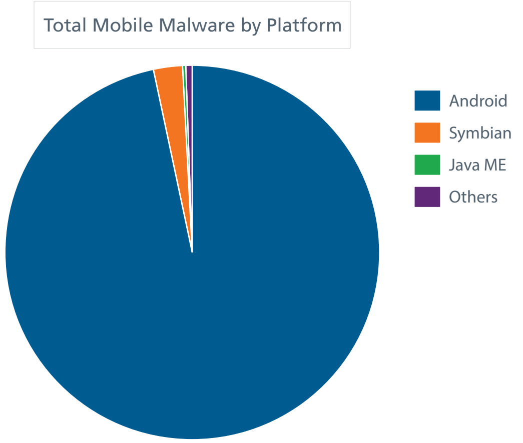
Mobile Threats

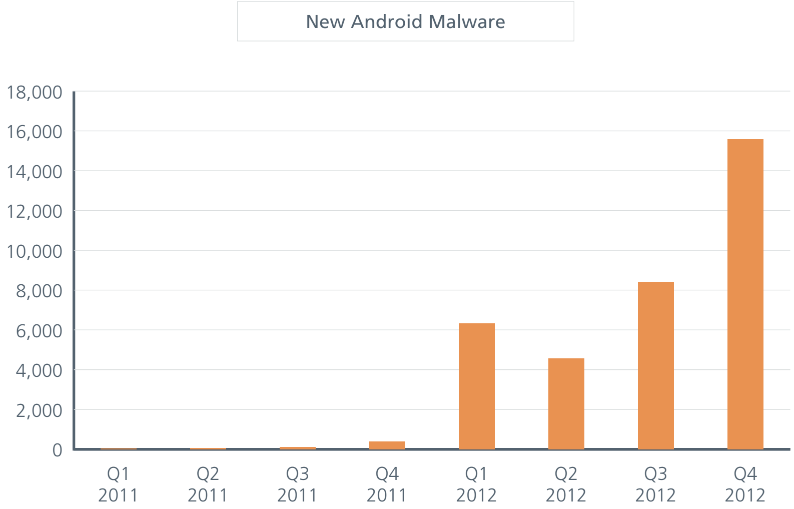
At the start of the new year, the total number of samples in our mobile malware "zoo" reached 36,699, with 95 percent of that arriving in 2012. In all of 2011 we gathered only 792 samples. Will 2013 display a similar amazing climb? We've watched the growth of mobile malware almost double in each of the last two quarters. Some researchers cite higher figures of new mobile malware, with predictions of up to one million binaries by the end of this year. But these numbers may include all files bundled in malicious Android apps and families that repackage APK files. At McAfee Labs, we count only unique malware families and variants and not, for example, common ad libraries and other redundant malicious files.

Total Mobile Malware Samples in the Database



Android, as usual, makes up the bulk of mobile malware, representing 97 percent of the quarterly "pie."





Spyware

Spyware, both commercial and malicious, continues to make up a tiny portion of new Android threats this quarter. Commercial spyware such as Android/SMSTrack.A performs as their manufacturers intend, but more notable are malicious threats Android/Ozotshielder.A and Android/PBL.A.

Android/PBL.A is an app that claims to store a copy of your phonebook and contacts on your phone, but actually sends them off to a server controlled by the attacker. If the author had informed users of what the app was actually doing, we would call this a potentially unwanted program (PUP); instead we classify it as malware.

Android/Ozotshielder.A is trickier. It pretends to be a simple live wallpaper. In reality it contacts the attacker's server to download a list of SMS messages it will send to a premium-rate number. Afterward it sends the list of successfully sent messages to the attacker. This behavior implies that the attacker leases the network of infected devices to various advertisers or crooks who make money from premium-rate SMS.

Mobile Exploits

Recent models of Samsung phones were vulnerable to a configuration error that allowed the legitimate rooting of your phone. This was good for skilled users who wanted to modify the operating system, customize the interface, or add security improvements. But this was bad in that attackers could use the same vulnerability to gain complete access to an unsuspecting user's phone.

The underlying vulnerability gives one complete access to all of the memory in the system. This allows someone skilled or with an exploit to patch the OS and remove all security restrictions. Exploit/ExymemBrk.A, detected as a PUP, serves this dual purpose for both legitimate users and criminals. We detect it in the event that malware authors use it along with their malware to take over your phone.

The legitimate rooting app Android/ExynosToor.A installs the exploit and roots vulnerable phones. This app was later updated to disable the vulnerability to prevent an attacker from entering a phone.

Mobile Backdoors

Attackers love it when users install malicious apps that let the bad guys gain complete control of victims' phones; it's no wonder that mobile backdoors remain popular with attackers.

Android/FakeLookout.A is a mobile backdoor that pretends to be an update to antivirus software. In reality it hands control of a phone to an attacker. It's designed to steal and upload text messages and other files to the attacker's server.

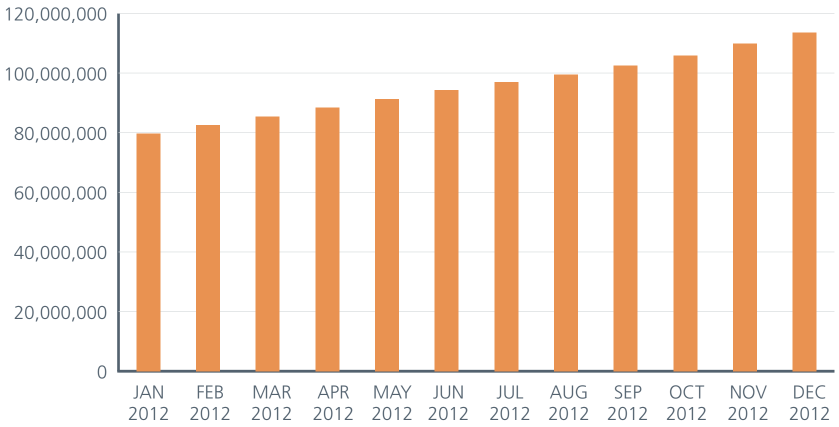
Android/GinMaster.A is a mobile backdoor that uses a root exploit to gain further access to a user's phone. It posts a number of pieces of identifying information to the attacker's server and accepts commands from the attacker.

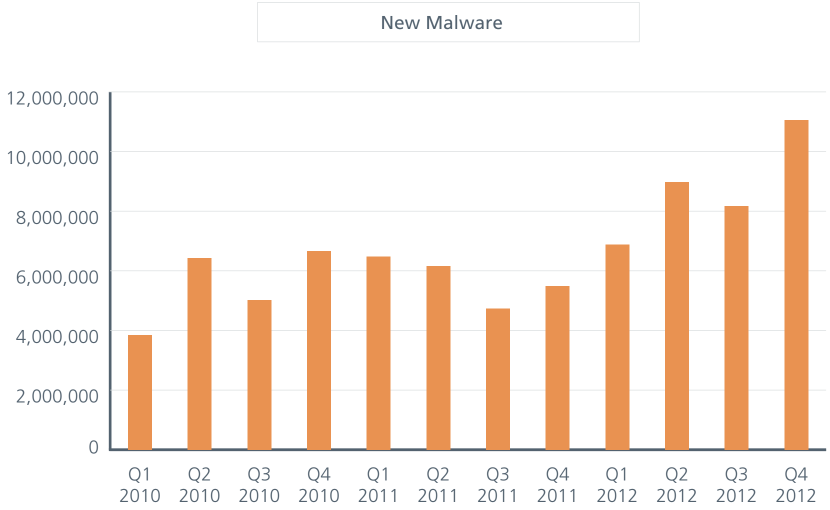
Crimeware on the PC has extended itself onto mobile phones many times. First we saw Zeus with Android/Zitmo, and then SpyEye with Android/Spitmo. Now we've seen Carberp extend itself with Android/Citmo.A. Like the previous malware, Android/Citmo.A is SMS-forwarding malware used by the Carberp authors to forward mobile Transaction Authorization Numbers (mTANs), the secret codes sent via text message to your phone to verify that you're logging in online. Once the attackers have infected your PC with Carberp, your browser will be modified to tell you to download Android/Citmo.A. The attackers will login and wait for the bank to send an mTAN. Your infected phone will immediately forward the mTAN to the attackers, allowing them to login and steal your money.

General Malware Threats

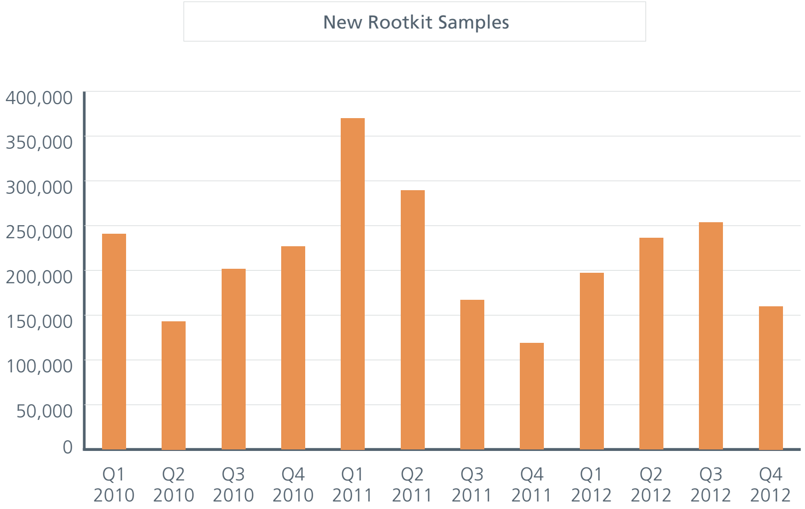
The growth of malware shows a very steady curve in the past year. We already have more than 113 million samples in our malware zoo, and should approach 120 million next quarter. Growth in new malware by quarter is also on a relatively steady, and steeper, path. The third quarter slipped a bit, but this quarter restored the trend, eclipsing 11 million new samples.

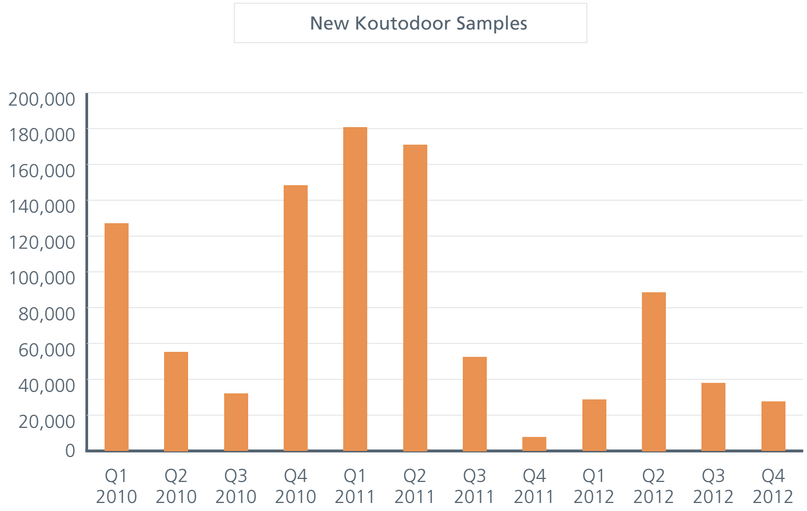
Total Malware Samples in the McAfee Labs Database

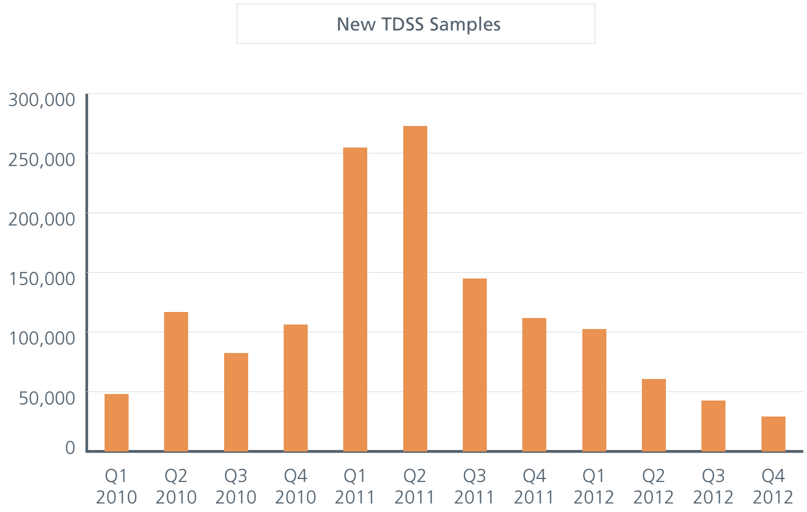


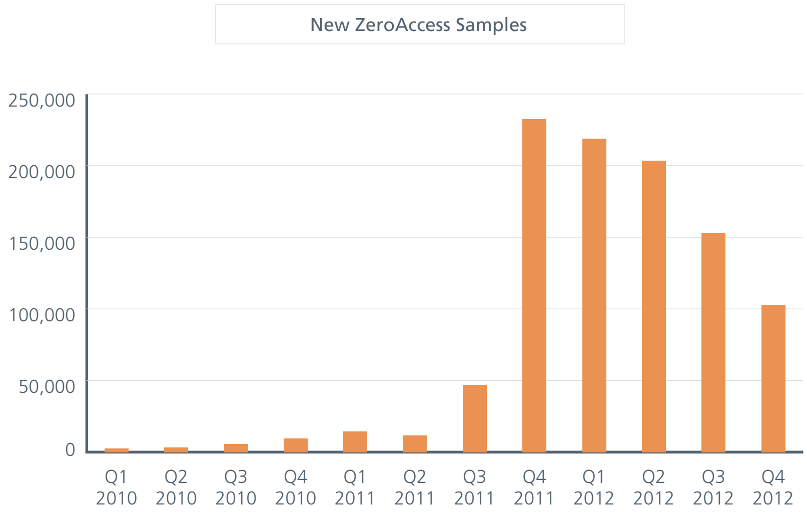


Rootkits, or stealth malware, are one of the nastiest classifications of malware we see. They are designed to evade detection and reside on a system for prolonged periods. After rising during most of the past year, the number of new rootkit samples took a steep downturn this quarter. All three of the rootkits types we track in this report matched this trend. You'll notice the total number of ZeroAccess files exceeds that of all new rootkits. That's because ZeroAccess is a malware family that uses a rootkit, but not all ZeroAccess files are rootkits. Nonetheless, ZeroAccess shows the same downward path as all rootkits.

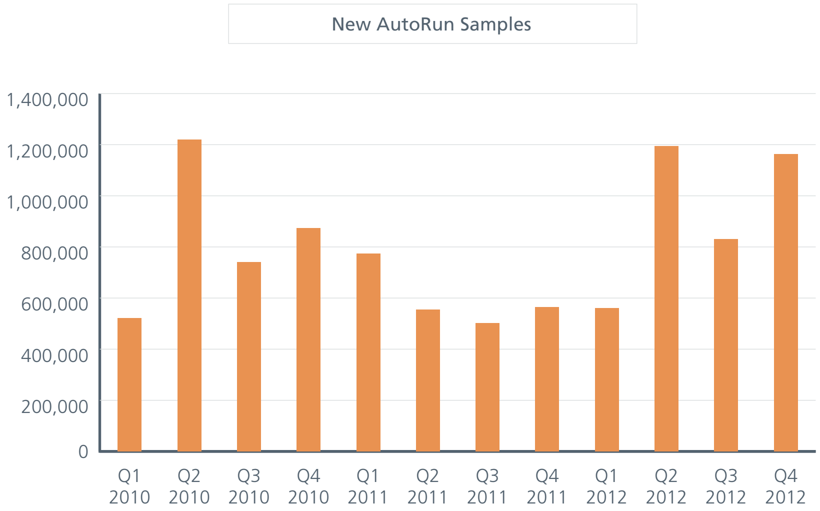


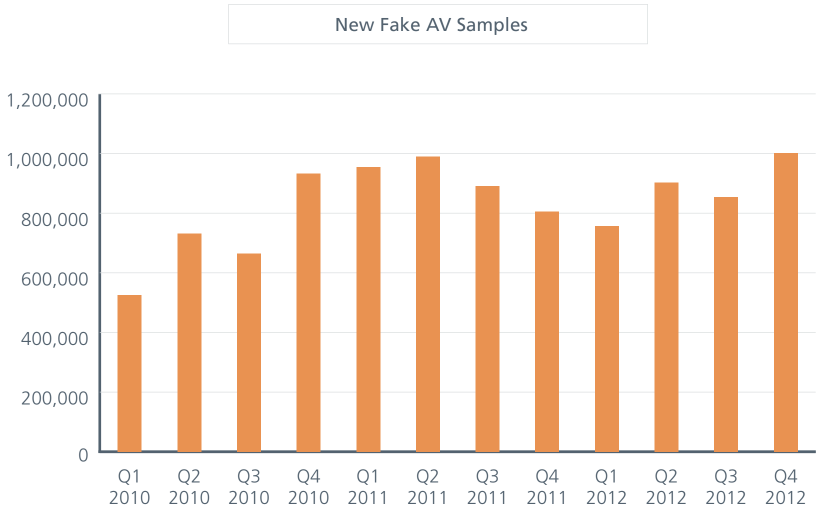

New Koutodoor Samples
200,000
180,000
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
Q1 2010
Q2 2010
Q3 2010
Q4 2010
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012
Q4 2012


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
Q4 2012

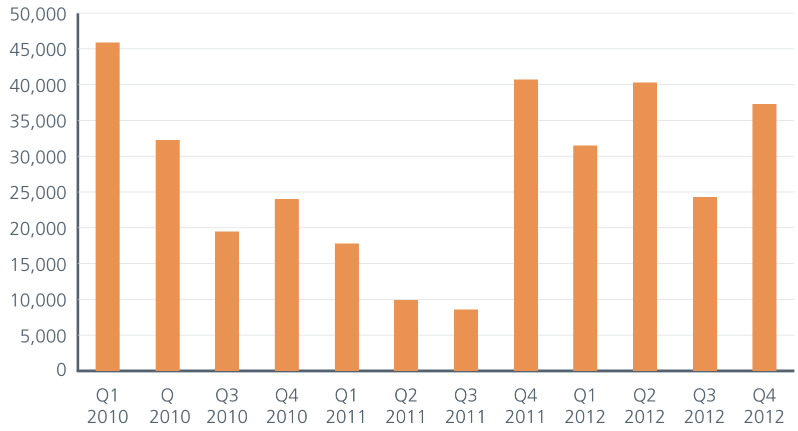

New ZeroAccess Samples
250,000
200,000
150,000
100,000
50,000
0
Q1 2010
Q2 2010
Q3 2010
Q4 2010
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012
Q4 2012

AutoRun malware, which often hides on USB drives and can allow an attacker to take control of a system, bounced back this quarter and almost regained its record high point, set in the second quarter of 2010. The number of fake antimalware products—which often behave as a form of ransomware, extorting money from victims to "clean" their computers—reached a new high, as we collected more than one million new samples during the quarter. Both Koobface, which attacks Facebook users, and password-stealing Trojans, which attempt to raid victims' bank accounts, remained active.

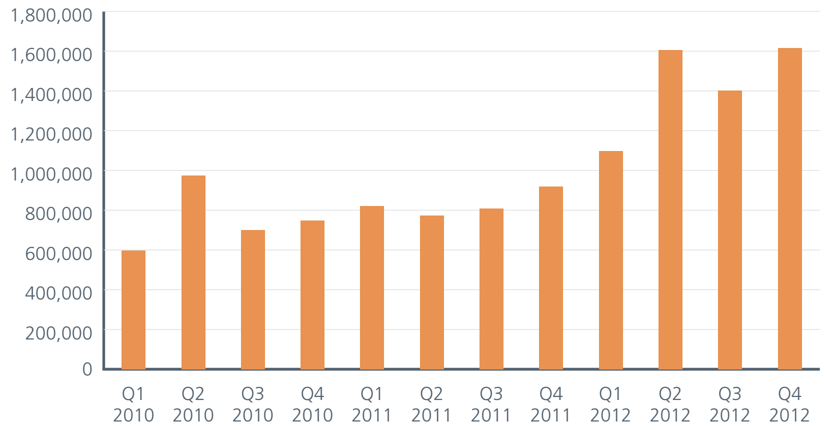




New Koobface Samples

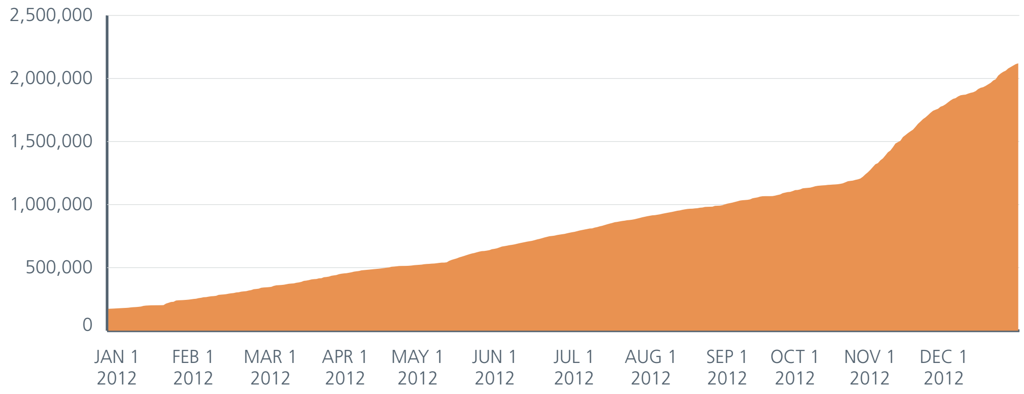


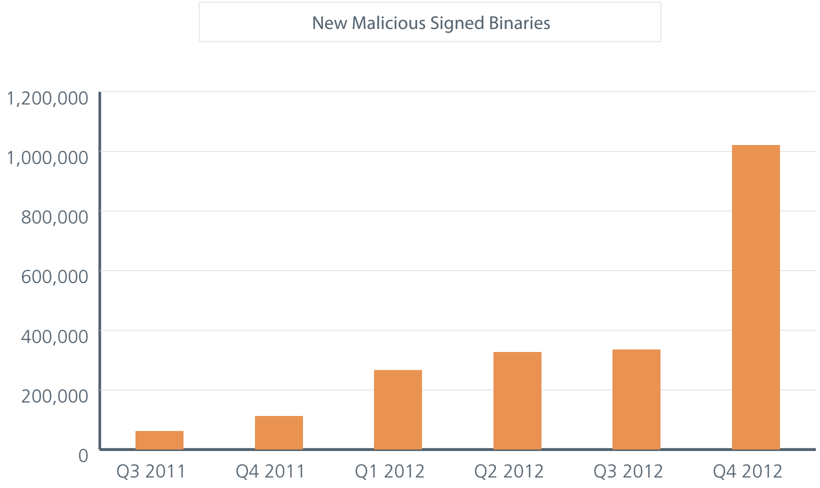
New Password Stealers Samples



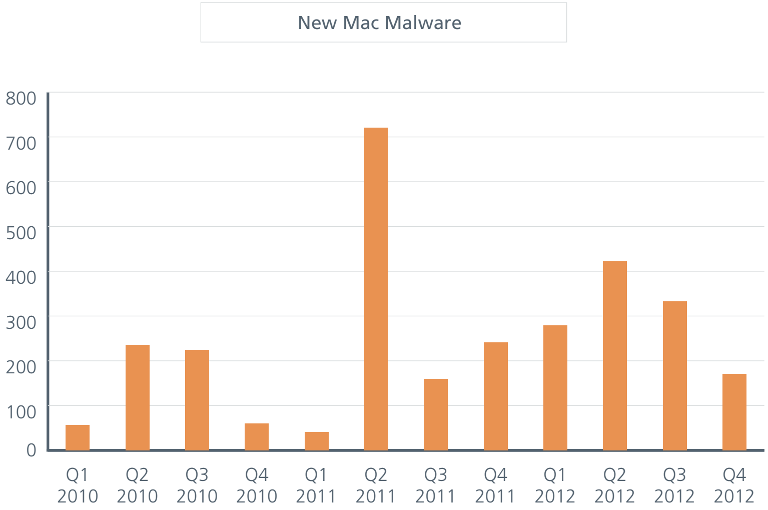
Signed malware, already on an upward trend, increased rapidly starting in November. This advanced technique is usually reserved for targeted attacks.

Total Malicious Signed Binaries



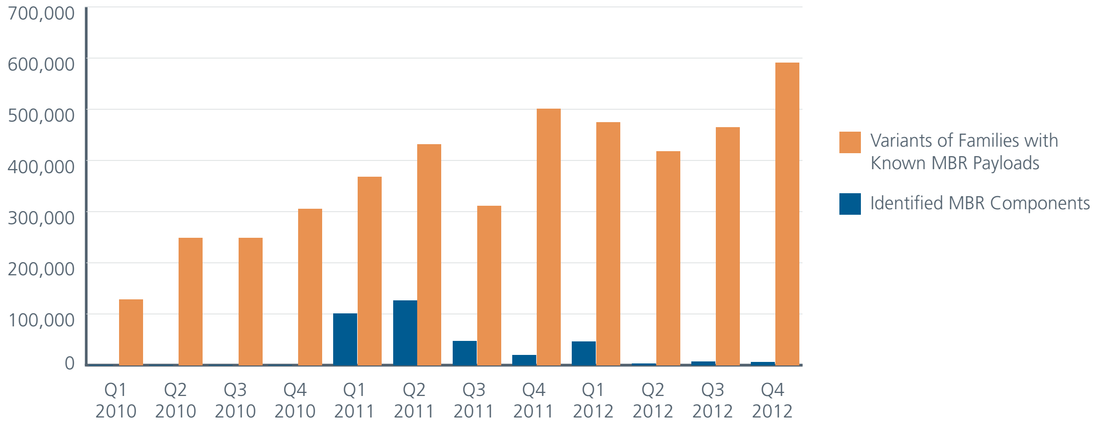


New malware that attacks the Mac declined for the second straight quarter. In spite of the small numbers, it's important that Mac users not think their systems are invulnerable to threats.



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

New Master Boot Record-Related Threats

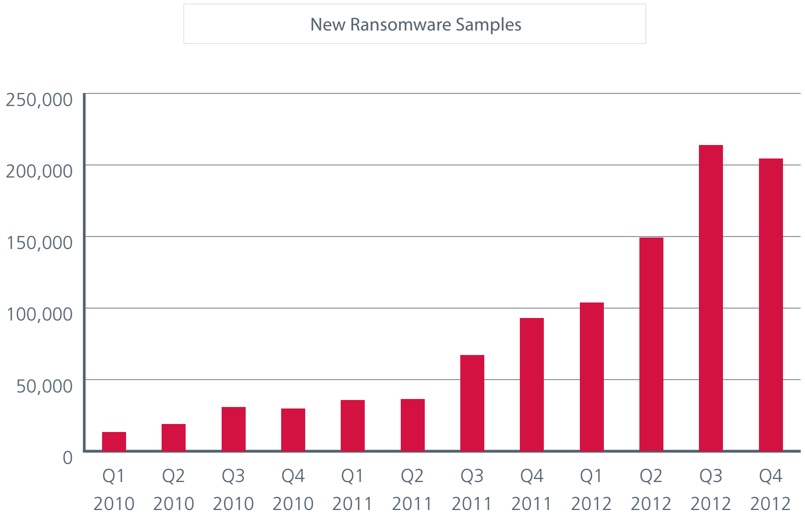


Ransomware

Ransomware has become an increasing problem during the last couple of quarters, and the situation continues to worsen. The number of new, unique samples is greater than 200,000, but the most worrying aspect is the number of reported infections. We have limited visibility into these figures because only our consumer products can share detection data with us. (We make that information public.[3]) We do know that significant numbers of detections began in late summer and spiked this quarter. This trend is also reflected by warnings from law enforcement and federal agencies around the globe.

One reason for ransomware's growth is that it is a very efficient means for criminals to earn money because they use various anonymous payment services. This method of cash collection is superior to that used by fake AV products, for example, which must process credit card orders for the fake software. Another reason is that an underground ecosystem is already in place to help with services such as pay-per-install on computers that are infected by other malware, such as Citadel, and easy-to-use crime packs are available in the underground market. Criminals can buy kits like Lyposit—whose malware pretends to come from a local law enforcement agency (based on the computer's regional settings) and instructs victims to use payment services in a specific country—for just a share of the profit instead of for a fixed amount.

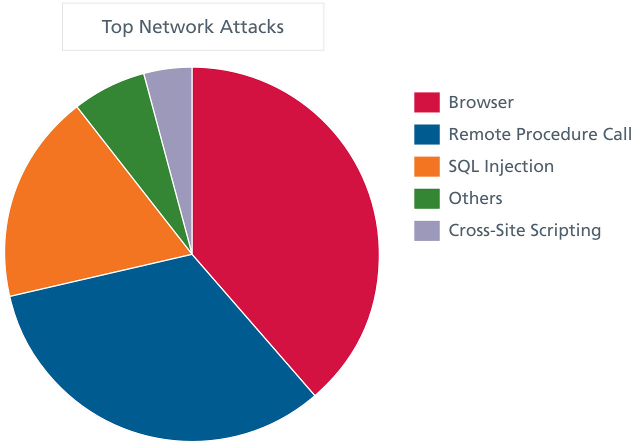
These advantages mean that the problem of ransomware will not disappear anytime soon. You should always take precautions to back up your valuable data.

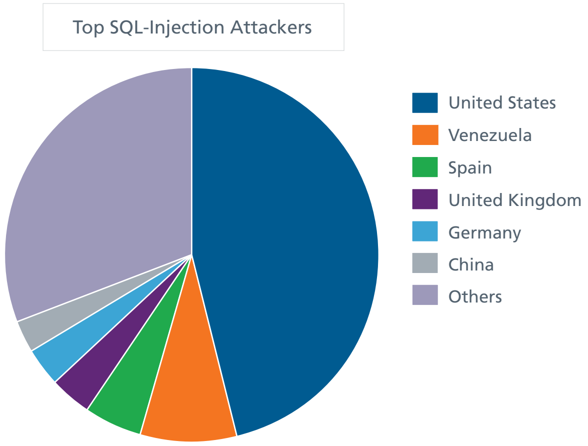

New Ransomware Samples

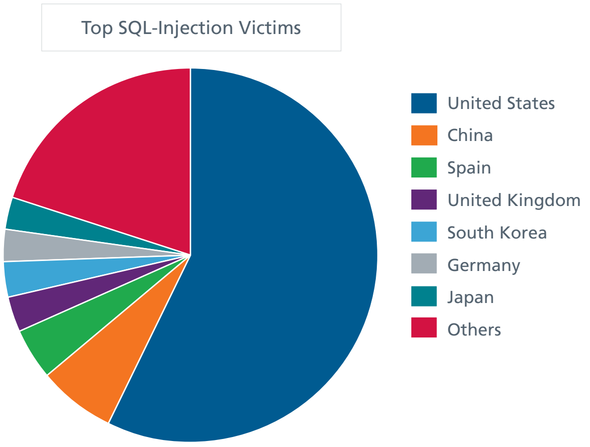
Network Threats

Once again the United States is both the source and the target of much of the Internet's malicious activity, according the McAfee Global Threat Intelligence™ network. However, looking at IP addresses and where they are "located" is only one attribute.

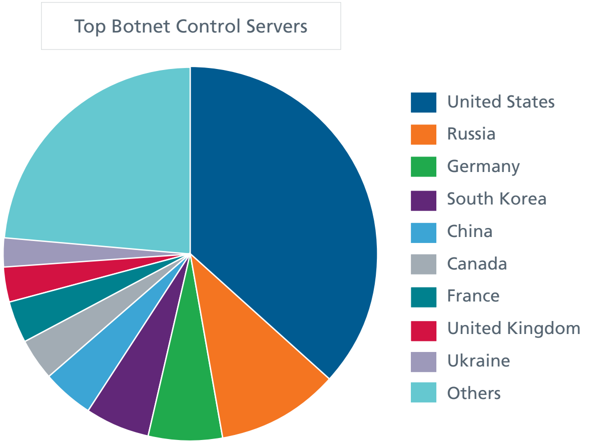
Both browser and remote procedure call attacks continue to outpace SQL injection in frequency.

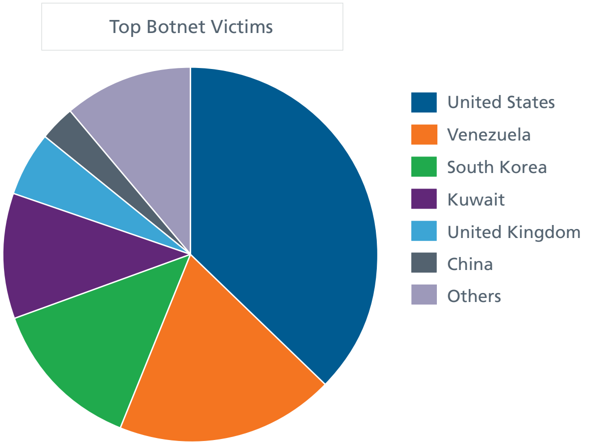

Top Network Attacks


Top SQL-Injection Attackers


Top SQL-Injection Victims

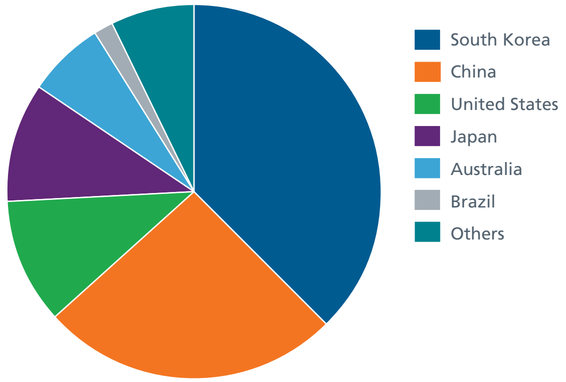
Among botnet victims, IP addresses in the United States reclaimed the top position from Venezuela, which led in the third quarter.


Top Botnet Control Servers


Top Botnet Victims

Last quarter the United States was the clear leader among countries hosting the most PDF exploits. This quarter, however, South Korea, with 38 percent of sources, and China, with 26 percent, led the way.

Top Malicious PDF Attackers

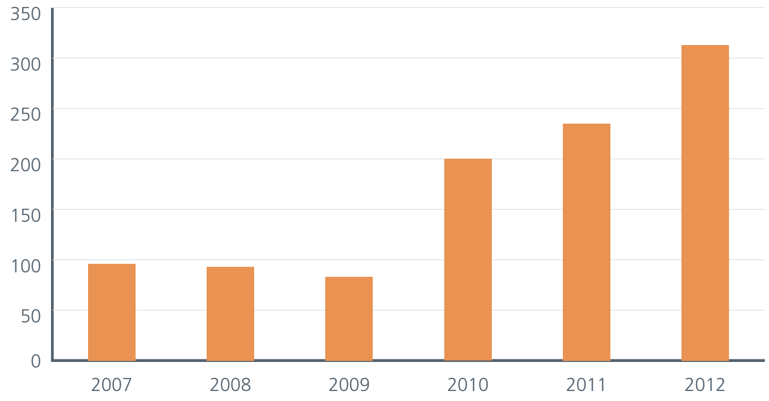


Database Security

This quarter was relatively quiet in the number of publicly reported data breaches, with just 47. But that figure is misleading: The total number of data breaches from the beginning of the year was more than 300, significantly higher than in previous years.

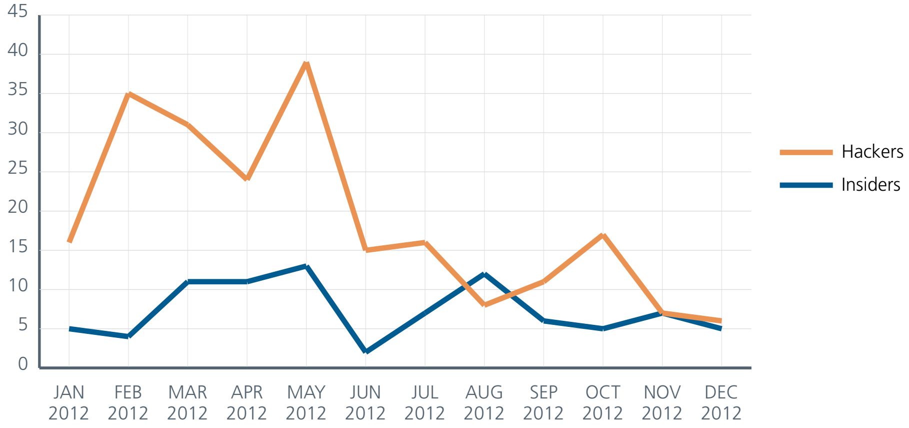
One of the biggest breaches this quarter affected the South Carolina Department of Revenue, whose website was hacked. More than 6.4 million citizens were affected. Another impressive data breach was discovered in more than 100 universities around the globe, including Princeton, Harvard, Cambridge, Moscow, and Tokyo. In this case the GhostShell hackers' team, associated with Anonymous, stole data records from more than 120,000 user accounts.

Data Breaches Made Public



Source: privacyrights.org.

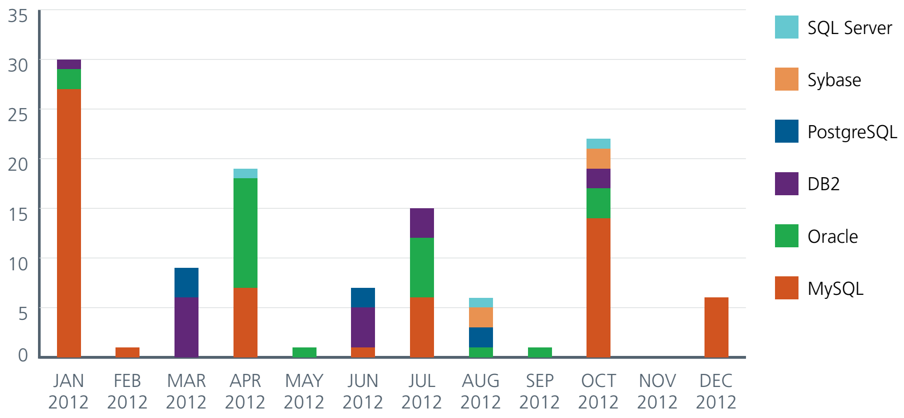
Sources of Data Breaches



Source: privacyrights.org.

Looking at database vulnerabilities, MySQL has set a remarkable pace, with the largest number of disclosed or patched vulnerabilities among leading products. On December 1 six new MySQL zero-day vulnerabilities were released in public. Overall 62 MySQL vulnerabilities were disclosed or fixed during 2012, far ahead of the second place product, Oracle, with 25 new vulnerabilities. MySQL is also an Oracle product.

New Vulnerabilities in Leading Databases



One outstanding threat in recent months is malware targeting business databases. "Narilam" is a first-class database sabotage mechanism. This worm installs itself on infected machines in a typical manner for malware. However its function is unusual: The worm tries to access preconfigured Microsoft SQL Server databases. Narilam was designed to damage Iranian accounting and banking software, looking for instances of Maliran, Shahd, and Amin systems. Once it find them, Narilam damages the content by updating data with random values or by deleting various objects.

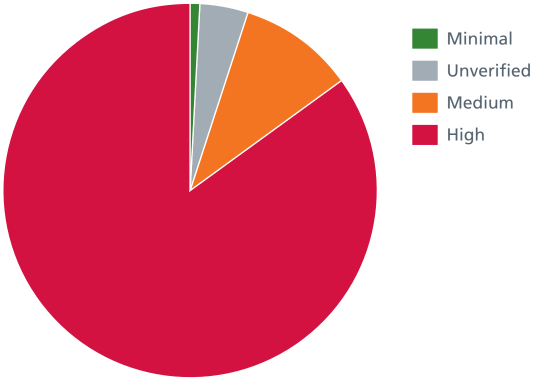
The big question about Narilam is whether it is an example of one-time database sabotage or the harbinger of a widely used trend. Considering other trends in the data security field, it's hard to remain optimistic regarding this question.

Web Threats

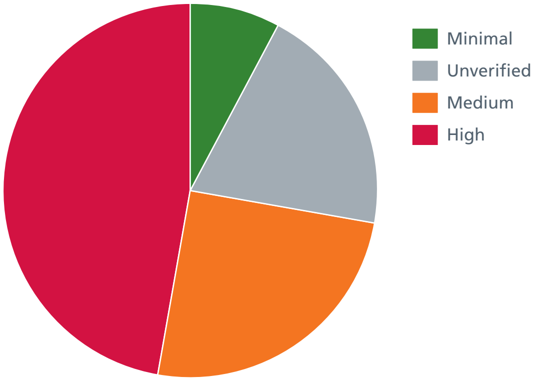
Websites can gain bad or malicious reputations for a variety of reasons. Reputations can be based on full domains and any number of subdomains, as well as on a single IP address or even a specific URL. Malicious reputations are influenced by the hosting of malware, potentially unwanted programs, or phishing 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.

In our databases, these URLs and domains are classified according to their risk ratings. This quarter the percentage of high-risk URLs increased to 85 percent, from 81 percent in the third quarter. The percentage of high-risk domains increased to 47 percent, up from 42 percent in the prior quarter.

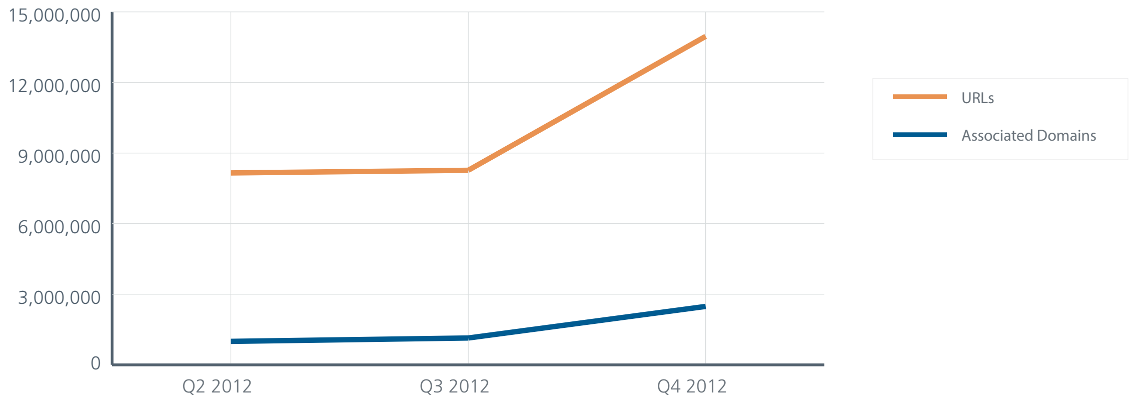
Risk Level of Suspect URLs



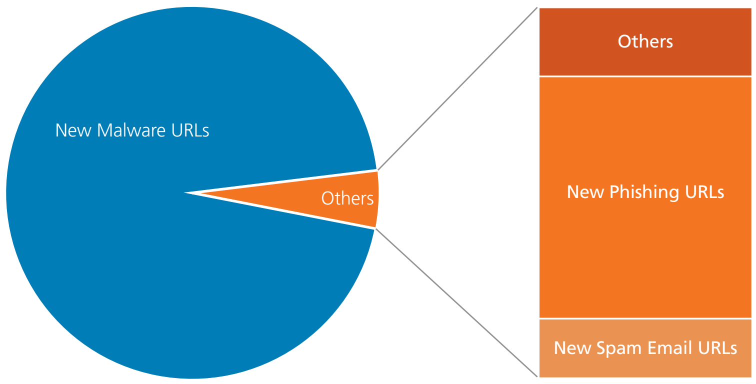
Risk Level of Suspect Domains



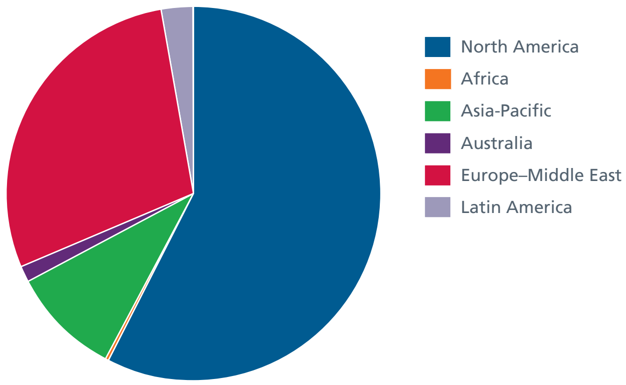
This quarter the number of new suspect URLs averaged 4.6 million per month, up from 2.7 million per month in the last two quarters.


New Suspect URLs

Most of these suspicious URLs (95 percent) host malware, exploits, or codes that have been designed specifically to compromise computers. Phishing and spam represent 3 percent and 1 percent, respectively.

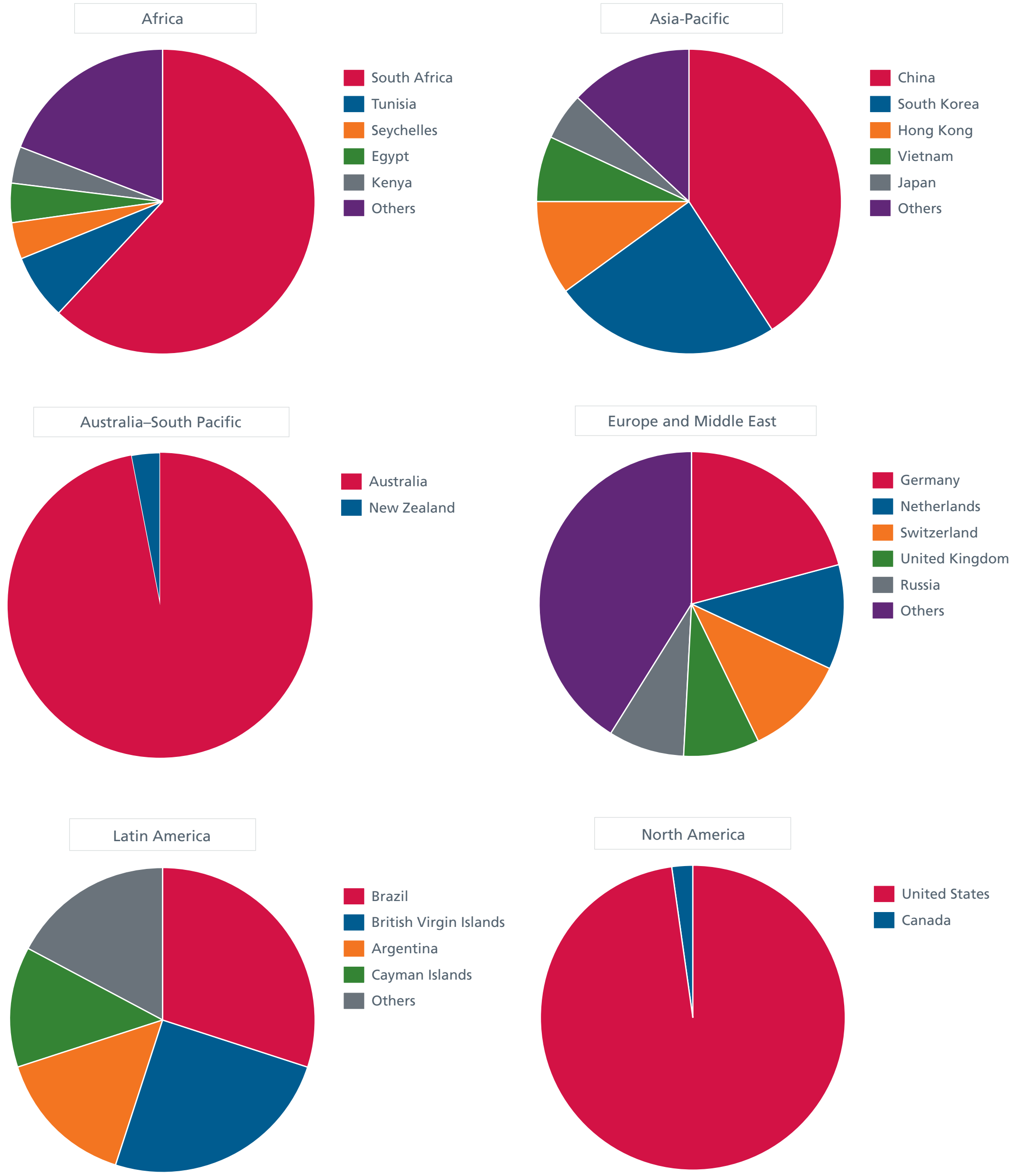

Distribution of New Suspect URLs

The domains associated with newly suspect URLs are located mainly in North America (chiefly the United States) and Europe and the Middle East (primarily Germany, followed by the Netherlands and Switzerland).


Location of Servers Hosting Suspect Content

Our analysis of servers hosting malicious content shows that most regions have a clearly dominant player.

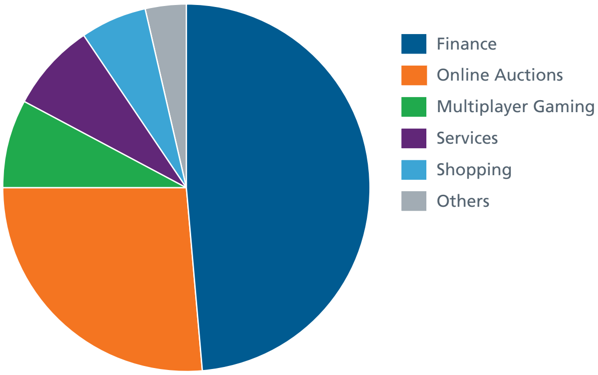
Location of Servers Hosting Malicious Content



Phishing

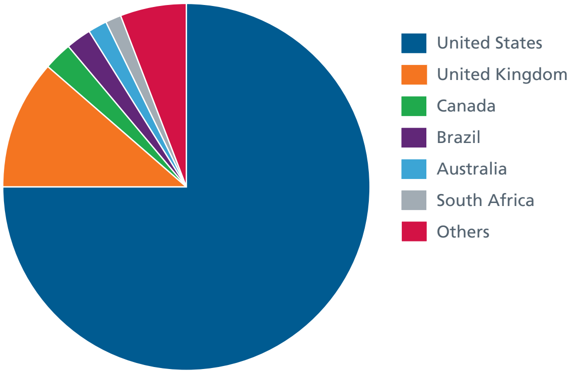
Although phishing attempts against financial targets remain popular, the overall percentage declined to less than 50 percent this quarter. Attacks against online auctions and multiplayer online gaming increased.

Phishing Targets by Industry



Systems in the United States have grown this quarter to 75 percent of all targets from more than 50 percent last quarter.

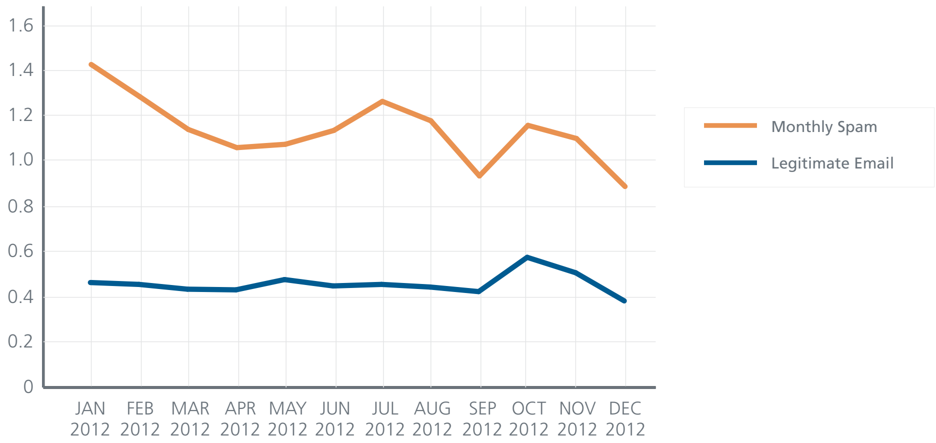
Phishing Targets by Country



Messaging Threats

The number of spam messages increased in October and then fell to the lowest point in several years.

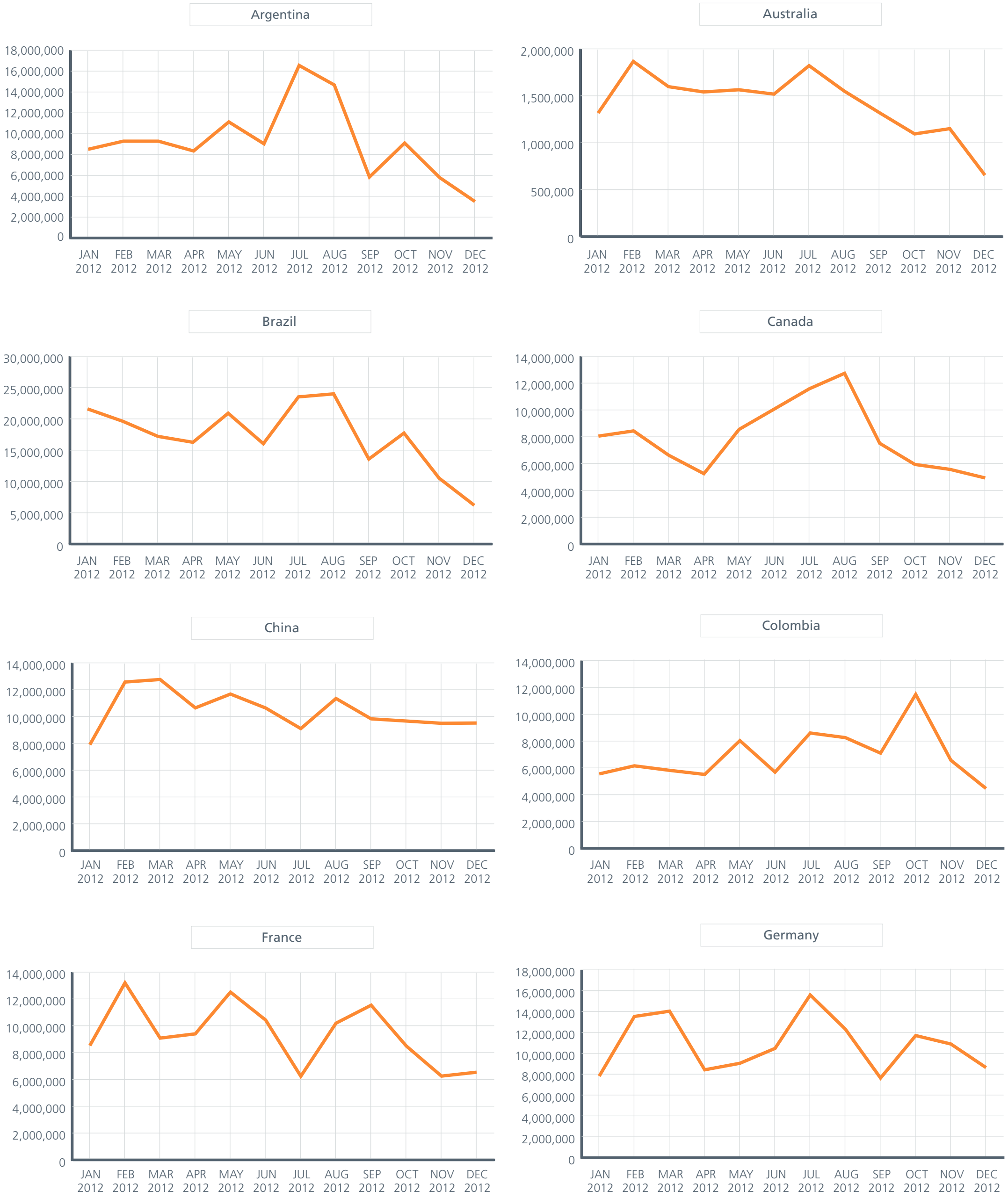
Global Email Volume, in Trillions of Messages



Spam volume

Falling spam counts were reflected by large decreases in Turkey (with a drop of 70 percent this quarter), India (67 percent), Spain (56 percent), and Argentina (50 percent). But spam behavior is localized; counts rose in Romania (54 percent) and Poland (35 percent).

Spam Volume



Argentina

Australia

Brazil

Canada

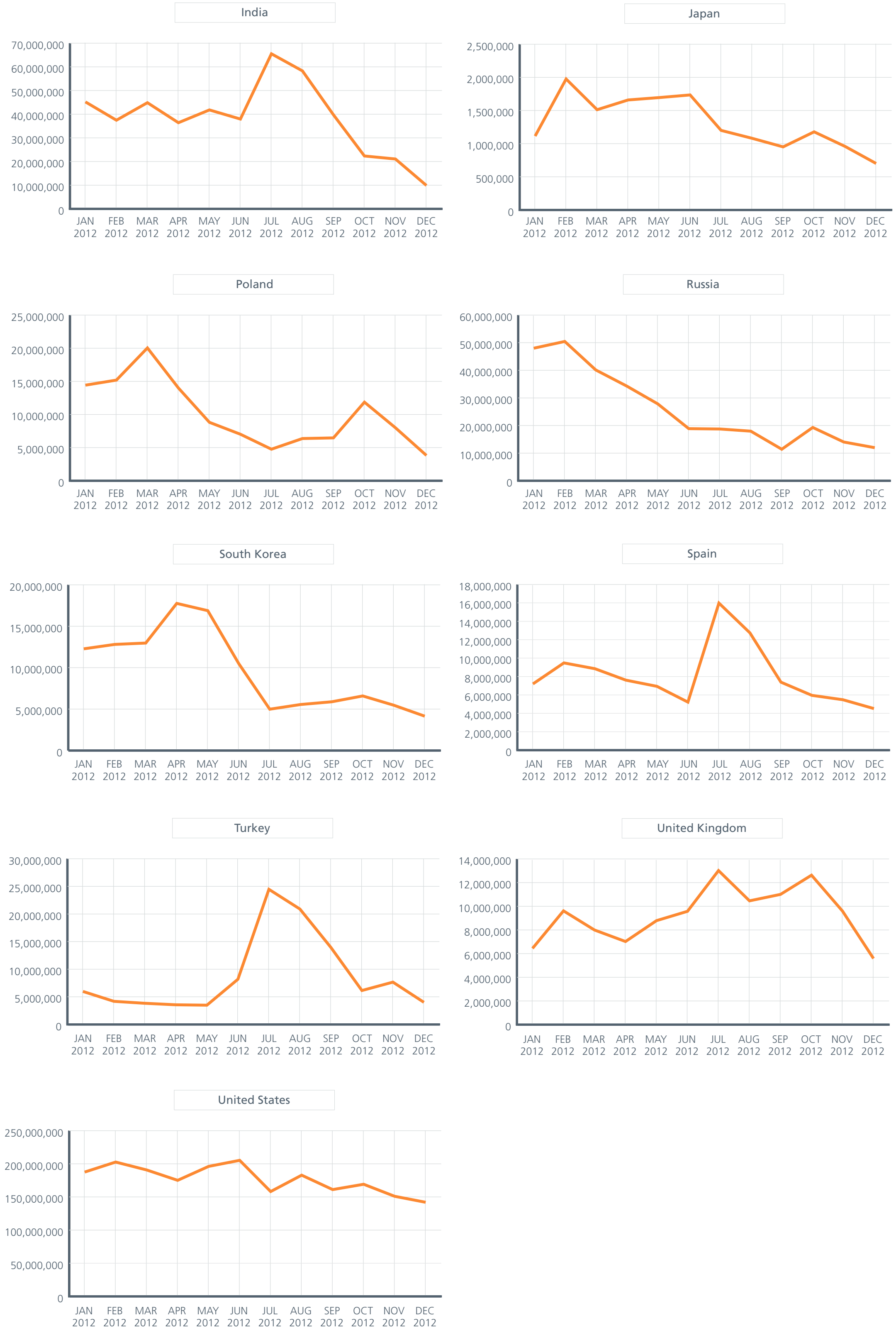
China

Colombia

France

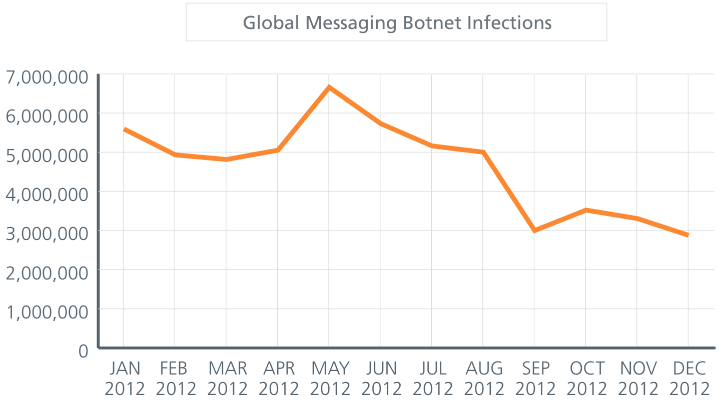
Germany

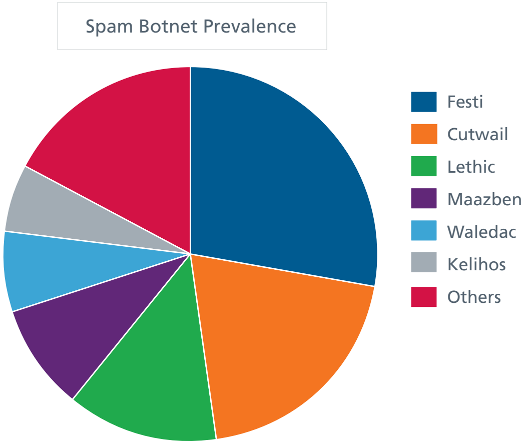
Spam Volume

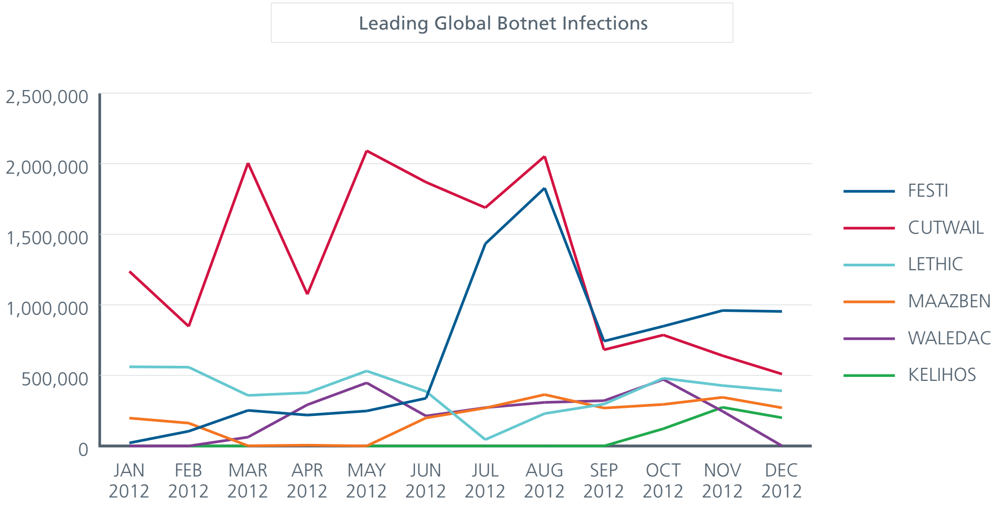

India
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
JAN 2012 FEB 2012 MAR 2012 APR 2012 MAY 2012 JUN 2012 JUL 2012 AUG 2012 SEP 2012 OCT 2012 NOV 2012 DEC 2012
Japan
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
JAN 2012 FEB 2012 MAR 2012 APR 2012 MAY 2012 JUN 2012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

Botnet breakdowns

Infections from messaging botnets were flat for the quarter. Volume has shown an overall decline since May. Waledac, which began in March and peaked in October, is basically dead. Will it rise again? It can happen. Festi and Lethic increased slightly during the quarter, while Cutwail, which three times this year infected more than two million computers in a month, dropped to 500,000 new infections in December. A new botnet, Kelihos, is now on the scene, though its numbers are still small in comparison with the other leaders.


Global Messaging Botnet Infections

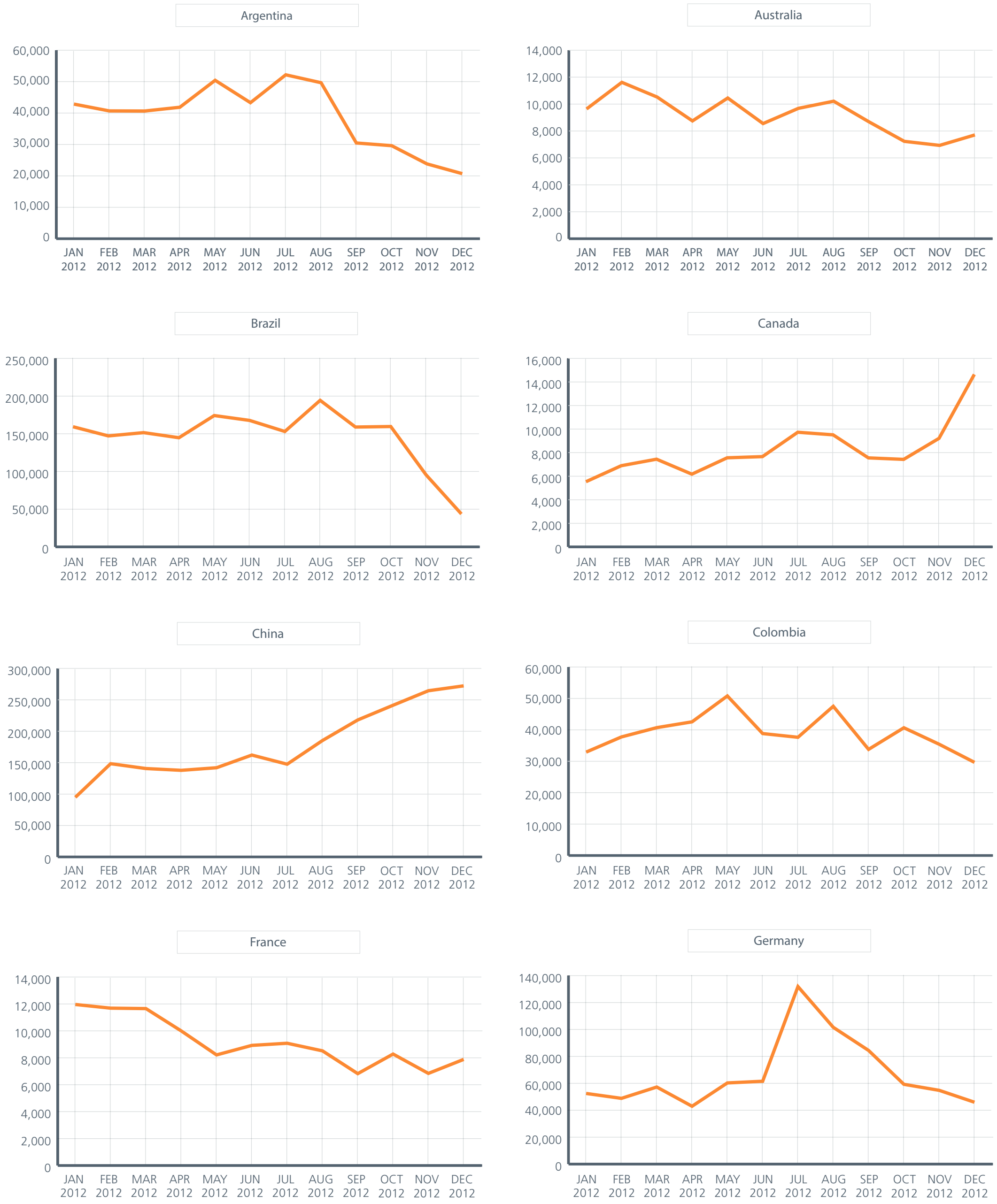

Spam Botnet Prevalence

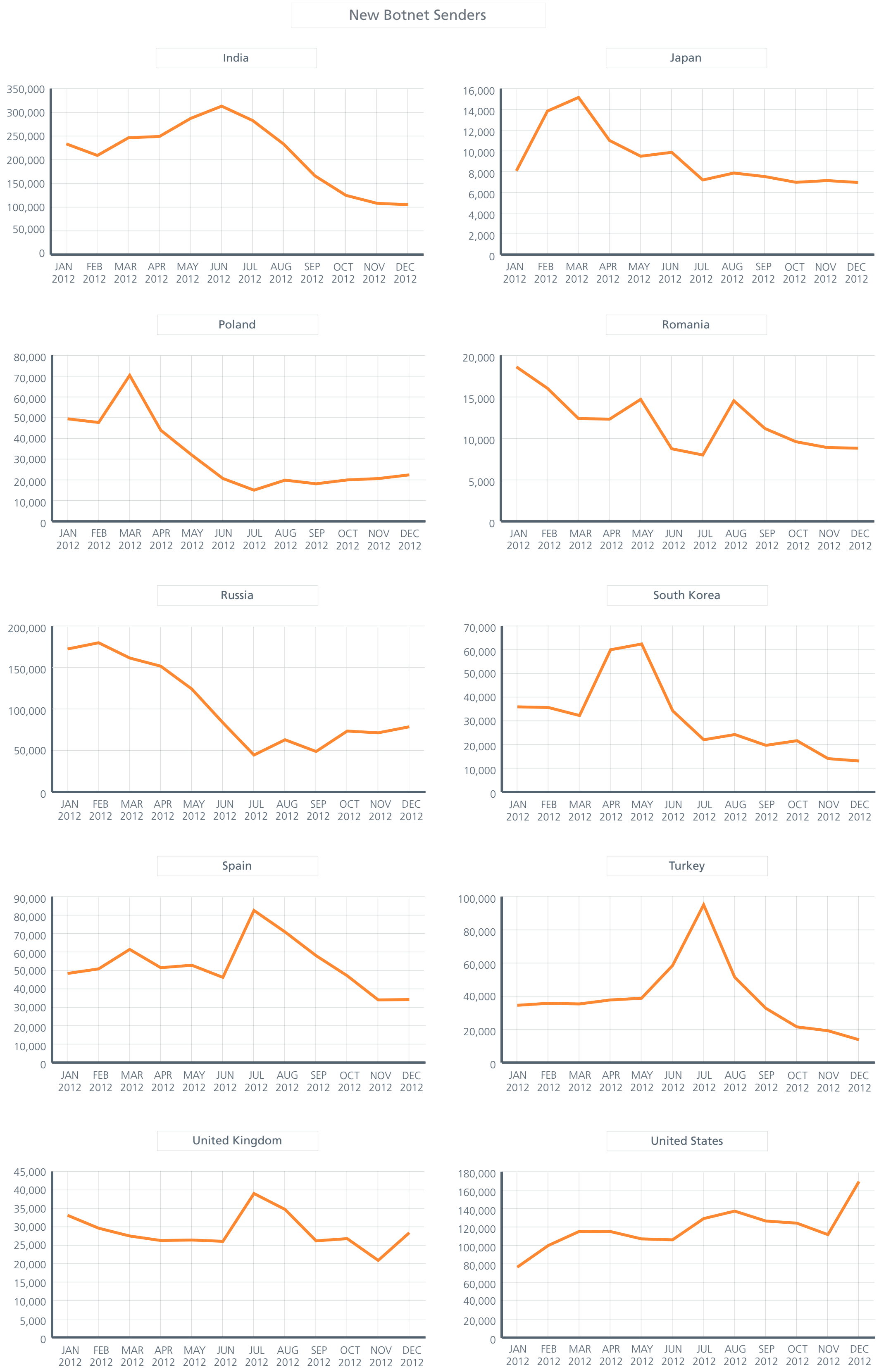

Leading Global Botnet Infections

New botnet senders

New botnet infections occurred this quarter at about the same rate as last quarter. Nonetheless, we saw considerable differences among countries. Infections increased notably in Russia (43 percent this quarter) and China (41 percent). Poland, Canada, and Indonesia also experienced growth between 19 and 11 percent. Infections in Turkey, on the other hand, decreased by 70 percent, as well as Germany and India (50 percent), Spain (45 percent), Argentina (44 percent), and Brazil (41 percent).

New Botnet Senders





New Botnet Senders

India

Japan

Poland

Romania

Russia

South Korea

Spain

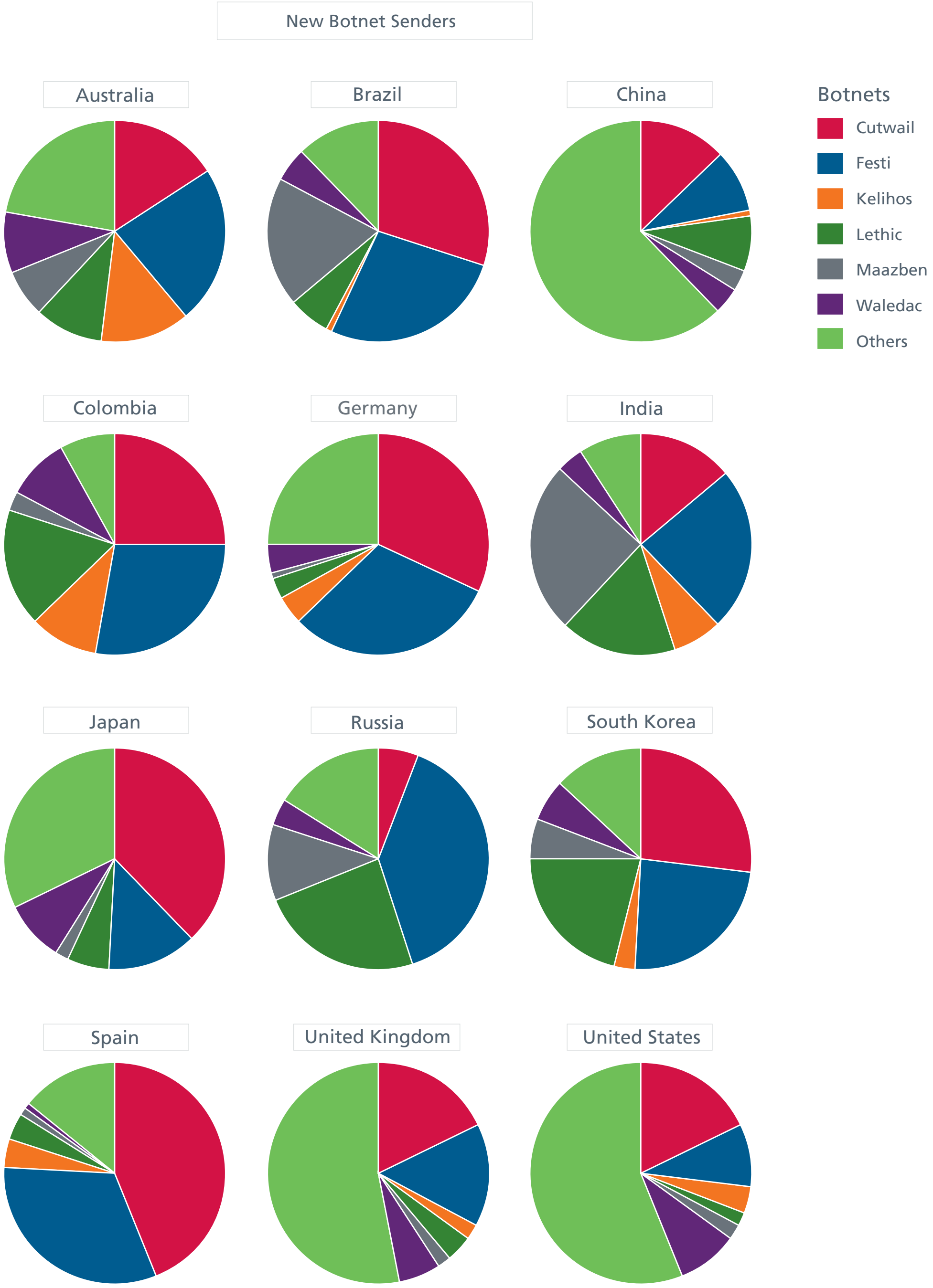
Turkey

United Kingdom

United States

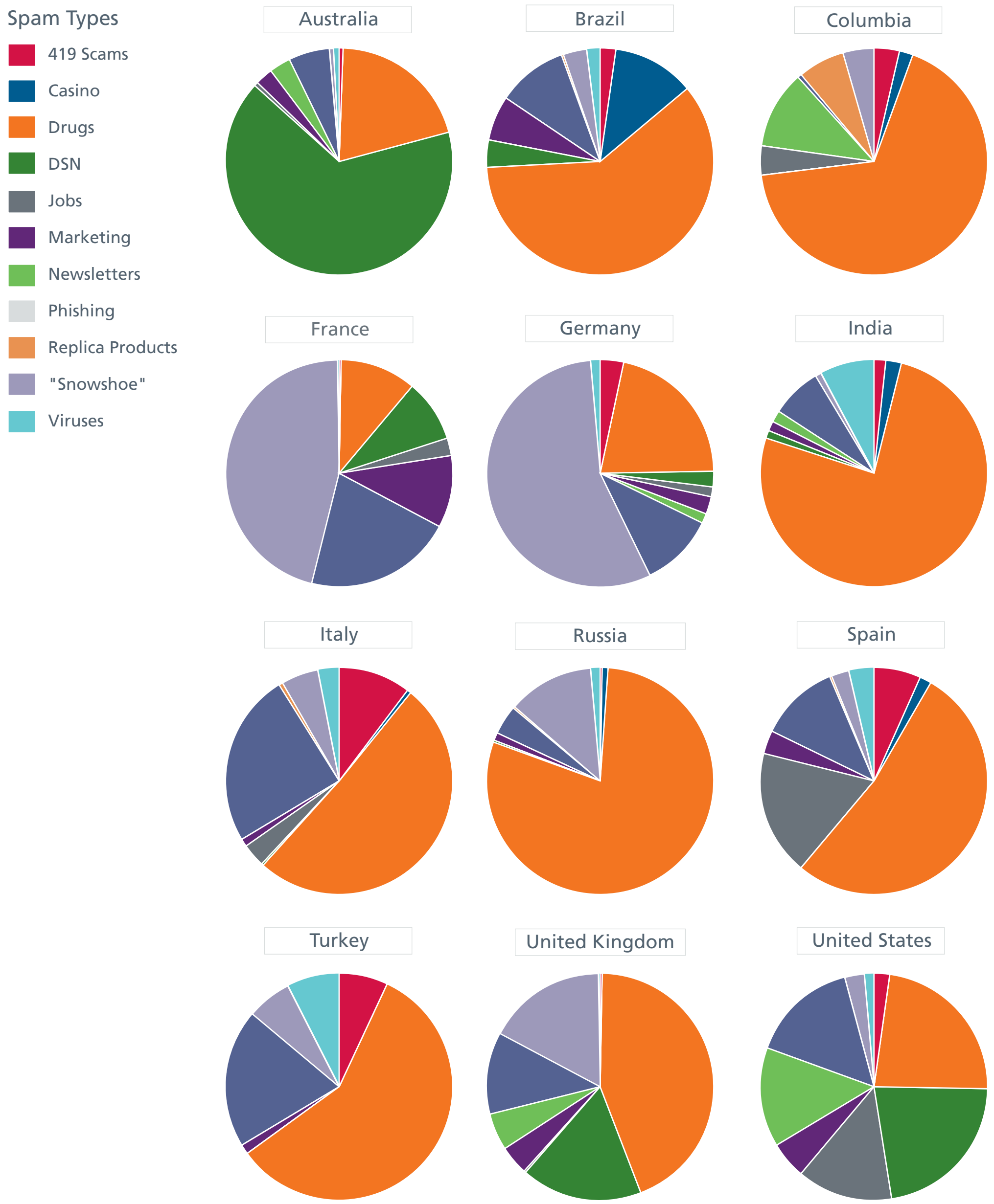
Messaging botnet prevalence

Our breakdown of botnets shows how the six most widespread botnet families are represented in various countries around the globe. Cutwail and Festi are the global leaders. But Maazben, in India, and Lethic, in Russia, are also very popular. In China, the United Kingdom, and the United States, "other" botnets exceed 50 percent, demonstrating the variety of malicious networks.



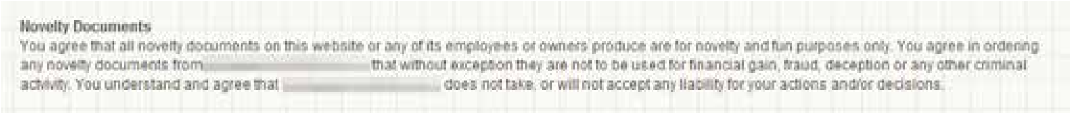
Drug spam remains strong

In our analysis of spam subject lines this quarter, we again find drug spam was the most popular by far in many nations. Australia (where Delivery Service Notifications were most popular), and France and Germany were exceptions. The last two most often saw "snowshoe" spam, which spreads out the load by sending spam from many IP addresses, even if the spammers are rapidly evicted from those sources.



Cybercrime

Selling fake documents and fake pay slips is lucrative work on the Internet. Many online stores offer these facilities. Let’s visit one of these shops hosted in Europe. To simulate a semblance of legality, the service explains it is just for fun and must not be used for fraudulent activity:

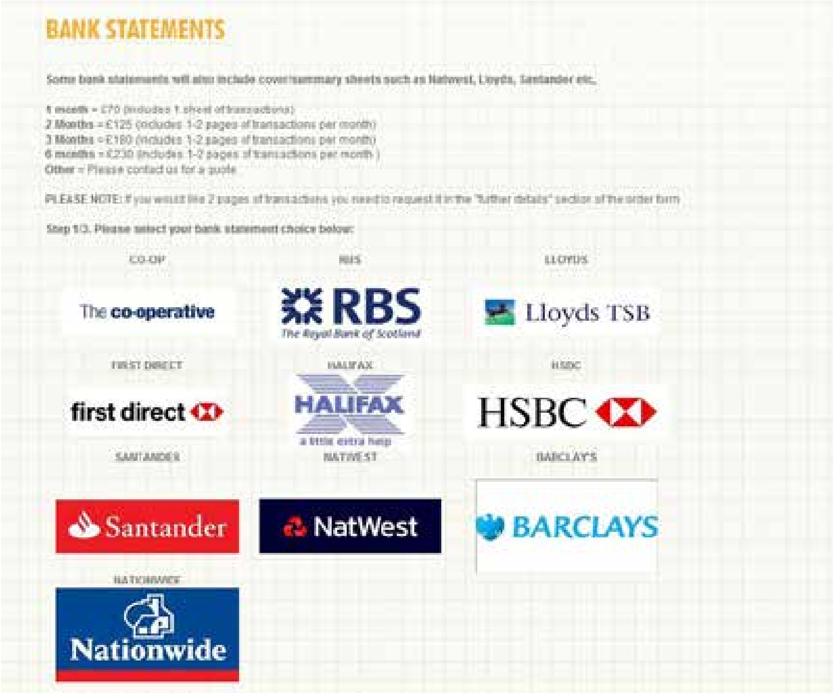


Novelty Documents

You agree that all novelty documents on this website or any of its employees or owners produce are for novelty and fun purposes only. You agree in ordering any novelty documents from [redacted] that without exception they are not to be used for financial gain, fraud, deception or any other criminal activity. You understand and agree that [redacted] does not take, or will not accept any liability for your actions and/or decisions.

The price for one utility bill is £30. Templates exist for British Gas, Southern Electric, United Utility, Talk Talk, Virgin Media, Tax Code, EON, EDF, and BT. One pay slip is £15. For a full year, you have to pay £60.

Bank statements, still for “fun,” are more expensive:



BANK STATEMENTS

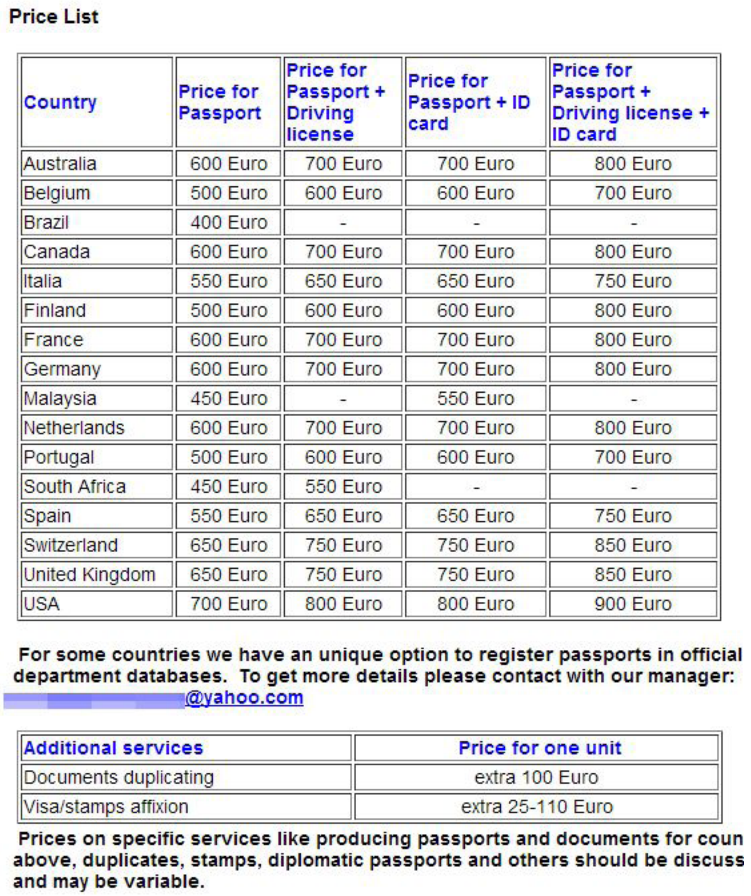
Some bank statements will also include cover/summary sheets such as Natwest, Lloyds, Santander etc.

1 month = £70 (includes 1 sheet of transactions)
2 Months = £125 (includes 1-2 pages of transactions per month)
3 Months = £180 (includes 1-2 pages of transactions per month)
6 months = £230 (includes 1-2 pages of transactions per month)
Other = Please contact us for a quote

PLEASE NOTE: If you would like 2 pages of transactions you need to request it in the "further details" section of the order form

Step 1/3. Please select your bank statement choice below:

Websites offering passports, driver’s licenses, and ID cards are also numerous online. They are built on the same model, and the price lists are often similar.



Price List

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	800 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	-	550 Euro	-
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
South Africa	450 Euro	550 Euro	-	-
Spain	550 Euro	650 Euro	650 Euro	750 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
United Kingdom	650 Euro	750 Euro	750 Euro	850 Euro
USA	700 Euro	800 Euro	800 Euro	900 Euro

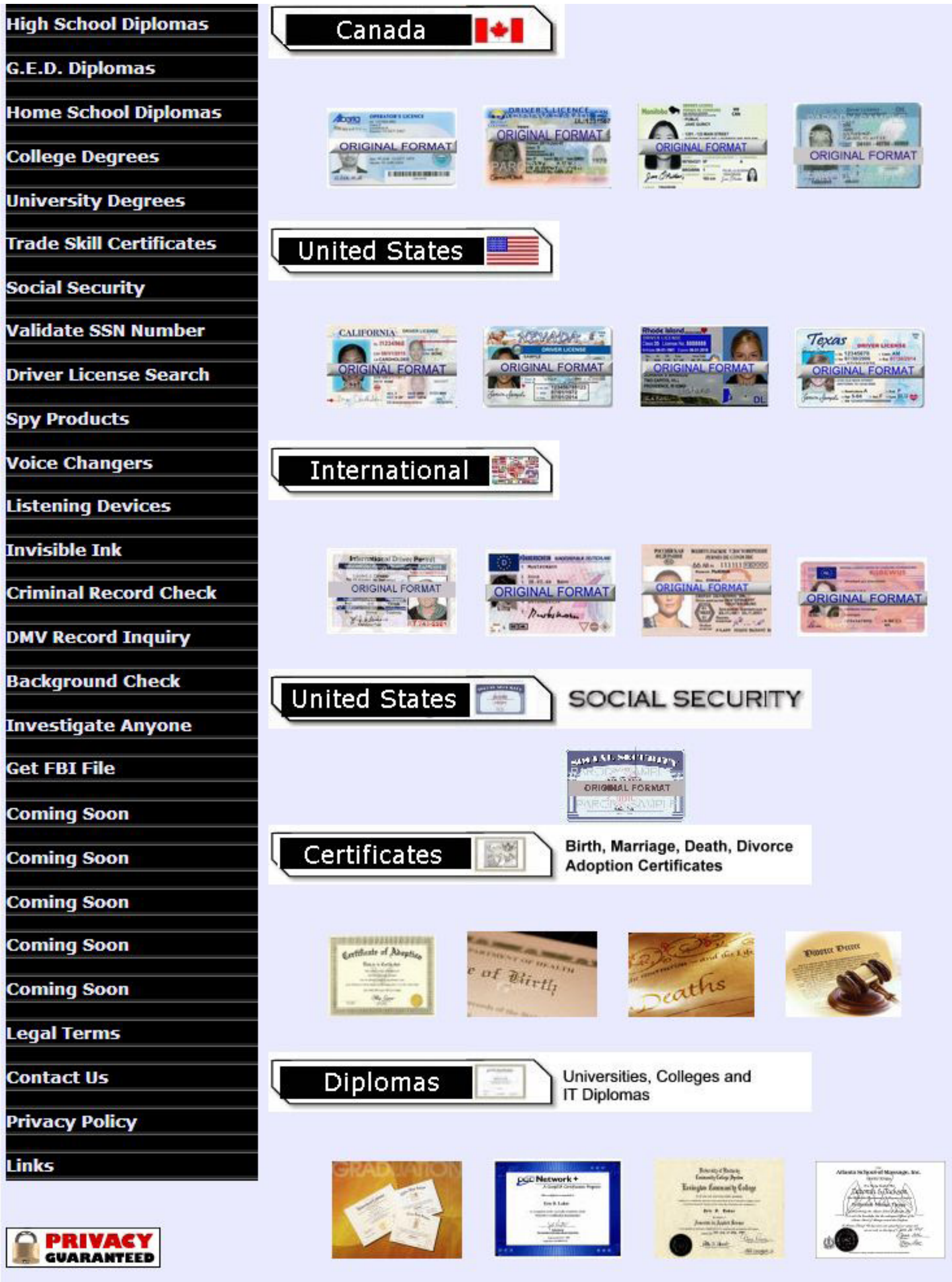
For some countries we have an unique option to register passports in official department databases. To get more details please contact with our manager: [redacted]@yahoo.com

Additional services	Price for one unit
Documents duplicating	extra 100 Euro
Visa/stamps affixion	extra 25-110 Euro

Prices on specific services like producing passports and documents for coun above, duplicates, stamps, diplomatic passports and others should be discuss and may be variable.

We have great doubts—regarding both the quality and delivery—about such transactions. We read in several forums that many buyers received no documents after they sent the money as specified via WebMoney, Western Union, or MoneyGram methods. These rip-offs work because most buyers will not file a complaint in cases of deception.

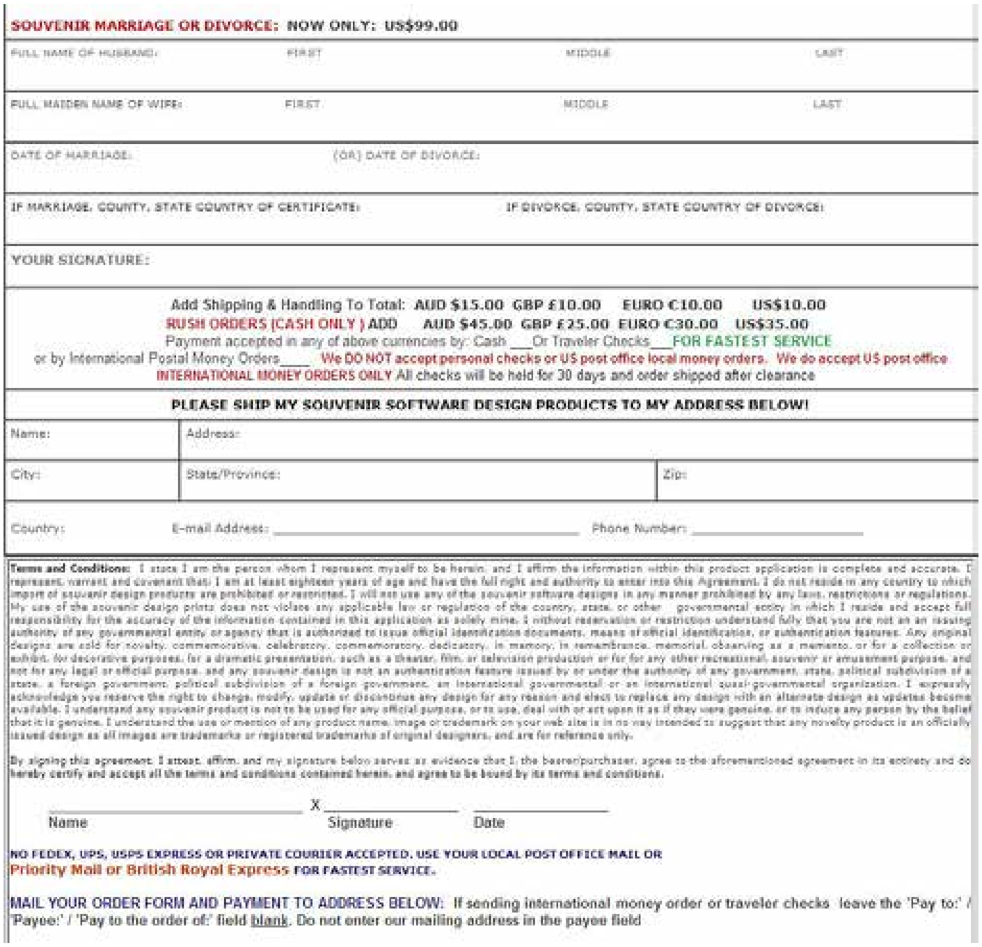
Some of these sites offer abundant choices. For around US$100, you can obtain papers for whatever you like: adoption, death, divorce, baptism, etc.



Birth, Marriage, Death, Divorce
Adoption Certificates

Universities, Colleges and
IT Diplomas

In all cases, the buyers have to fill in a product-order form. Every form starts with the label "souvenir." Despite the fact that the FAQ explains that buyers can use these documents instead of real ones, the terms and conditions are supposed to protect the seller.



SOUVENIR MARRIAGE OR DIVORCE: NOW ONLY: US$99.00

FULL NAME OF HUSBAND: FIRST MIDDLE LAST

FULL MAIDEN NAME OF WIFE: FIRST MIDDLE LAST

DATE OF MARRIAGE: (OR) DATE OF DIVORCE:

IF MARRIAGE, COUNTY, STATE COUNTRY OF CERTIFICATE: IF DIVORCE, COUNTY, STATE COUNTRY OF DIVORCE:

YOUR SIGNATURE:

Add Shipping & Handling To Total: AUD $15.00 GBP £10.00 EURO €10.00 US$10.00
RUSH ORDERS (CASH ONLY) ADD AUD $45.00 GBP £25.00 EURO €30.00 US$35.00
Payment accepted in any of above currencies by: Cash ___Or Traveler Checks___FOR FASTEST SERVICE
or by International Postal Money Orders____ We DO NOT accept personal checks or US post office local money orders. We do accept US post office
INTERNATIONAL MONEY ORDERS ONLY All checks will be held for 30 days and order shipped after clearance

PLEASE SHIP MY SOUVENIR SOFTWARE DESIGN PRODUCTS TO MY ADDRESS BELOW!

Name: Address:

City: State/Province: Zip:

Country: E-mail Address: ________________ Phone Number: ____________

Terms and Conditions: I state I am the person whom I represent myself to be herein, and I affirm the information within this product application is complete and accurate. I represent, warrant and covenant that: I am at least eighteen years of age and have the full right and authority to enter into this Agreement. I do not reside in any country to which import of souvenir design products are prohibited or restricted. I will not use any of the souvenir software designs in any manner prohibited by any laws, restrictions or regulations. My use of the souvenir design prints does not violate any applicable law or regulation of the country, state, or other governmental entity in which I reside and accept full responsibility for the accuracy of the information contained in this application as solely mine. I without reservation or restriction understand fully that you are not an an issuing authority of any governmental entity or agency that is authorized to issue official identification documents, means of official identification, or authentication features. Any original designs are sold for novelty, commemorative, celebratory, commemoratory, dedicatory, in memory, in remembrance, memorial, observing as a memento, or for a collection or exhibit, for decorative purposes, for a dramatic presentation, such as a theater, film, or television production or for for any other recreational, souvenir or amusement purpose, and not for any legal or official purpose, and any souvenir design is not an authentication feature issued by or under the authority of any government, state, political subdivision of a state, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization. I expressly acknowledge you reserve the right to change, modify, update or discontinue any design for any reason and elect to replace any design with an alternate design as updates become available. I understand any souvenir product is not to be used for any official purpose, or to use, deal with or act upon it as if they were genuine, or to induce any person by the belief that it is genuine. I understand the use or mention of any product name, image or trademark on your web site is in no way intended to suggest that any novelty product is an officially issued design as all images are trademarks or registered trademarks of original designers, and are for reference only.

By signing this agreement I attest, affirm, and my signature below serves as evidence that I, the bearer/purchaser, agree to the aforementioned agreement in its entirety and do hereby certify and accept all the terms and conditions contained herein, and agree to be bound by its terms and conditions.

________________ X ____________ ____________
Name Signature Date

NO FEDEX, UPS, USPS EXPRESS OR PRIVATE COURIER ACCEPTED. USE YOUR LOCAL POST OFFICE MAIL OR
Priority Mail or British Royal Express FOR FASTEST SERVICE.

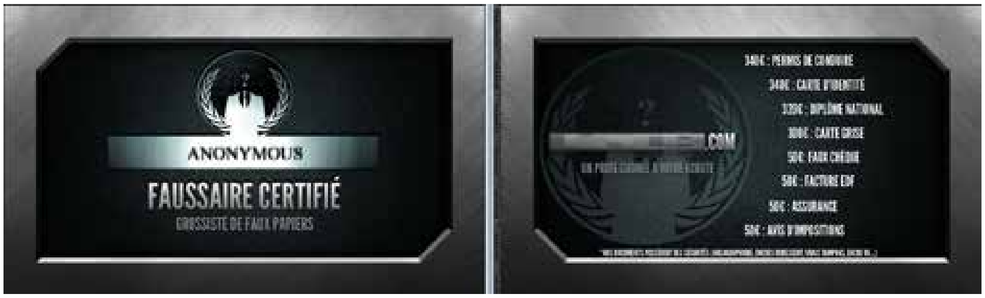
MAIL YOUR ORDER FORM AND PAYMENT TO ADDRESS BELOW: If sending international money order or traveler checks leave the 'Pay to:' / 'Payee:' / 'Pay to the order of:' field blank. Do not enter our mailing address in the payee field

Terms and Conditions: I state I am the person whom I represent myself to be herein, and I affirm the information within this product application is complete and accurate. I represent, warrant and covenant that: I am at least eighteen years of age and have the full right and authority to enter into this Agreement. I do not reside in any country to which import of souvenir design products are prohibited or restricted. I will not use any of the souvenir software designs in any manner prohibited by any laws, restrictions or regulations. My use of the souvenir design prints does not violate any applicable law or regulation of the country, state, or other governmental entity in which I reside and accept full responsibility for the accuracy of the information contained in this application as solely mine. I without reservation or restriction understand fully that you are not an an issuing authority of any governmental entity or agency that is authorized to issue official identification documents, means of official identification, or authentication features. Any original designs are sold for novelty, commemorative, celebratory, commemoratory, dedicatory, in memory, in remembrance, memorial, observing as a memento, or for a collection or exhibit, for decorative purposes, for a dramatic presentation, such as a theater, film, or television production or for any other

> *recreational, souvenir or amusement purpose, and not for any legal or official purpose, and any souvenir design is not an authentication feature issued by or under the authority of any government, state, political subdivision of a state, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization. I expressly acknowledge you reserve the right to change, modify, update or discontinue any design for any reason and elect to replace any design with an alternate design as updates become available. I understand any souvenir product is not to be used for any official purpose, or to use, deal with or act upon it as if they were genuine, or to induce any person by the belief that it is genuine. I understand the use or mention of any product name, image or trademark on your web site is in no way intended to suggest that any novelty product is an officially issued design as all images are trademarks or registered trademarks of original designers, and are for reference only.*
>
> *By signing this agreement, I attest, affirm, and my signature below serves as evidence that I, the bearer/purchaser, agree to the aforementioned agreement in its entirety and do hereby certify and accept all the terms and conditions contained herein, and agree to be bound by its terms and conditions.*

In France, a "new life" pack sells for around €1,500. It contains:

- 1 identity card
- 1 driver's license
- 1 national diploma
- 6 pay slips
- 3 energy invoices
- 3 tax assessments



In underground advertising, this "certified counterfeiter/fake document wholesaler" seeks freelancers and immigration authorities to sell these products. They can earn a monthly salary from €1,500 to €5,000.

Crimeware tools

Last quarter, the Java SE 7 vulnerability CVE-2012-4681 made the headlines. This quarter, it is CVE-2012-5076, a vulnerability in the Java Runtime Environment (JRE) allowing unexpected download and execution of files from a remote host or URL. Blackhole (Version 2.0.2), Sakura, Sweet Orange, and ProPack are among the long list of exploit kits that include this new Java vulnerability.

The following table summarizes some other exploit packs that researchers have discovered for sale during the quarter.

Name	
Propack[4] (October)	• CVE-2006-0003: MDAC • CVE-2010-0188: PDF LibTiff • CVE-2012-0507: Java Atomic • CVE-2012-1723: Java Applet Field • CVE-2012-4681: Java Gondvv • CVE-2012-5076: JAX-WS
Gong Da 1.2[5] (November)	• CVE-2011-3544: Java Rhino • CVE-2012-0507: Java Atomic • CVE-2012-1535 • CVE-2012-1723: Java Applet Field • CVE-2012-1889: MS XML Core • CVE-2012-4681: Java Gondvv • CVE-2012-5076: JAX-WS
KaiXin 1.1[6] (November)	• CVE-2011-3544: Java Rhino • CVE-2012-0507: Java Atomic (removed) • CVE-2012-0754: Flash MP4 (removed) • CVE-2012-1723: Java Applet Field • CVE-2012-1889: MS XML Core • CVE-2012-4681: Java Gondvv • CVE-2012-5076: JAX-WS
Cool 1.1[7] (November)	• CVE-2007-5659 • CVE-2008-2992 • CVE-2009-0927 • CVE-2009-4324 • CVE-2010-0188: PDF LibTiff • CVE-2011-0611 • CVE-2011-2110: Flash AVM • CVE-2011-3402: TTF Font • CVE-2012-1723: Java Applet Field (removed) • CVE-2012-5076: JAX-WS

Name	
CritXPack[8] (November)	• CVE-2006-0003: MDAC • CVE-2010-0188: PDF LibTiff • CVE-2011-2110: Flash AVM • CVE-2011-3544: Java Rhino • CVE-2012-0507: Java Atomic • CVE-2012-1723: Java Applet Field • CVE-2012-4681: Java Gondvv
Styx 2.0[9] (December)	• CVE-2008-0655: Collab.collectEmailInfo • CVE-2010-0188: PDF LibTiff • CVE-2012-0507: Java Atomic • CVE-2012-1723: Java Applet Field • CVE-2012-4681: Java Gondvv • CVE-2012-4969: IE 6-9 • CVE-2012-5076: JAX-WS

Actions against Cybercriminals

During this quarter we noted several successes in law enforcement:

- On October 14, Chinese authorities announced their police units had solved 4,400 recent Internet-related cases, busted 700 cybercriminal gangs, and arrested 8,900 suspects. The police also deleted 1.88 million harmful messages while closing down about 3,500 spam websites.[10] According to researchers with knowledge of the Chinese situation,[11] more than half were porno or other unhealthy content providers or webcam girls, the rest being local small-time cybercrime gangs that target Chinese-language Internet users in China or overseas.
- In November, a 20-year-old man was sentenced in France to one year in prison, six months of which will be probation with an electronic tag, for hacking apps on unlocked Android phones. The hack affected at least 17,000 smart phones and caused €500,000 of damage. The phone victims, after downloading fake applications from illegal platforms, sent, without the user's knowledge, text messages to premium-rate numbers with counterpart codes for gaming and gambling websites forwarded to the hacker.[12]
- In late November Romania's Directorate for Investigating Organized Crime and Terrorism announced the arrest of members of a criminal ring suspected of breaching several computer systems, from which they stole sensitive information, including credit card details. Between December 2011 and October 2012, the crooks are alleged to have sold the details of 68,000 cards in a specialized underground market, earning a profit of US$270,000. In total, the cybercriminals used 500,000 payment cards to perform fraudulent transactions worth over US$25 million.[13]
- In December, investigators led by the Federal Bureau of Investigation and aided by Facebook, busted an international criminal ring that infected 11 million computers around the world and caused more than US$850 million in total losses—one of the largest cybercrime hauls in history. The suspected crooks were arrested in Bosnia and Herzegovina, Croatia, Macedonia, New Zealand, Peru, the United Kingdom, and the United States. It appears they used a strain of malware known as Yahos to assemble a collection of hijacked computers, which the FBI has labeled the Butterfly Botnet, to steal banking details and commit fraud.[14]

Hacktivism

In the first two months of the quarter, Anonymous was kept busy by the Israeli-Palestinian crisis in Gaza and the shutdown of Internet connections in Syria. On November 14, Anonymous started a cyberoffensive against Israel to protest the attacks on Gaza. For several days they defaced and took offline hundreds of websites, such as the Jerusalem Bank, the Israeli Ministry of Foreign Affairs, the Home Front Command, and the Prime Minister's office. Hackers also violated many poorly secured targets, exposing private info of tens of thousands of Israeli citizens and personal data of 5,000 Israeli government officials.[15]

Anonymous also distributed a "care package" named OpIsrael.Care.Package.v2.0. It contained first-aid instructions in English and Arabic, a technical guide with information on how to circumvent authoritarian Internet shutdowns, and a Vidalia bundle that could be used to hide the IP address and location of a computer.[16] Furthermore, the Telecomix group reiterated its Syrian operation, claiming it offered an independent dial-up infrastructure more difficult for Israeli security services to observe.

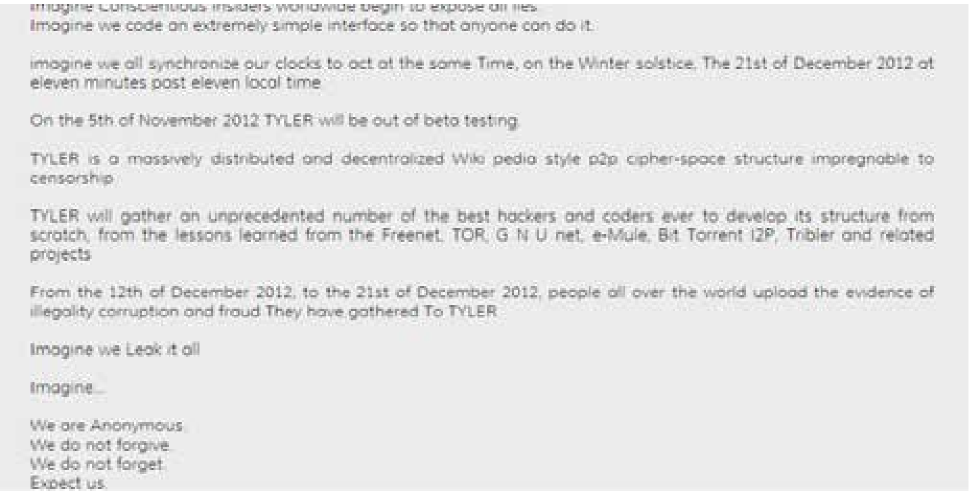
In reply to these anti-Israeli attacks, the hacker Yourikan leaked the database from PALNET, which is said to be one of the largest ISPs in Palestine. Data from hundreds of credit cards was disclosed on the Internet. This last attack demonstrates that cyberpatriots are active in both camps, sometimes using the methods of cybercrime.

On November 30, a press release announced that Anonymous had made an "exhaustive analysis" and declared that Syrian President Bashar al-Assad was behind the country's Internet blackout that began the day before.[17] A long list of targets including Syrian embassy servers was suggested in the statement. But unlike in Israel, it seems the attacks did not reach the level that Anonymous hoped for.

In December, the Westboro Baptist Church planned to picket the funerals of victims of the Sandy Hook (Connecticut) Elementary School shootings. Anonymous launched distributed denial of service (DDoS) attacks and leaked personal information about the church group. A text file with the names, phone numbers, and social security numbers of numerous supposed members or close family members was posted on Pastebin. More than 100,000 people have looked at the Pastebin file. This was one of a broad array of actions carried out in the United States that has reinvigorated, at least for a time, the Anonymous movement.

On October 23, some Anonymous members defaced a UK police web forum and claimed they stole the private email addresses of various current and retired officers.[18] Earlier that month, they defaced some other police websites as part of Operation Jubilee, which along with OpVendetta2012 aimed to rally millions of people to the British Parliament on November 5 (Guy Fawkes Day) for a large demonstration to cancel debt and end the economic crisis.[19] Wearing masks, several hundred demonstrators gathered outside the building.[20]

This quarter, YouTube became saturated with hundreds of Project Mayhem's call-to-action videos, which mainly appeal to those who want to expose corruption or support the hacktivist cause. As reported by the Examiner.com,[21] it may be hard to determine who is associated with the Anonymous hacktivist group and who is part of other "establishment"-related entities set up to gather information on participants and entrap those who are actively leaking information. Their data was available via TYLER,[22] a Wikipedia-style peer-to-peer network.[23]



Imagine Conscientious insiders worldwide begin to expose all lies.
Imagine we code an extremely simple interface so that anyone can do it.

imagine we all synchronize our clocks to act at the same Time, on the Winter solstice. The 21st of December 2012 at eleven minutes past eleven local time

On the 5th of November 2012 TYLER will be out of beta testing.

TYLER is a massively distributed and decentralized Wiki pedia style p2p cipher-space structure impregnable to censorship.

TYLER will gather an unprecedented number of the best hackers and coders ever to develop its structure from scratch, from the lessons learned from the Freenet, TOR, G N U net, e-Mule, Bit Torrent I2P, Tribler and related projects

From the 12th of December 2012, to the 21st of December 2012, people all over the world upload the evidence of illegality corruption and fraud They have gathered To TYLER

Imagine we Leak it all

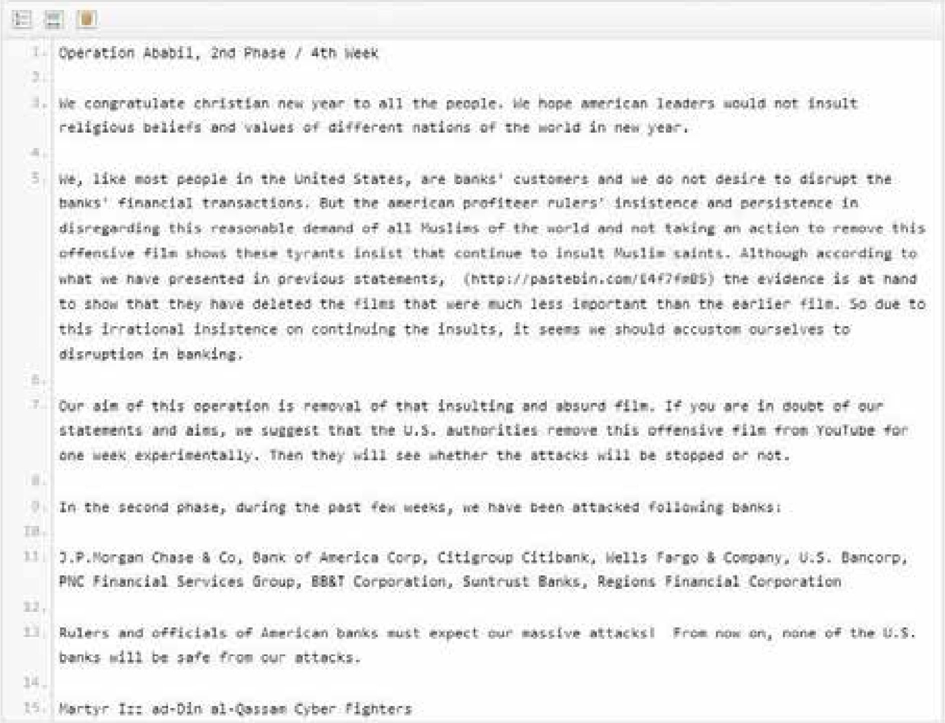
Imagine...

We are Anonymous.
We do not forgive.
We do not forget.
Expect us.

Cyberextremism: Terrorism and the Internet

In our previous quarterly report, we briefly introduced the group Izz ad-Din al-Qassam Cyber Fighters, after they claimed responsibility for various cyberattacks launched in September on US banks and financial-services companies.

Those actions are now known as part of Operation Abadil. This quarter, calling themselves al-Qassam Cyber Fighters, the group posted claims and threats under Pastebin.



Operation Ababil, 2nd Phase / 4th Week

We congratulate christian new year to all the people. We hope american leaders would not insult religious beliefs and values of different nations of the world in new year.

We, like most people in the United States, are banks' customers and we do not desire to disrupt the banks' financial transactions. But the american profiteer rulers' insistence and persistence in disregarding this reasonable demand of all Muslims of the world and not taking an action to remove this offensive film shows these tyrants insist that continue to insult Muslim saints. Although according to what we have presented in previous statements, (http://pastebin.com/E4f7fmB5) the evidence is at hand to show that they have deleted the films that were much less important than the earlier film. So due to this irrational insistence on continuing the insults, it seems we should accustom ourselves to disruption in banking.

Our aim of this operation is removal of that insulting and absurd film. If you are in doubt of our statements and aims, we suggest that the U.S. authorities remove this offensive film from YouTube for one week experimentally. Then they will see whether the attacks will be stopped or not.

In the second phase, during the past few weeks, we have been attacked following banks:

J.P.Morgan Chase & Co, Bank of America Corp, Citigroup Citibank, Wells Fargo & Company, U.S. Bancorp, PNC Financial Services Group, BB&T Corporation, Suntrust Banks, Regions Financial Corporation

Rulers and officials of American banks must expect our massive attacks! From now on, none of the U.S. banks will be safe from our attacks.

Martyr Izz ad-Din al-Qassam Cyber fighters

The Wells Fargo website was struck with high traffic volumes on December 18 and 19 that limited or prevented access by online customers.[24] This may have been an attack by al-Qassam Cyber Fighters.

On October 22, the United Nations Office on Drugs and Crime launched a publication to provide practical guidance to member states for more effective investigation and prosecution of terrorist cases involving the use of the Internet. "The Use of the Internet for Terrorist Purposes" explains how terrorist groups and their supporters use the Internet to recruit, finance, spread propaganda, train, and incite followers to commit acts of terrorism.[25]

Rumors claimed the film "Salil al-Sawarim 3" was scheduled to be released in December to promote the return of Al Qaeda in Iraq. Online jihadists had discussed the release for more than a month, and had shared images and footage from the production.[26] It appears that DDoS attacks on official websites of Al Qaeda disrupted its release.

In December, the Iranian media announced the country had used cyberdefense techniques in its Velayat 91 naval military exercises.[27] They claimed the exercises covered a vast area, including the Strait of Hormuz, the Sea of Oman, the northern Indian Ocean, the Gulf of Aden, and Bab-el-Mandeb Strait. A senior Iranian commander added that "during one of the practices of the second day of the drills, aggressive forces launched a cyberattack against the computer network of defensive forces in order to infiltrate the network and hack information or spread viruses."

About the Authors

This report was prepared and written by Xiaobo Chen, Toralv Dirro, Paula Greve, Haifei Li, François Paget, Vadim Pogulievsky, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Dan Sommer, Bing Sun, 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
http://www.mcafee.com/us/resources/reports/rp-operation-high-roller-revisited.pdf

[2] http://www.mcafee.com/us/resources/white-papers/wp-analyzing-project-blitzkrieg.pdf

[3] http://home.mcafee.com/virusinfo/global-virus-map

[4] http://malware.dontneedcoffee.com/2012/11/meet-propack-exploit-pack.html

[5] http://eromang.zataz.com/2012/11/24/gong-da-gondad-exploit-pack-add-adobe-flash-cve-2012-1535-support/

[6] http://eromang.zataz.com/2012/12/05/kaixin-exploit-kit-evolutions/

[7] http://eromang.zataz.com/2012/12/02/cool-exploit-kit-remove-support-of-java-cve-2012-1723/

[8] http://malware.dontneedcoffee.com/2012/11/meet-critxpack-previously-vintage-pack.html

[9] http://malware.dontneedcoffee.com/2012/12/crossing-styx-styx-sploit-pack-20-cve.html

[10] http://www.zdnet.com/china-busts-700-cybercriminal-gangs-7000005742/

[11] http://www.linkedin.com/groupItem?view=&type=member&gid=2677290&item=177364070&commentID=100965887&trk=eml-anet_dig-b_pd-pmr-cn&ut=0xwp-Je1NICls1#commentID_100965887

[12] http://www.bbc.co.uk/news/world-europe-19994944

[13] http://www.diicot.ro/index.php/arhiva/782-comunicat-de-presa-27-11-2012

[14] Don't confuse the Yahos/Butterfly botnet with the Mariposa/Butterfly botnet dismantled in December 2009. http://www.fbi.gov/news/pressrel/press-releases/fbi-international-law-enforcement-disrupt-international-organized-cyber-crime-ring-related-to-butterfly-botnet

[15] http://securityaffairs.co/wordpress/10428/intelligence/opisrael-all-about-offensive-of-anonymous-against-israel.html?goback=%2Egde_2677290_member_187642368

[16] http://www.vice.com/read/the-gaza-strip-cyber-war

[17] http://www.huffingtonpost.com/2012/11/30/anonymous-declares-war-syrian-government-websites_n_2218447.html

[18] http://www.telegraph.co.uk/technology/internet/9631245/Anonymous-hacks-into-private-emails-of-police-officers.html

[19] http://news.softpedia.com/news/Anonymous-to-Initiate-Operation-Jubilee-on-November-5-2012-Video-286821.shtml

[20] Some photos are available here: http://www.demotix.com/news/1575001/anonymous-mark-5th-november-march-parliament#media-1574926

[21] http://www.examiner.com/article/anonymous-launches-multiple-leak-platforms-under-operation-mayhem-tyler

[22] http://anonnews.org/press/item/1783/

[23] http://anonukire.wordpress.com/2012/12/23/tyler-live-9-pm-gmt-23-december-2012/

[24] http://www.bizjournals.com/washington/morning_call/2012/12/wells-fargo-facing-possible-cyber-attack.html

[25] http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[26] http://www.wtop.com/807/3163232/Al-Qaida-hit-by-cyber-attack

[27] http://www.presstv.ir/detail/2012/12/30/280855/cyber-defense-used-in-iran-naval-drills/

McAfee®
An Intel Company

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

60058rpt_quarterly-threat-q4_0213_fnl_ETMG