CYREN

INTERNET THREATS
TREND REPORT

JULY 2014

ATTACKS ON ANDROID PREDOMINATE

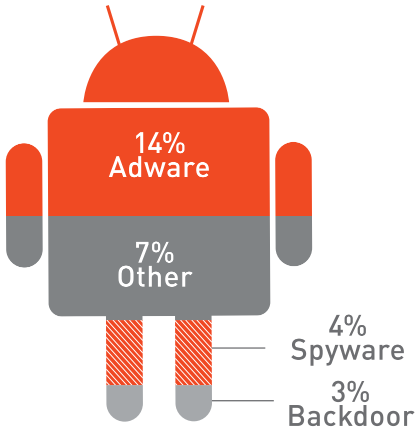
While attacks on the Android operating system continued to predominate this quarter, the big news is the debut of the first type of Android ransomware, which locks valuable user files, such as photos and documents, using strong encryption. PC-focused malware also continued its dogged march, with CYREN analysts observing the continued use of PDFs embedded with malware code (including variants using a Dropbox link), as well as the exploitation of a year-old MS Office vulnerability; phishing trends emphasize financial gain, focusing on global banks and the World Cup; and spam levels remain essentially unchanged at an average of 55 billion emails per day for the quarter, although June experienced a noticeable drop to the lowest level in five years.

Further Report Highlights:
"Pump-and-dump" stock spam featured heavily, accounting for 17% of all spam emails this quarter, and Spain and Argentina continue to lead as spam producing countries. And, for the first time in four years, India lost the top "zombie country" spot, relinquishing the crown to the Russian Federation.

72%

OF ALL ANDROID MALWARE IN Q2 WAS SMS TROJAN.

The remaining 28% breaks down as follows:

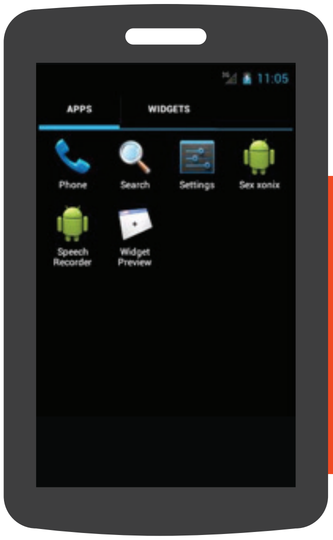


Android malware took a step forward (or a step back, depending on how you look at it), with the appearance of the first true ransomware. In addition, malware focusing on iBanking applications continued to plague Android users. CYREN experts found that 72% of all Android malware was SMS Trojan. The remaining 28% broke down as follows: 14%—adware, 7%—other (such as banking or fake antivirus), and 4%—spyware/monitor, and 3%—backdoor.

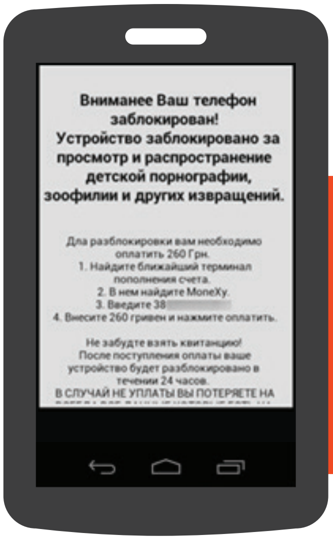
Android Ransomware Debuts

PC-based ransomware made the news repeatedly in 2013 but this form of extortion had not threatened mobile users until now. Ransomware typically blocks access to user files using very strong encryption. Users are then forced to pay for their files to be unencrypted or see them disappear forever.

The first version of Android ransomware appeared in May, but lacked a true encryption threat. In this instance, the malware takes over the phone and displays a message (claiming to be from the "Internet police") over any app that is subsequently launched on the device, stating that the user had been



<< The application in the Apps drawer



Вниманее Ваш телефон заблокирован!
Устройство заблокировано за просмотр и распространение детской порнографии, зоофилии и других извращений.

Для разблокировки вам необходимо оплатить 260 Грн.
1. Найдите ближайший терминал пополнения счета.
2. В нем найдите MoneXy.
3. Введите 38[redacted]
4. Внесите 260 гривен и нажмите оплатить.

Не забудте взять квитанцию!
После поступления оплаты ваше устройство будет разблокировано в течении 24 часов.
В СЛУЧАЙ НЕ УПЛАТЫ ВЫ ПОТЕРЯЕТЕ НА

<< After the application is launched, this screen appears

watching child pornography and demanding a fine to use the device again.

The real thing appeared a month later, actually encrypting files on the device's secure digital (SD) card and blocking phone use by displaying a similar message stating that the user had been watching child pornography and demanding a fee to decrypt the blocked files. The Simplocker ransomware is hidden in an app that presents itself as a pornography player under the name "Sex Xonix". After launching the app, a message appears on the screen accusing the user of watching and distributing child pornography (among "other perversions") and demands payment to decrypt the user's now encrypted Android files. The user is asked to pay 260 Ukraine Hryvnia (UAH), around $22, via MoneXy, a money transferring service used mostly in Russia and Ukraine.

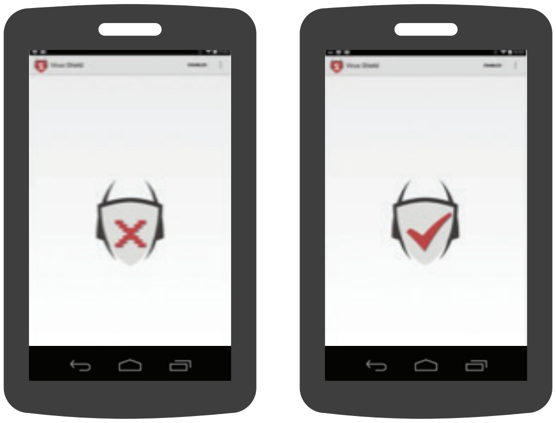
It appears that this particular cybercriminal is at least attempting to provide good customer service. After payment is made, the Russian message reminds the Android victim "Don't forget to take a receipt!"

Android iBanking Malware

CYREN security experts have observed quite a few fake banking applications targeting Android users over the last few months. Detected by CYREN's AntiVirus as Android "OS/Agent.HJ", the iBanking malware collects sensitive data, including text messages, recorded audio, and banking information, from Android phones. Once installed, the SMS/spyware also intercepts phone calls and sends text messages to any number, and uploads the victim's personal Android information directly to the attacker. According to researchers at RSA, the app also works in tandem with PC-based malware to intercept SMS codes sent by banks to authenticate access to banking sites online.

Fake Antivirus App Does Nothing

A "Virus Shield", priced at $3.99 in the Google Play store and providing no antivirus security, sold 30,000 copies in April. After downloading and analyzing the code, security experts determined that the application did absolutely nothing; fortunately, it also did no harm to the data on the users' Android phones. When launched it simply showed two different icons. Google fully refunded money to all the buyers and provided them with a Play Store credit. News reports later quoted the app's developer as claiming that the app had been mistakenly released and was an early placeholder. This situation illustrates the struggles associated with scanning and evaluating the sheer number of Android apps appearing on the market.



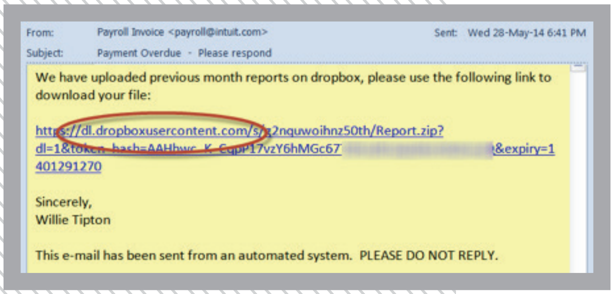
"Virus Shield" sold for $3.99, but only displayed two different icons.

Dangerous PDFs and Year-old MSOffice Malware Resurfaces

Malware criminals are, if anything, persistent. In the some of the latest malware to affect PCs, CYREN security analysts detected malware distributed via the PDF's built-in scripting capabilities. And, although patched by Microsoft, malware targeting the CVE-2010-3333 vulnerability continues to pop up.

To PDF or not to PDF

In the 2nd quarter, CYREN observed cybercriminals using both real and phony PDF files and Dropbox to distribute malware. In one version (the "Gameover" variant of Zbot), malware arrives in the victim's email inbox as a bill supposedly from a large British energy provider. The file "Eonenergy-Bill-29052014.zip," contains an executable file (detected as W32/Zbot.BXN) that is represented by a standard PDF icon. Gameover uses a P2P command-and-control (C&C) network to transfer commands (such as downloading more malware) between the infected system and the network. The malware also uses pseudo-random domain names and attempts connections with each of these to download configuration files.



From: Payroll Invoice <payroll@intuit.com>
Sent: Wed 28-May-14 6:41 PM
Subject: Payment Overdue - Please respond

We have uploaded previous month reports on dropbox, please use the following link to download your file:

https://dl.dropboxusercontent.com/s/z2nquwoihnz50th/Report.zip?dl=1&token_hash=AAHbwc_K_CqpP17vzY6hMGc67[redacted]&expiry=1401291270

Sincerely,
Willie Tipton

This e-mail has been sent from an automated system. PLEASE DO NOT REPLY.

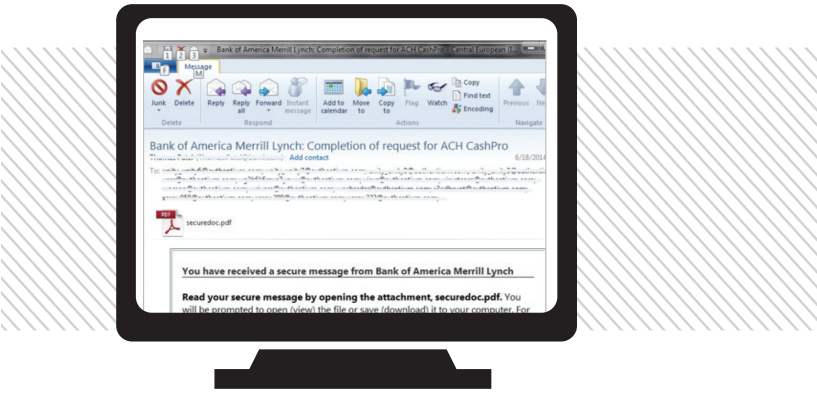
Dropbox Malware

In a variation on this same theme, malware distributors spread similar Zbot malware using Dropbox. The Dropbox links were included in payroll-related emails. Dropbox disabled the links within a few hours.

The Friendly PDF Really Can Be Dangerous

Despite general beliefs to the contrary, PDF files can be embedded with executable malware. While this has been a known threat for several years, many computer users dismiss suggestions that PDFs can be dangerous since they are "just text and images." However, it is entirely possible to insert malicious code into a PDF document using built-in scripting functions.

Users of Bank of America ACH CashPro online services recently found this out, when an email purportedly from Bank of America reached user inboxes. The email message contained a link that pointed to a valid Bank of America site to legitimize the attached (but malicious) PDF document. When opened, the PDF attachment attacks a known vulnerability (CVE-2010-0188) of Adobe Reader. The embedded PDF script validates the target Adobe Reader version (9.303 through 11.001). If successfully exploited, the malicious PDF then executes an embedded shellcode that downloads another malicious executable "backdoor" from the following link (http://88.{--masked---}5.44/images/banniers1/Andr.exe) which CYREN detected as W32/Androm.AQ. New malware is executed and installed on the user's system, enabling an attacker to take full control of the user's system from any location, at any time, without the user's knowledge.



Bank of America Merrill Lynch: Completion of request for ACH CashPro

[redacted]

To: [redacted]

You have received a secure message from Bank of America Merrill Lynch

Read your secure message by opening the attachment, securedoc.pdf. You will be prompted to open (view) the file or save (download) it to your computer. For

Many Bank of America ACH CashPro users were victims of this malware scheme.

Old MSOffice Vulnerability Still Exploited by Cybercriminals

Despite being patched by Microsoft over a year ago, the CVE-2010-3333 vulnerability is still targeted by cybercriminals, primarily because some users have not applied the MS10-087 update. The exploit sample typically arrives as an attachment file with a ".doc" extension. CYREN experts have observed numerous different filenames for the attachment including "traking_doc_MW421330771CA.doc," "aircanada_eticket_[random_number].doc," and "President Obama's Speech.doc." The exploit sample dismantles the pFragments structure in the RTF to avoid detection. Just one more reason to keep antivirus definitions up-to-date and apply the latest software updates.

Global Banking and World Cup Criminals

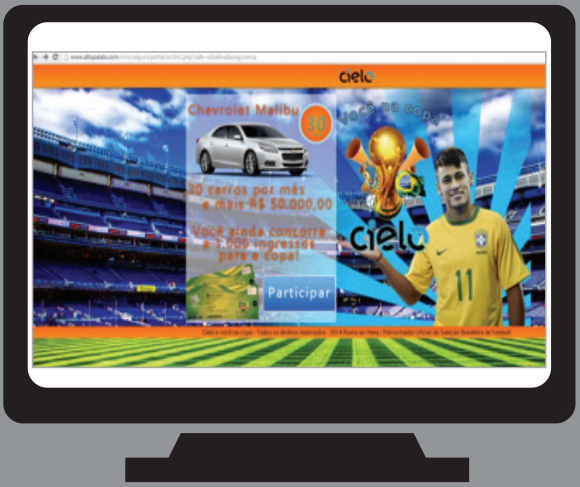
Phishing continued unabated this quarter, with CYREN researchers observing the financial industry and World Cup as the focus of several schemes.

No Corner of the Banking Globe is Safe from Phishing Criminals

From Italy to India, few banking customers were spared the trouble of phishing emails this quarter. Whether it was large-scale, global brands such as American Express, Bank of America, or Barclays, or country-specific financial institutions such as Natwest (Britain), Danske Bank (Denmark), Swedbank and SEB (Sweden), Bank of India (India), Credem (Italy), or Hypovereinsbank (Germany), cybercriminals continued to try to find ways to gain access to personal and corporate financial data.

Details, Details, Details

The enticement of prizes (such as a Chevy Malibu car) and the smiling face of Brazilian football star Neymar, was enough to convince users of Brazil's largest credit and debit card operator, Cielo, to provide copious amounts of personal and financial data to cybercriminals through this phishing scheme.


cielo
Chevrolet Malibu
30
Você na copa
30 carros por mês e mais R$ 50.000,00
Você ainda concorre a 1.000 ingressos para a copa!
Participar
cielo
11

Key Spammer Relationships, Quarterly Spam Levels, and Pump and Dump Stock Spam.

Second quarter highlights include a new research study that examines the relationship between the email address harvester, the botmaster, and the spammer; a noticeable increase in pump-and-dump stock spam; and the lowest spam distribution level in five years during the month of June, despite an overall daily average for the quarter that remains essentially unchanged from Q1.

Trust Among Thieves

Overview:
The Harvester, the Botmaster, and the Spammer: On the Relations Between the Different Actors in the Spam Landscape; by Gianluca Stringhini, Oliver Hohlfeldy, Christopher Kruegel, and Giovanni Vigna of the Department of Computer Science, UC Santa Barbara and Aachen University in Germany. Published in ASIA CCS '14 Proceedings of the 9th ACM symposium on Information, computer and communications security, pages 353 – 364; ACM New York, NY, USA ©2014..

A paper presented in June at the 9th Annual ACM Symposium on Information, Computer and Communications Security provides in-depth research into the relationship between three key contributors to the spam process: the harvester who creeps around the Web collecting valid email addresses; the botmaster, who controls the Internet-connected programs that distribute the spam; and the spammer—the communicator who develops emails that both evade anti-spam filters and entice the reader. The research suggests that the roles are intrinsic to each other, with the profitability of a spam campaign contingent upon "a reliable email list, filter-busting content, and a botnet for distribution". Spammers, we learn, establish a form of customer and brand loyalty with the harvesters and botmasters.

Top 3 countries who host the largest number of harvesters*:

Germany	**73%**
China	**9%**
Spain	**5%**

**Within the dataset analyzed.*

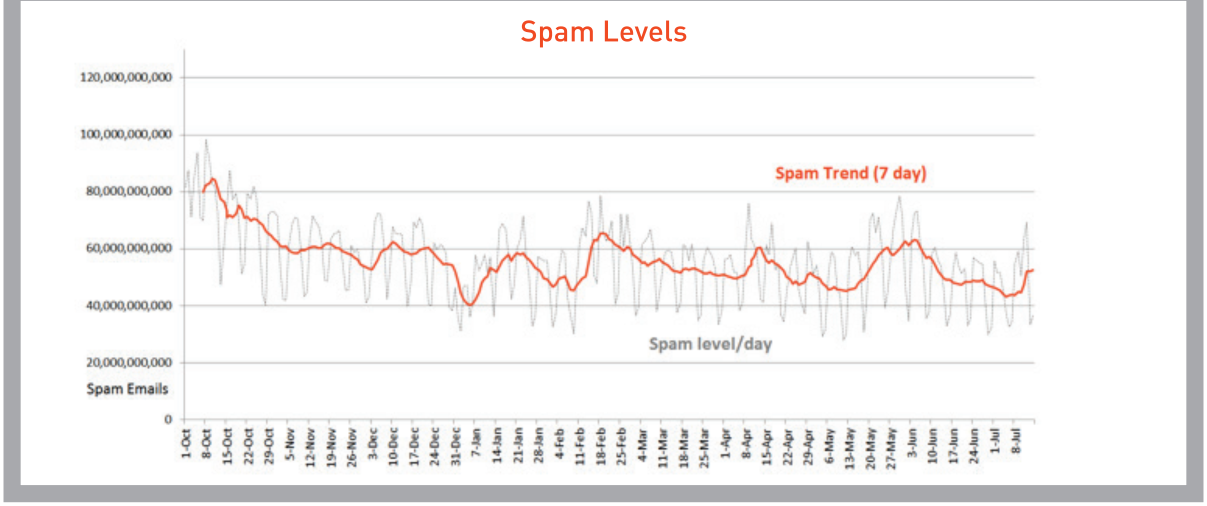
To conduct their research, the authors built a spam trap that contained a large number of email addresses, created specifically for the purposes of the experiment. The web pages with these email addresses were advertised and the research team logged and analyzed those who accessed the email addresses and the botnet connections made to the mail server. The researchers learned that:

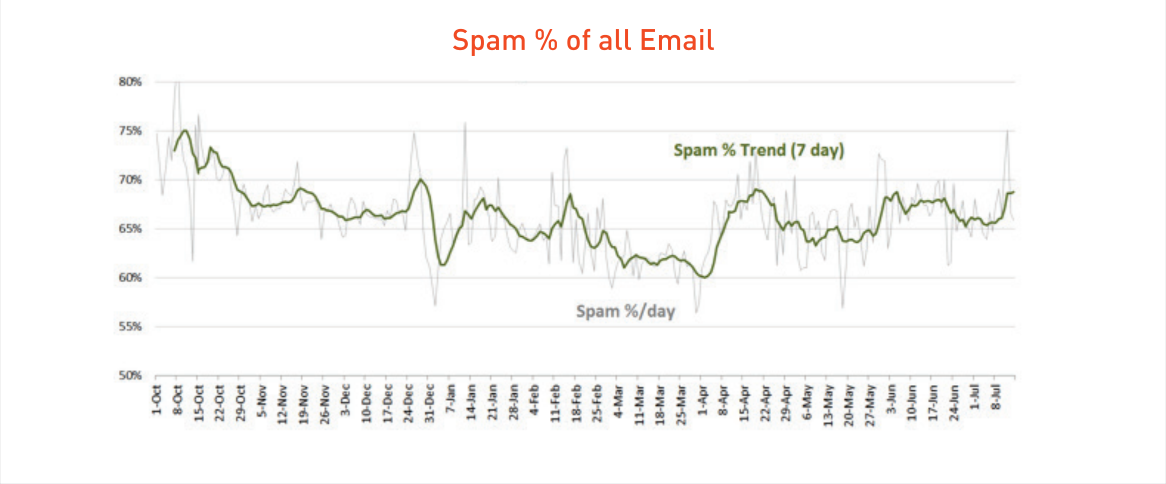
- Harvesters may have extremely well-developed processes and black market relationships, as two harvesters in particular sent spam within five days of harvesting the email addresses.
- Harvesters may use search engines as a proxy to either 1) hide their identity or 2) optimize the harvesting process.
- Within the dataset analyzed, Germany hosted the largest number of harvesters (73%), followed by China (9%), and Spain (5%), although this is likely specific to the researchers' experience and not necessarily reflective of global harvester locations.
- Spammers tend to stick with a single list of email addresses for long periods, even years.
- Successful spammers may finesse or expand their purchased lists by adding generic email addresses (such as info@, media@, or admin@).
- Spammers may have target markets. Researchers did not receive any pharmaceutical spam via the harvested email addresses. Considering that pharmaceutical spam continues to predominate spam topics worldwide (although some reports suggest that this type of spam is on the decline), the researchers speculate that pharmaceutical affiliate programs could be harvesting their own email addresses and not purchasing them on the black market.
- Spammers typically rent a single botnet, with only a fraction setting up their own mail transfer agents (MTAs).
- Spammers are not necessarily influenced by the country the bot is located in; the physical location of the bot has little influence on the overall spam performance.

The researchers cite spamming pipeline bottlenecks and fingerprinting a particular botnet's email engine as opportunities for identification and the development of future threat mitigation.

Monthly Spam Levels Fluctuate; Overall Average Remains Steady

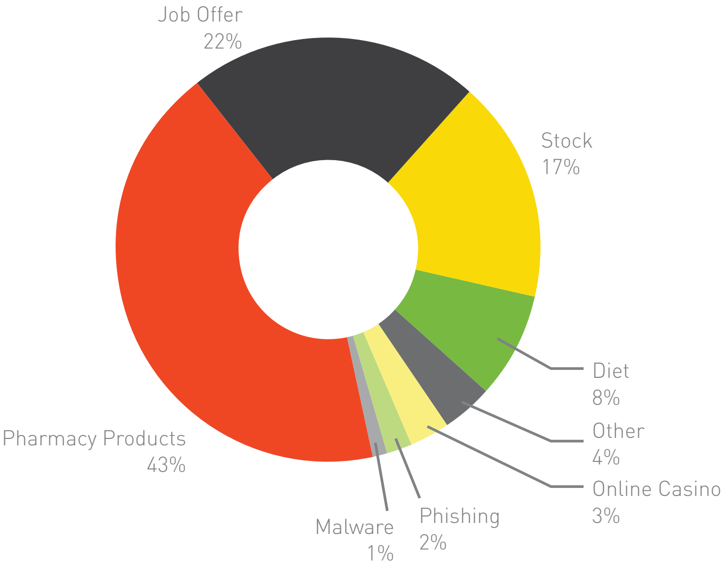
During the 2nd quarter, while overall average spam levels remained essentially unchanged, from a daily average of 54 billion in Q1 to 55 billion in Q2, there were a number of dramatic peaks and valleys. April started off remaining fairly steady with an average of 54 billion spam emails sent daily. In the month of May, spam jumped dramatically to 60 billion, followed by a five-year low in June at 49 billion. (CYREN security analysts speculate that the noticeable June drop may be related to several well-publicized botnet takedowns.) Spam accounted for 66% of all emails during the 2nd quarter of 2014.





2nd Quarter Spam Topic Trends

Pharmaceutical spam still leads the pack this quarter, accounting for 43% of all total spam. Job offers hold steady at number two, with 22% of total spam. The notable shift in topics is the sudden increase in "pump-and-dump" stock spam, accounting for 17% of all spam emails sent in the 2nd quarter. Diet spam also increased noticeably from last quarter, accounting for a total of 8%, compared with only 1% previously. Spam advertising online casinos and gambling also made it onto the list this quarter at 3%.

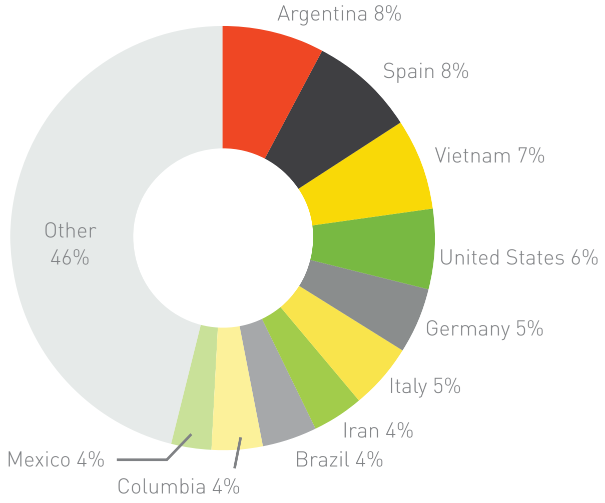


Wolves of the Wall Street Internet

It seems that cybercriminals can't get enough of the "pump-and-dump" stock spam, with several versions appearing in the 2nd quarter, including one for a "bioceutical" penny stock. In this case, the spammer purchased 417,000 shares at $0.19 per share, spending $79,230. The spammer then commenced the spam email campaign, suggesting that the stock "RCHA" was on the move. The spammer even attempted to legitimize the spam by adding well-known investor and news outlet logos. As with any pump-and-dump stock scam, unsuspecting and naïve investors purchase the stock, causing the stock's value to rise. The spammer then sells off his initial purchase, making a tidy profit. This pump-and-dump schemer's choice of pseudonym, "Oakmont Stratton", particularly amused CYREN researchers. The topic of the recent Academy Award-nominated film, The Wolf of Wall Street, Stratton Oakmont was the name of a firm whose owners were prosecuted and found guilty in the 1990s for stock and investment fraud.

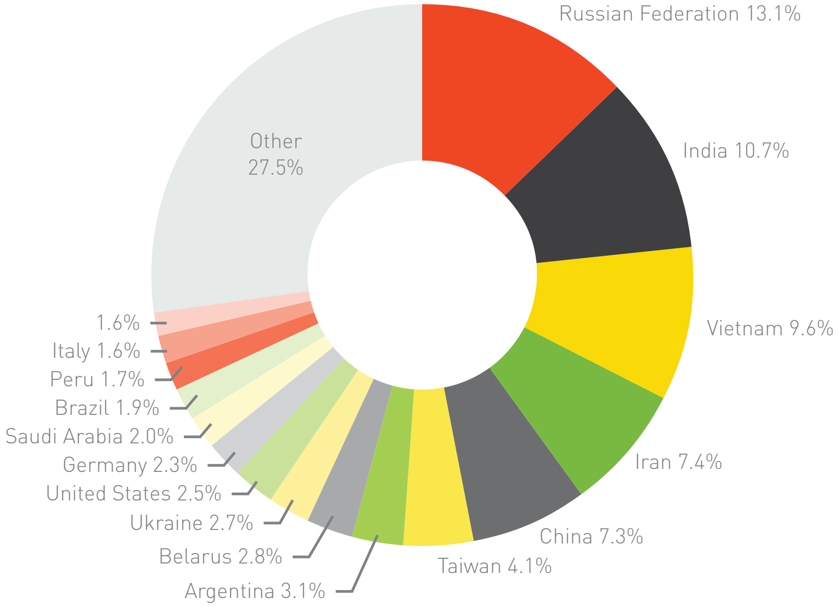
Countries of Origin

While Spain (8%), Argentina (8%), and the United States (6%) continued to be among the leading spam-producing countries this quarter, the surprise was Vietnam, which accounted for 7% of all spam. Germany rounded out the top five, producing 5% of all spam. Noticeably missing among the leaders this quarter was India.



Zombie Countries

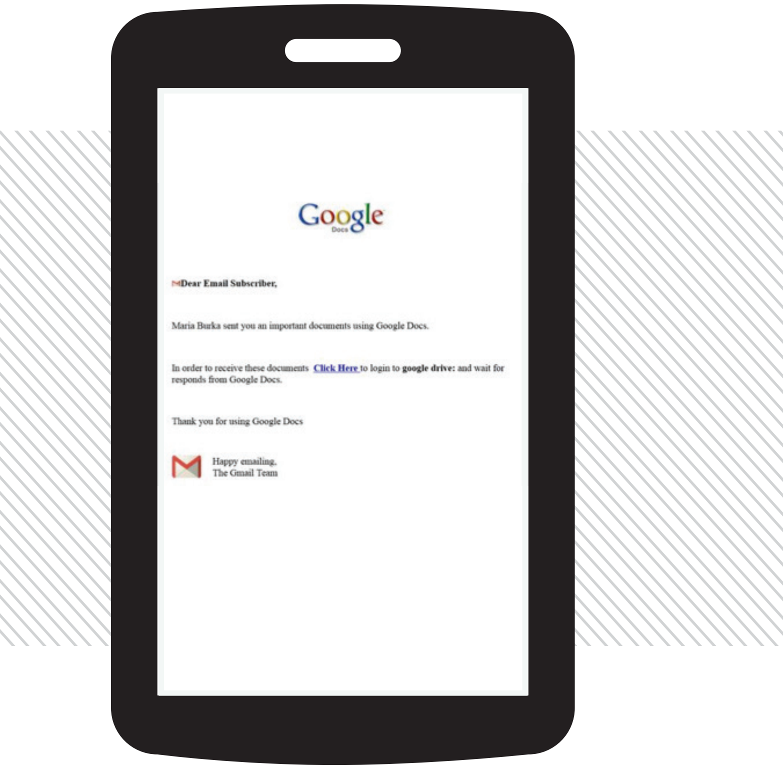
The Russian Federation led the zombie countries at 13.1%, following by India at 10.7%. Interestingly, this is the first time India has been deposed from the top spot in over four years. Peru joined the list this quarter, while Spain fell off.



AND FINALLY...

Want to save money on hosting fees and add legitimacy to your phishing-malware-spam campaign? Incorporate a real corporate logo and link that logo back to a well-known Internet security blog!

CYREN researchers came across this scheme in the 2nd quarter, in which a cybercriminal used a typical phishing email in the form of a "Google Doc". The Google logo at the top actually linked back to a legitimate Internet security blog called http://www.onlinethreatalerts.com/.



Dear Email Subscriber,

Maria Burka sent you an important documents using Google Docs.

In order to receive these documents Click Here to login to **google drive:** and wait for responds from Google Docs.

Thank you for using Google Docs

Happy emailing,
The Gmail Team

CYREN

ABOUT CYREN

CYREN is the global leader in information security solutions for protecting web, email, and mobile transactions. Our GlobalView Security Lab continuously innovates our cloud-based threat detection and proactive data analytics to provide comprehensive security solutions for businesses of all sizes. Our award-winning, patented technologies and global security platform increase the value and profitability of our partners' solutions as CYREN email, web, and antivirus capabilities protect over 550 million end users in 190 countries.

www.CYREN.com