INTERNET THREATS TREND REPORT

APRIL 2014

PHISHING ATTACKS CONTINUED TO BE PROMINENT IN THE FIRST QUARTER OF 2014, INCLUDING THE TRADITIONAL TARGETS OF PAYPAL AND APPLE, AS WELL AS A DISTURBING NEW WAVE OF ATTACKS USING RESIDENTIAL IP ADDRESS SPACE AND PERSONAL COMPUTERS TO INSTALL AND HOST PHISHING SITES.

A new and improved version of Android "notcom" malware has resurfaced; spam levels continued to drop; spam topics focused on pharmaceuticals and jobs, with particularly creative ways to sell new diet aids. The first FIFA World Cup Soccer spam is hitting inboxes; and Western Europe led the way this quarter collectively generating almost 1/5th of the world's spam.

PHISHING TRENDS

ANALYZING TRENDS THROUGH CYREN'S NEW PHISHING FEED

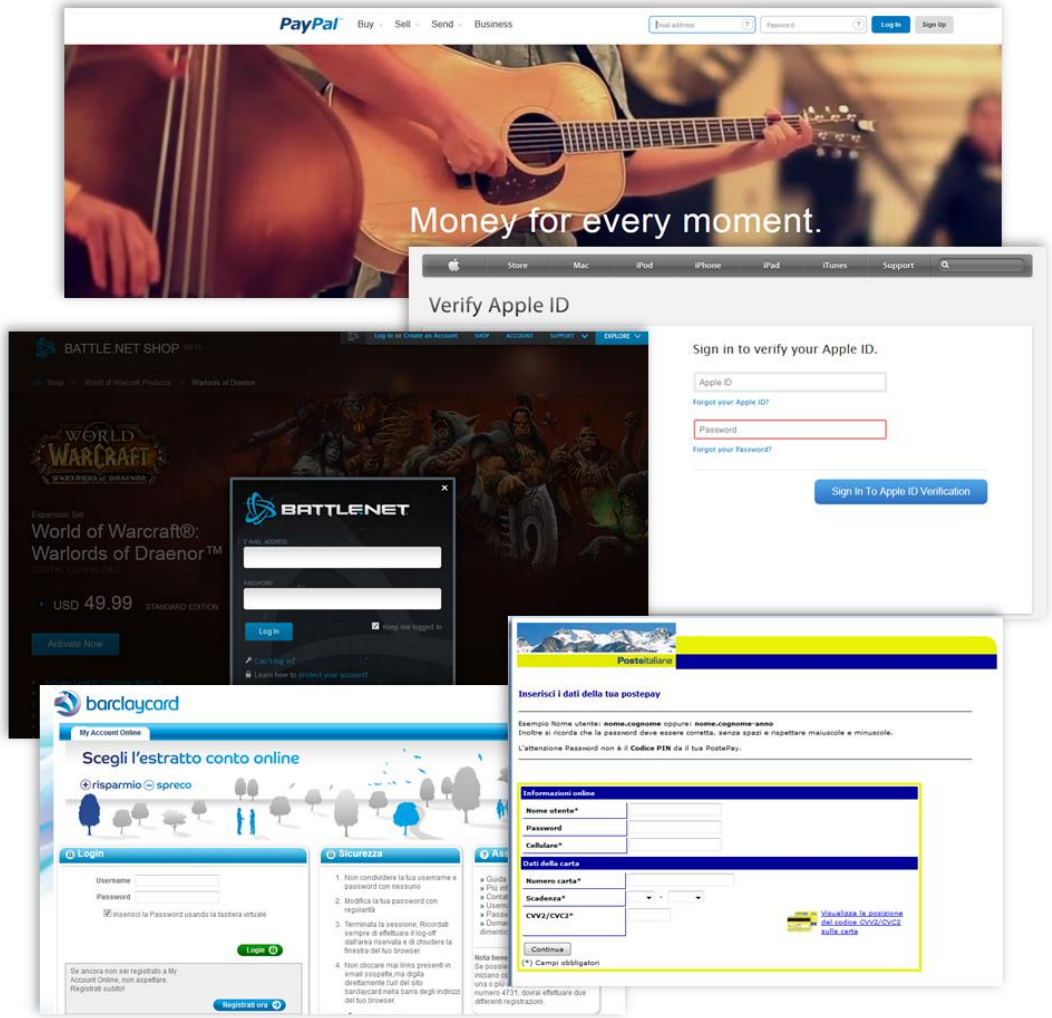
In April 2014, CYREN released its new phishing URL feed. Curious about the trends, we looked at a two-week sample. The most notable result was an approximate 73% increase in the number of phishing URLs/sites related to PayPal (from ~750/day in Q4 of 2014 to ~1300/day in Q1 of 2013).

Below are the top six most frequently 'phished' properties:

Rank	Site	Phishing Purpose	# of Phishing URLs/Sites Over 2-Week Study
1	**PayPal**	Access to financial data and assets, identity (name, address, and social security number), email, and passwords	18,600; up by more than 70% from 2013 data
2	**Apple**	Apple IDs, billing information (credit card #s, expiration dates, names, addresses)	2, 261
3	**Poste Italiane**—Italy's largest postal service providing financial and payment services.	Access to financial data, assets, identity (name, address), email/user ID and passwords	1,720
4	**Barclays Bank**	Access to financial data, assets, identity (name, address), user ID/email, and passwords	830
5	**Battle.net**—Online gaming site	User name/ID, passwords, billing information	436
6.	**Sparkasse**— German Savings Banks Finance Group (Sparkassen-Finanzgruppe), a sub-sector of the German banking system, with 431 savings banks using the Sparkasse brand	Access to financial data, assets, identity (name, address), user ID/email, and passwords	180

A sample of the destination sites illustrates the typically convincing copies of trusted login pages.

Copyright© 2014 CYREN



PHISHLABS THREAT ANALYSIS: PHISHING @ HOME

PhishLabs (www.phishlabs.com), a CYREN partner through our Security Alliance, recently released an in-depth study examining a new wave of phishing attacks using the residential IP address space and personal computers to install and host phishing sites.

By scanning the residential service IP address space, attackers exploit individuals who have (1) enabled the remote desktop protocol (RDP) service on Microsoft Windows and (2) use a weak password. The attackers then install PHP Triad (free, open-source, web server software) and upload a number of different phishing pages. Links to the phishing sites (usually financial institutions and payment websites) are sent out via spam email messages. As pointed out by PhishLabs, this trend is highly significant, as phishing sites hosted on compromised personal home computers are more likely to have a longer lifespan than those located in a traditional hosting environment. (The hosting provider's terms of service typically enables them to quickly shut down malicious sites; Internet service providers (ISPs), on the other hand, have little control over customer-owned home computers linked to the ISP by residential broadband networks.)

While RDP is turned off by default on desktops with modern versions of Windows, PhishLabs found that the many individuals still use RDP as a free, no third-party way to remotely access at-home systems. According to the report, few of these recent phishing attacks suggested "evidence of social engineering to get the user to enable RDP or create

Remote Assistance invitations; exploits with shellcode or malware that enables RDP; or attacks that target other possible weaknesses in RDP configurations such as Restricted Admin mode in RDP 8.1." In every attack analyzed, attackers gained access only through RDP-enabled connections and weak passwords.

The full report is available here: http://blog.phishlabs.com/phishers-set-up-sites-on-residential-broadband-hosts

PHISHERS GOOGLING YOU

Billed as a one-stop shop for everything including email, calendar, documents, videos, and now social networking, Google grants users access with only one user name and password. The ease of access is great for everyone, particularly phishers. In a recent example identified by CYREN, a hacked Gmail account sends out an email entitled "Wealth management article for your review". The link, suggesting that the user review information contained in a "Google docs" document, leads the to a fake Google login/phishing site, asking for the Google user name and password (and similar credentials for a bunch of other sites).

From: @gmail.com> Sent: Tue 04-Mar-14 4:21 PM
Subject: Fwd: Wealth management article for your review

Hi All,

Attached is an article for your review. It is quite a good read and definitely the most insightful I have read on wealth management. :

Click here and log in to read the document in Google docs.

NOTE: This is a general message I'm sending to my contact list, to enlighten friends and family on wealth management, so feel free to login and view document for your financial enlightenment, this is only useful to those with wealth to manage and if you've no wealth to manage, don't bother opening.

Regards

Of course, this particular phisher is only interested in "working" with the most educated and discerning wealth managers, as the last line states, "…if you've no wealth to manage, don't bother opening."

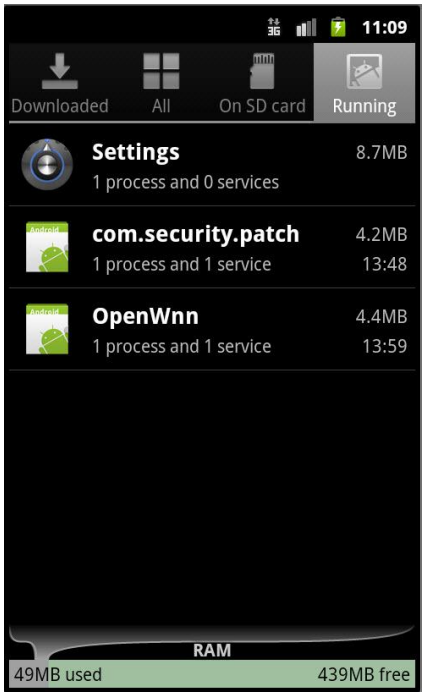
MALWARE TRENDS

IMPROVED ANDROID NOTCOM MALWARE

You may remember the emergence of Android "notcom" malware that appeared roughly a year ago, distributed in email links sent from compromised email accounts. Then, depending on the visiting device, the same link directed users to different destinations. PC or iOS users were simply sent to a diet scam site; Android users were targeted with a malware download.

Once again, malware authors are targeting Android users with the same method. While non-Android devices are sent to a diet scam page, Android users find themselves again a victim of the malware package "security.update.apk".

The malware creates a service that runs in the background called “com.security.patch”. The code creates a proxy and is then used as a P2P client. All the data that it sends out is encrypted. Our AV lab did a test to see how much data was sent and received by the malware and it turns out quite a lot. There was no service that connects to the internet running on the phone except for the malware “com.security.patch” and after 15 minutes it had transmitted almost 1 mb of data.



Using the Android device, our AV lab then opened a webpage that used 0.83 MB; the malware doubled that amount of data right away. Watch out mobile Internet users! With this malware on your Android, your data usage bills could get quite expensive, and of course, forget private browsing as everything is funneling through some proxy server. The main

address that the malware is connecting to—"172.16.1.5"— is a private IP address, which appears to be the P2P service of the malware. By sniffing through the packages from "172.16.1.5", we observed numerous other addresses.

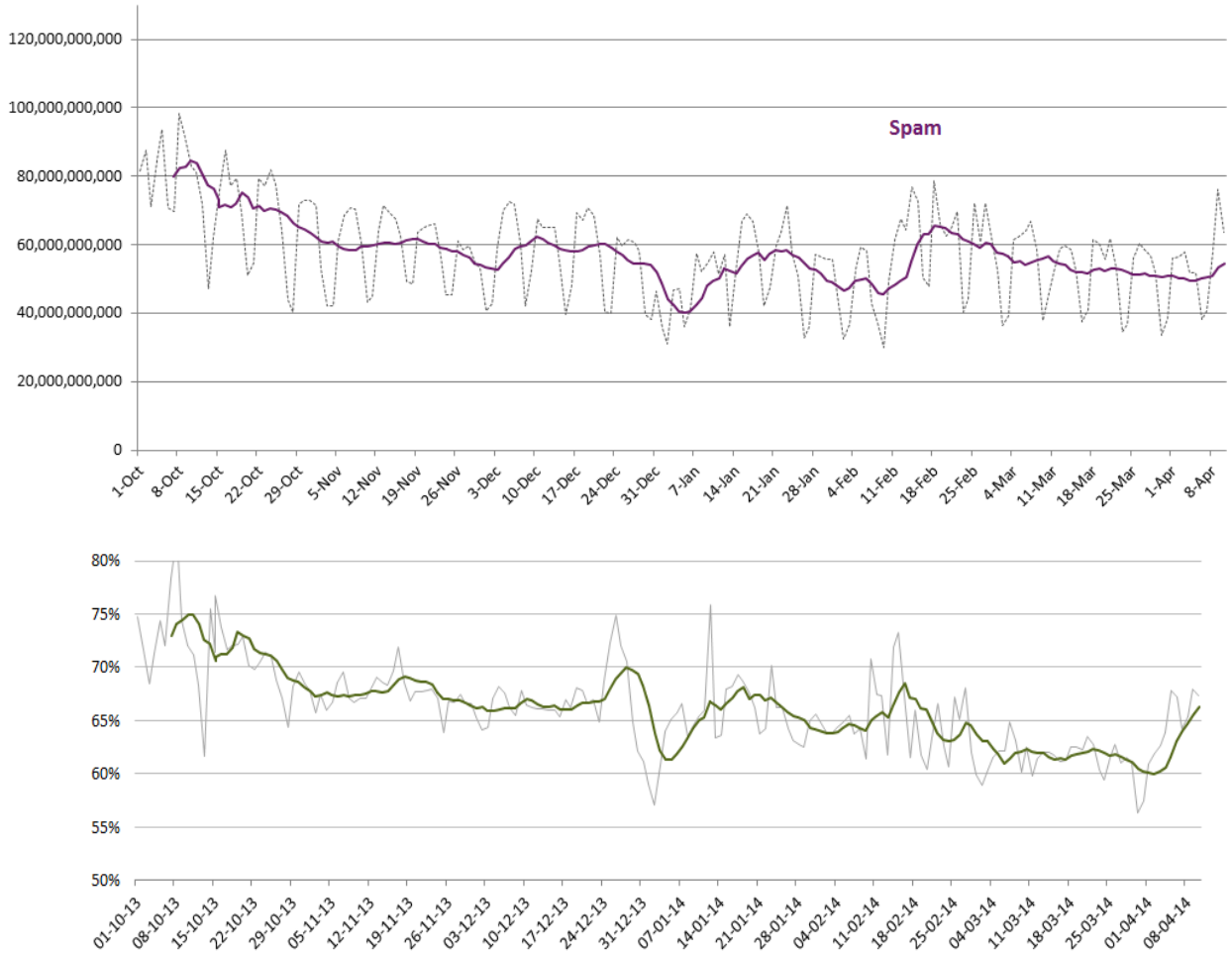
```
206.44.135.173.in-addr.arpa.....206.44.135.173.in-addr.arpa.....$..".173-135-44-206.pools.spcsdns.net.
76.128.121.108.in-addr.arpa.....76.128.121.108.in-addr.arpa.....$..".108-121-128-76.pools.spcsdns.net.
76.128.121.108.in-addr.arpa.....76.128.121.108.in-addr.arpa.....$..".108-121-128-76.pools.spcsdns.net.
71.245.33.107.in-addr.arpa.....C.....71.245.33.107.in-addr.arpa.....#.!107-33-245-71.pools.spcsdns.net.
80.164.213.106.in-addr.arpa.....80.164.213.106.in-addr.arpa.....M.ns1.apnic.net.'read-txt-record-of-zone-first-dns-admin.=..N.... .....:.....
38.59.152.105.in-addr.arpa.....H.....38.59.152.105.in-addr.arpa..... .2.ns1.afrinic.net.dnsmasters.<x.....*O... .....
47.163.235.117.in-addr.arpa.....S.....47.163.235.117.in-addr.arpa.....M.ns1.apnic.net.'read-txt-record-of-zone-first-dns-admin.=.-..... .....:.....
131.85.185.94.in-addr.arpa.....131.85.185.94.in-addr.arpa.....8@.5.ns1netrouting.net.hostmaster.<w..K..p.... ..:...Q.
```

As a result of the encryption we can only speculate as to the purpose of the malware. It seems likely that it could steal device and user data and, as with last year's, may be part of some Android botnet.

SPAM TRENDS

SPAM LEVELS

In the first quarter of 2014, spam levels continued their general downward trend. The new year period produced the traditional drop with spam representing only 57% of all global email at its lowest. The average daily spam level for the quarter was 54 billion emails per day – with some days seeing levels approaching 30 billion emails.



Copyright© 2014 CYREN

SPAM TOPICS

Pharmaceutical products (Viagra and the like) jumped up 45% from last quarter's analysis, leading this quarter's spam pack. Emails purporting to offer jobs with fast, easy cash come in at number two, accounting for approximately 15% of all spam email. And, rounding off at number three are spam emails about diet products (such as Garcinia gummi-gutta or Garcinia Cambogia), accounting for approximately 1%.

The surprise (and amusement) this quarter is the sophistication of the spam emails associated with these diet products. While Garcinia gummi-gutta may sound like the name for a long lost song by the Grateful Dead, it is actually a fruit, native to Indonesia that received attention in 2011 as an aid to natural weight loss, despite little or no scientific evidence or clinical trials to support the claim.

Spammers are going to great lengths to get you to purchase their Jerry Garcinia gummi-gutta. First, they issue a press release containing bogus diet research through a recognized news agency or wire, such as Reuters. A reputable publication, such as the Wall Street Journal, unknowingly picks up the press release and publishes it without review or rewrite. (Fake news releases get issued and published with surprising regularity.) Included in the release are direct links to the diet scam website, as well as language that appears to legitimize the content, such as "As Featured in the Wall Street Journal". What makes the scam even more insidious is the fact that the press release appears to actually question the reliability and efficacy of the diet product. Headlines such as Garcinia Cambogia Warning - Misleading Advertising Exposed are followed by content advising the reader to "please visit the links below for this most important resource and reference points". The links then lead to a different website where users can click to order the so-called diet product.

THE WALL STREET JOURNAL.

US$1 A WEEK for 12 WEEKS SUBSCRIBE NOW

EUROPE EDITION Wednesday, December 11, 2013 As of 11:37 PM EST

Subscribe | Log In

Home | World | Europe | U.K. | U.S. | Business | Markets | Market Data | Tech | Life & Culture | Opinion | Heard on the Street | Property

Europe | Asia | Earnings | Economy | Health | Law | Autos | Management | CFO Journal | CIO Journal | Risk & Compliance | More Industries

The Wall Street Journal news department was not involved in the creation of this content.

PRESS RELEASE | December 11, 2013, 11:37 p.m. ET

Investigated Reviews Research Releases Critical News On Garcinia Cambogia

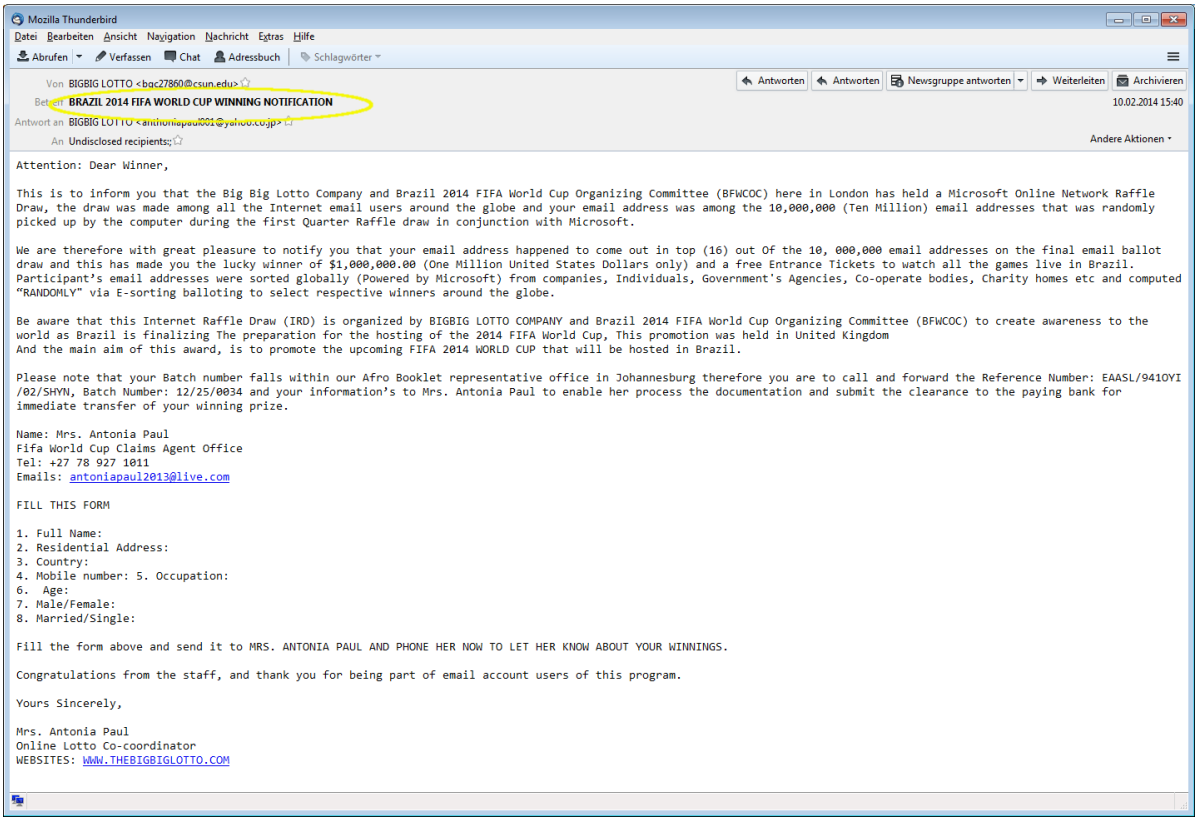
Garcinia Cambogia is commonly used for dieting, but Investigated Reviews' research analyst Cindy Walters has attracted press attention by breaking down key essential facts.

Philadelphia, PA, United States of America - December 11th, 2013 /MarketersMedia/ -- Garcinia Cambogia has proven to be an incredibly popular supplement for dieting and weight loss, but not all supplements are created equal. Many buyers have been the victim of low quality products that fail to be effective. With disillusionment everywhere, research analyst Cindy Walters has readdressed clinical data and revealed crucial insights that have been released to the press in order to restore faith in the supplement, as well as giving advice on how to avoid the scams and purchase only high quality products from recommended providers. These new investigations on Garcinia Cambogia extract are spreading like wildfire through major press resource centers.

THE FIRST WORLD CUP SCAMS APPEAR

Spammers are wasting no time with the FIFA World Cup just around the corner. During the first quarter, CYREN observed some of the first emails related to this major world-sporting event. Employing a typical lottery scam, the email informs the recipients that the "Big Big Lotto Company", with the support of the "Microsoft Online Network Raffle", has selected them to receive $1 million US dollars and one free entrance ticket to watch all games live in Brazil. To allay any

fears the recipients may have about the objectivity of the drawing, the email further informs them that "email addresses were sorted globally (Powered by Microsoft) from companies, Individuals, government agencies, co-operate bodies, and Charity homes, etc." If only the co-operate bodies would cooperate and provide a little coaching on grammar and punctuation.



Mozilla Thunderbird

Datei Bearbeiten Ansicht Navigation Nachricht Extras Hilfe

Abrufen | Verfassen | Chat | Adressbuch | Schlagwörter

Antworten | Antworten | Newsgruppe antworten | Weiterleiten | Archivieren

Von: BIGBIG LOTTO <bgc27860@csun.edu>

Betreff: **BRAZIL 2014 FIFA WORLD CUP WINNING NOTIFICATION** 10.02.2014 15:40

Antwort an: BIGBIG LOTTO <antoniapaul001@yahoo.co.jp>

An: Undisclosed recipients:; Andere Aktionen

Attention: Dear Winner,

This is to inform you that the Big Big Lotto Company and Brazil 2014 FIFA World Cup Organizing Committee (BFWCOC) here in London has held a Microsoft Online Network Raffle Draw, the draw was made among all the Internet email users around the globe and your email address was among the 10,000,000 (Ten Million) email addresses that was randomly picked up by the computer during the first Quarter Raffle draw in conjunction with Microsoft.

We are therefore with great pleasure to notify you that your email address happened to come out in top (16) out Of the 10, 000,000 email addresses on the final email ballot draw and this has made you the lucky winner of $1,000,000.00 (One Million United States Dollars only) and a free Entrance Tickets to watch all the games live in Brazil. Participant's email addresses were sorted globally (Powered by Microsoft) from companies, Individuals, Government's Agencies, Co-operate bodies, Charity homes etc and computed "RANDOMLY" via E-sorting balloting to select respective winners around the globe.

Be aware that this Internet Raffle Draw (IRD) is organized by BIGBIG LOTTO COMPANY and Brazil 2014 FIFA World Cup Organizing Committee (BFWCOC) to create awareness to the world as Brazil is finalizing The preparation for the hosting of the 2014 FIFA World Cup, This promotion was held in United Kingdom
And the main aim of this award, is to promote the upcoming FIFA 2014 WORLD CUP that will be hosted in Brazil.

Please note that your Batch number falls within our Afro Booklet representative office in Johannesburg therefore you are to call and forward the Reference Number: EAASL/941OYI /02/SHYN, Batch Number: 12/25/0034 and your information's to Mrs. Antonia Paul to enable her process the documentation and submit the clearance to the paying bank for immediate transfer of your winning prize.

Name: Mrs. Antonia Paul
Fifa World Cup Claims Agent Office
Tel: +27 78 927 1011
Emails: antoniapaul2013@live.com

FILL THIS FORM

1. Full Name:
2. Residential Address:
3. Country:
4. Mobile number: 5. Occupation:
6. Age:
7. Male/Female:
8. Married/Single:

Fill the form above and send it to MRS. ANTONIA PAUL AND PHONE HER NOW TO LET HER KNOW ABOUT YOUR WINNINGS.

Congratulations from the staff, and thank you for being part of email account users of this program.

Yours Sincerely,

Mrs. Antonia Paul
Online Lotto Co-coordinator
WEBSITES: WWW.THEBIGBIGLOTTO.COM

Proving that this sort of scam is successful, the World Cup Lottery theme is simply a repeat of similar scams from 2010 – which were repeats of similar scams predeeding the 2006 World Cup.

Add contact 28-May-10

To: undisclosed recipients:

FROM: MRS, MARIA STEVEN {ZIMBABWE}

Lottery Canada

South Africa 2010

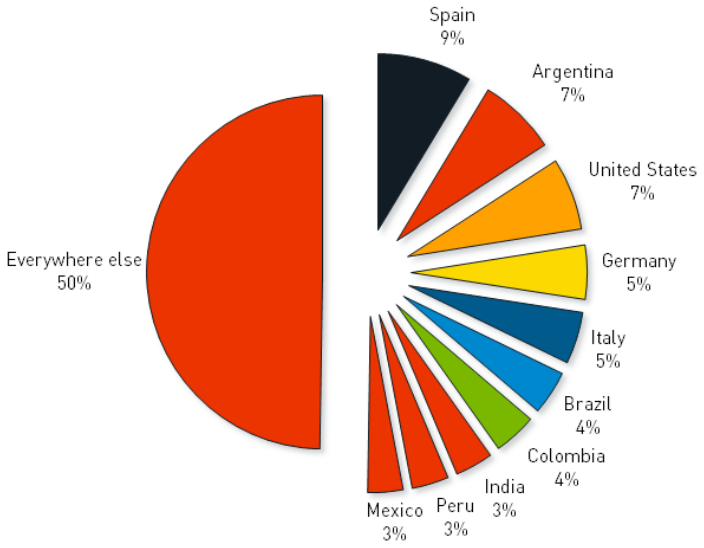
From: Mrs. Cynthia Chalker
1550 Princess Street
Kingston, ON, Canada, K7M 9E3
Ref: EAAL/851OYHI/08 Ontario Canada
Email:mrscynthia_chalker@live.com

WINNING NOTIFICATION

The Canadian Government in Conjuction with Fifa Local Organizing Committee South Africa sponsors this lottery for the promotion of the 2010 Soccer World cup to be hosted in South Africa. We happily announce to you the draw of the Special Global 2010 World Cup Promotional Draw held on the Wednesday, 26th May 2010 in Essex United Kingdom and Ontario Canada. Your - mail address attached to Ticket Number: B9564 75604545 100, with Serial Number 4391886 drew the winning numbers 6 15 22

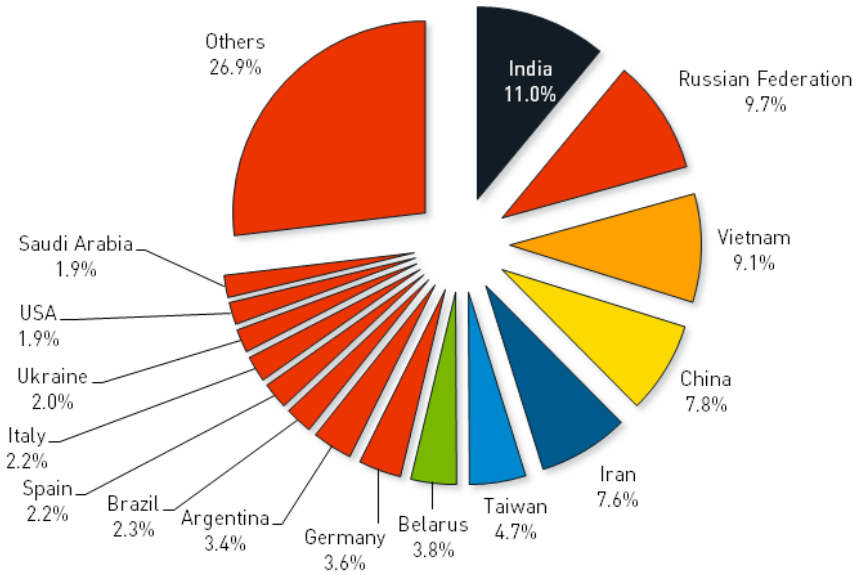
SPAM: COUNTRIES OF ORIGIN

As we noted in our 2013 Security Yearbook, an increasing amount of spam seems to be originating in Spain. For the first time, during Q1 of 2014, Spanish spammers led the way with 9% of all global spam, followed by Argentina and the United States with 7% each. Germany and Italy followed, producing 5% of global spam. South American countries, Brazil and Columbia took 6th and 7th place with 4% each. Noticeably missing from the list this time were Russia and China. In contrast, Western European countries, Spain, Germany, and Italy took three of the top five spots.



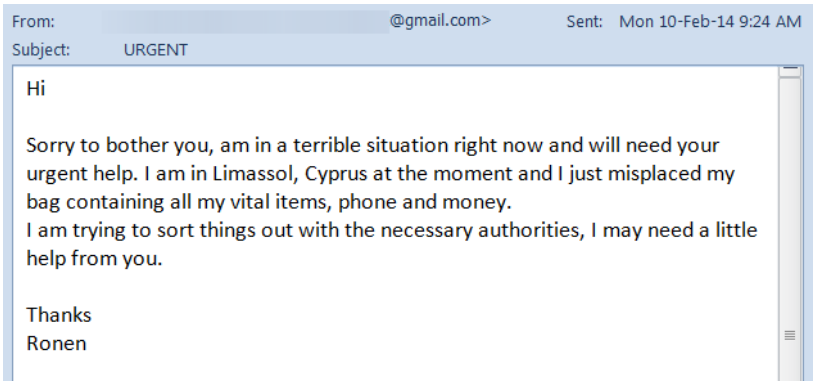
SPAM ZOMBIES

During the first quarter of 2014, India stayed in first place with the most spam sending bots (11%) followed by Russia with a significant increase to nearly 10%. Brazil returns to the top 15 along with Spain, Ukraine and Saudi Arabia. Peru, Colombia, Serbia and Mexico ended their brief visit to the list and dropped of this quarter.



THE ONE WORD EMAIL SCAM

And finally; You may be familiar with the "stuck overseas" scam email received from friends/family/acquaintances who have had their accounts hacked. Like this one:

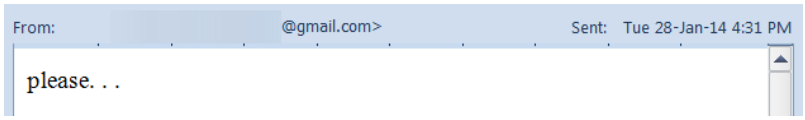

From: @gmail.com> Sent: Mon 10-Feb-14 9:24 AM
Subject: URGENT

Hi

Sorry to bother you, am in a terrible situation right now and will need your urgent help. I am in Limassol, Cyprus at the moment and I just misplaced my bag containing all my vital items, phone and money.
I am trying to sort things out with the necessary authorities, I may need a little help from you.

Thanks
Ronen

But, we assume that scammers are trying to save time with a less wordy approach:


From: @gmail.com> Sent: Tue 28-Jan-14 4:31 PM

please. . .

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.

ABOUT CYBEROAM

Cyberoam Technologies, a Sophos Company, is a global Network Security appliances provider, offering future-ready security solutions to physical and virtual networks in organizations with its Next-Generation Firewalls (NGFWs) and Unified Threat Management (UTM) appliances. The virtual and hardware Cyberoam Central Console appliances offer Centralized Security Management options to organizations, while Cyberoam iView allows intelligent logging and reporting with one-of-their-kind, in-depth reports. Cyberoam is accredited with prestigious global standards and certifications like EAL4+, CheckMark UTM Level 5 Certification, ICSA Labs, IPv6 Gold logo, and is a member of the Virtual Private Network Consortium. For more information, please visit www.cyberoam.com

CYREN, Recurrent Pattern Detection, RPD, and GlobalView are trademarks, and CYREN, Eleven, Authentium, F-Prot, Command Antivirus, and Command Anti-malware are registered trademarks, of CYREN. U.S. Patent No. 6,330,590 is owned by CYREN.