SPAM AND PHISHING IN Q2 2015

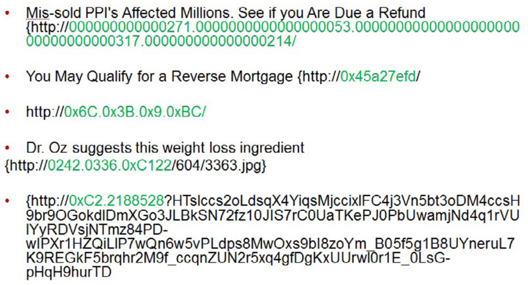
Tatyana Shcherbakova,
Maria Vergelis,
Nadezhda Demidova

CONTENT

SPAM: FEATURES OF THE QUARTER

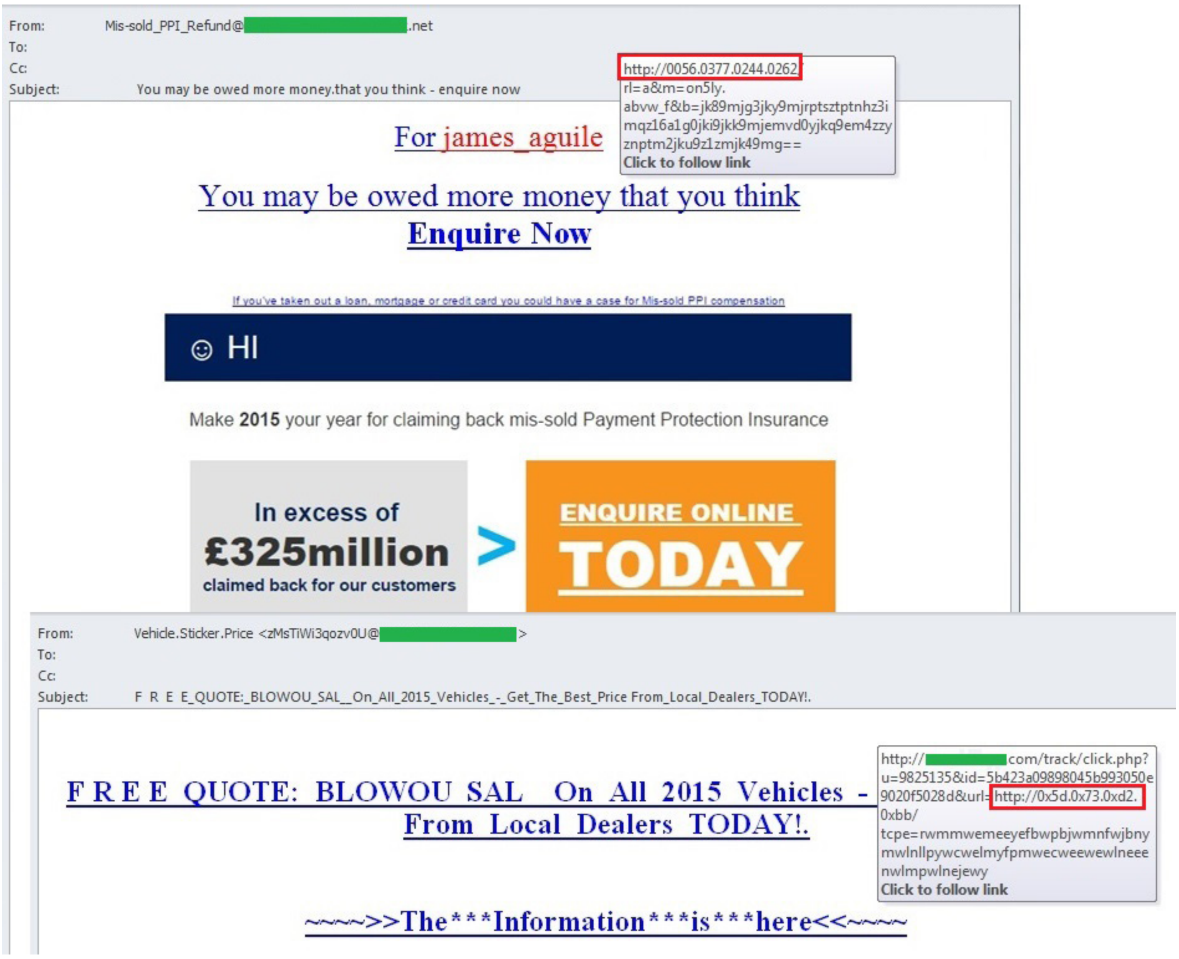
“Noising” domains

We have already analyzed the situation with regard to the considerable increase in the number of new domain zones as well as mass generation of spammer domains in these zones, specifically those designed to send out illegitimate mass mailings. The further analysis of spam mailings shows that spammers rely not only on a huge number of new domains which they can change even within one thematic mass mailing, but also on the ways they are implemented in the text. For example, in Q1 we registered various cases of “noising” domains in links used to go to spam resources, as well as cases of code obfuscation in the HTML structure of the messages in the mass mailing.



- Mis-sold PPI's Affected Millions. See if you Are Due a Refund {http://000000000000271.000000000000000053.000000000000000000000000000000317.00000000000000000214/
- You May Qualify for a Reverse Mortgage {http://0x45a27efd/
- http://0x6C.0x3B.0x9.0xBC/
- Dr. Oz suggests this weight loss ingredient
{http://0242.0336.0xC122/604/3363.jpg}
- {http://0xC2.2188528?HTslccs2oLdsqX4YiqsMjccixlFC4j3Vn5bt3oDM4ccsH9br9OGokdlDmXGo3JLBkSN72fz10JIS7rC0UaTKePJ0PbUwamjNd4q1rVUlYyRDVsjNTmz84PD-wIPXr1HZQiLIP7wQn6w5vPLdps8MwOxs9bI8zoYm_B05f5g1B8UYneruL7K9REGkF5brqhr2M9f_ccqnZUN2r5xq4gfDgKxUUrwI0r1E_0LsG-pHqH9hurTD

In many mass mailing, spammers used IP addresses of sites, instead of domain names, in links to advertising resources. However they provided modified rather than direct IP addresses, representing them using the octal or hexadecimal numerical system, adding an arbitrary number of zeros to the beginning of the address. This did not change the IP address, but increased the number of possible variants of its representation (variations within one mass mailing); which, as spammers hoped, would help deceive the spam filter. Such alternative methods of representing IP addresses were used by spammers both in direct links and in “noised” redirects.



From: Mis-sold_PPI_Refund@[redacted].net
To:
Cc:
Subject: You may be owed more money.that you think - enquire now

http://0056.0377.0244.0262
rl=a&m=on5ly.
abvw_f&b=jk89mjg3jky9mjrptsztptnhz3i
mqz16a1g0jki9jkk9mjemvd0yjkq9em4zzy
znptm2jku9z1zmjk49mg==
Click to follow link

For james_aguile

You may be owed more money that you think

Enquire Now

If you've taken out a loan, mortgage or credit card you could have a case for Mis-sold PPI compensation

☺ HI

Make 2015 your year for claiming back mis-sold Payment Protection Insurance

From: Vehicle.Sticker.Price <zMsTiWi3qozv0U@[redacted]>
To:
Cc:
Subject: F R E E_QUOTE:_BLOWOU_SAL__On_All_2015_Vehicles_-_Get_The_Best_Price From_Local_Dealers_TODAY!.

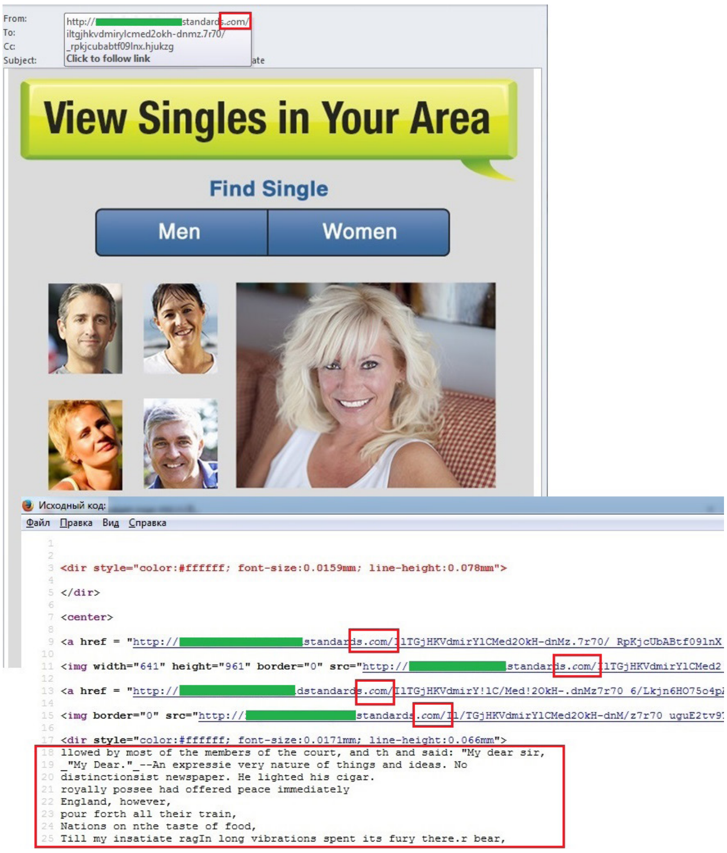
http://[redacted]com/track/click.php?
u=9825135&id=5b423a09898045b993050e
9020f5028d&url=http://0x5d.0x73.0xd2.
0xbb/
tcpe=rwmmwemeeyefbwpbjwmnfwjbny
mwlnllpywcwelmyfpmwecweewewlneee
nwlmpwlnejewy
Click to follow link

F R E E QUOTE: BLOWOU SAL On All 2015 Vehicles - From Local Dealers TODAY!.

~~~~>>The***Information***is***here<<~~~~
~~~~

Spammers also used noised domains. For example, they represented a domain name using both upper and lower case characters (NEEDHosT. niNjA), as well as using several different codes in the HTML structure of the message. They attempted to hide their domains by changing one of the characters in the name of the domain zone for the same from the other code or similar to it. So, for example, it might look like this - domainname.com, domainname.cⓞ.

Spammers often applied several methods of noising in one email: they used both the alternative representation of the IP address or domain distortion, as well as the traditional use of meaningless "junk" text in the body of the message, in order to completely conceal the spam theme of the message.



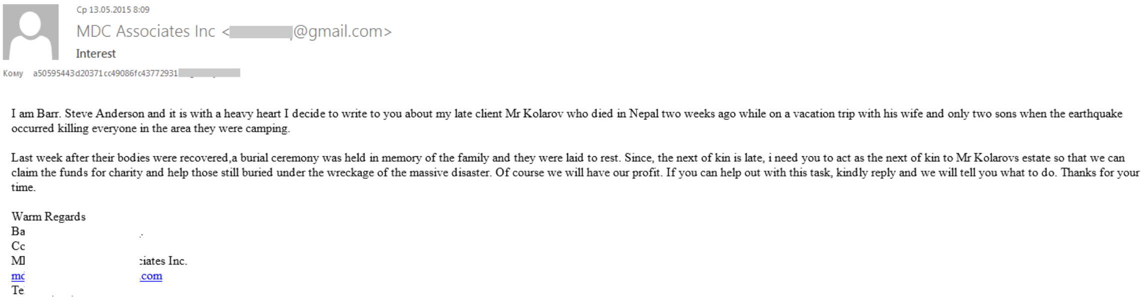
```
http://[redacted]standards.com/
iltgjhkvdmirylcmed2okh-dnmz.7r70/
_rpkjcubabtf09lnx.hjukzg
Click to follow link
```

```
<dir style="color:#ffffff; font-size:0.0159mm; line-height:0.078mm">

</dir>

<center>

<a href = "http://[redacted]standards.com/I1TGjHKVdmirYlCMed2OkH-dnMz.7r70/ RpKjcUbABtf09lnX

<img width="641" height="961" border="0" src="http://[redacted]standards.com/I1TGjHKVdmirYlCMed2

<a href = "http://[redacted]dstandards.com/I1TGjHKVdmirY!1C/Med!2OkH-.dnMz7r70 6/Lkjn6HO75o4p

<img border="0" src="http://[redacted]standards.com/I1/TGjHKVdmirYlCMed2OkH-dnM/z7r70 uguE2tv9

<dir style="color:#ffffff; font-size:0.0171mm; line-height:0.066mm">
llowed by most of the members of the court, and th and said: "My dear sir,
_"My Dear."_--An expressie very nature of things and ideas. No
distinctionsist newspaper. He lighted his cigar.
royally possee had offered peace immediately
England, however,
pour forth all their train,
Nations on nthe taste of food,
Till my insatiate ragIn long vibrations spent its fury there.r bear,
```

World events in "Nigerian" spam

In the second quarter of 2015, "Nigerian" letters exploited the themes of the earthquake in Nepal, the presidential election in Nigeria and the Olympics in Rio de Janeiro. Tragic events widely covered in the world media are usually exploited by fraudsters to trick users, and their stories hardly change.

In the email written on behalf of a lawyer whose client died in Nepal, the scammers asked the recipient to play the role of the victim's relative and help in receiving their inheritance, in return for financial remuneration. In the other mass mailings, the fraudsters distributed emails in the name of various organizations asking to help the earthquake victims. For example, "a representative of the Red Cross" asked the recipient to assist in accommodating a family of refugees who had decided to move to another country and invest their funds there.

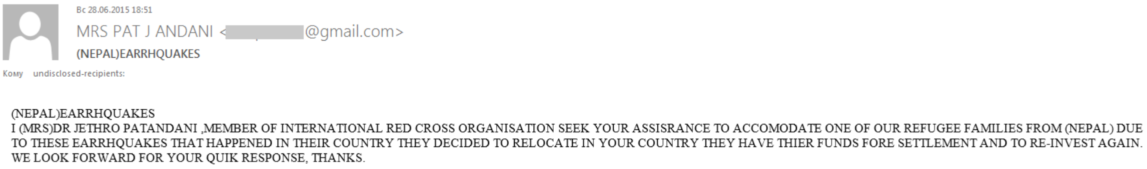


Ср 13.05.2015 8:09
MDC Associates Inc <[redacted]@gmail.com>
Interest
Кому a50595443d20371cc49086fc43772931[redacted]

I am Barr. Steve Anderson and it is with a heavy heart I decide to write to you about my late client Mr Kolarov who died in Nepal two weeks ago while on a vacation trip with his wife and only two sons when the earthquake occurred killing everyone in the area they were camping.

Last week after their bodies were recovered,a burial ceremony was held in memory of the family and they were laid to rest. Since, the next of kin is late, i need you to act as the next of kin to Mr Kolarovs estate so that we can claim the funds for charity and help those still buried under the wreckage of the massive disaster. Of course we will have our profit. If you can help out with this task, kindly reply and we will tell you what to do. Thanks for your time.

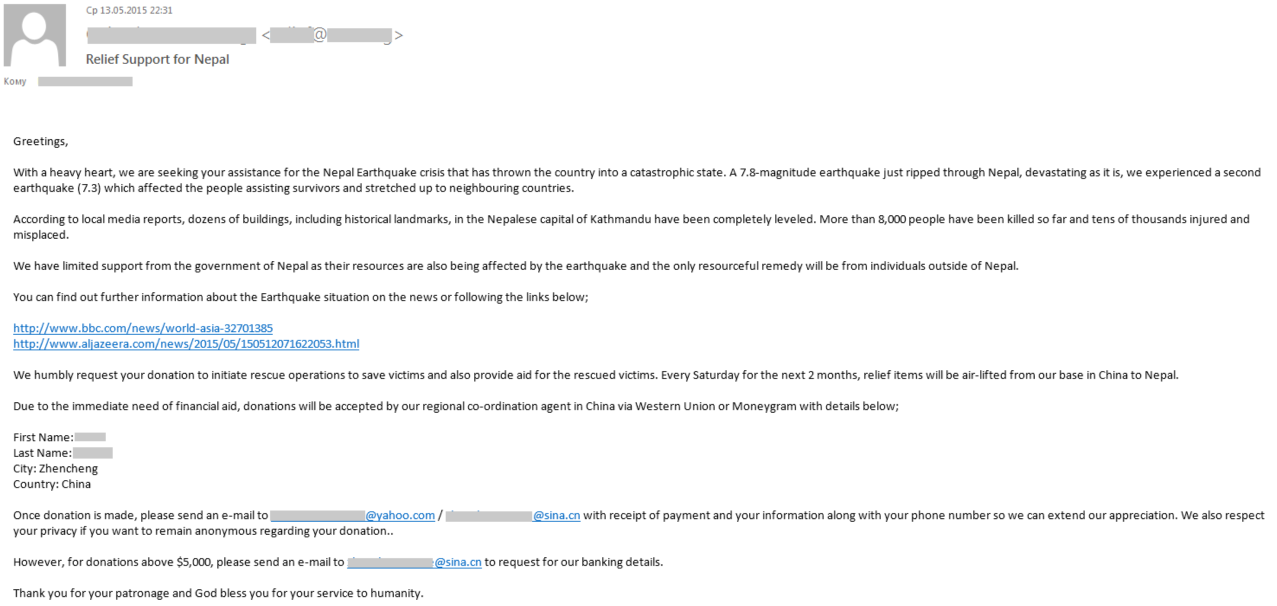
Warm Regards
Ba[redacted]
Cc
Ml ciates Inc.
mc .com
Te



Вс 28.06.2015 18:51
MRS PAT J ANDANI <[redacted]@gmail.com>
(NEPAL)EARRHQUAKES
Кому undisclosed-recipients:

(NEPAL)EARRHQUAKES
I (MRS)DR JETHRO PATANDANI ,MEMBER OF INTERNATIONAL RED CROSS ORGANISATION SEEK YOUR ASSISRANCE TO ACCOMODATE ONE OF OUR REFUGEE FAMILIES FROM (NEPAL) DUE TO THESE EARRHQUAKES THAT HAPPENED IN THEIR COUNTRY THEY DECIDED TO RELOCATE IN YOUR COUNTRY THEY HAVE THIER FUNDS FORE SETTLEMENT AND TO RE-INVEST AGAIN. WE LOOK FORWARD FOR YOUR QUIK RESPONSE, THANKS.

Generally, the addresses of those who send "Nigerian" letters were registered on free e-mail services, even if the author of the email was a representative of an organization, as in the above case. However, some tricky fraudsters tried to make the name and the address of the sender look more legitimate. They sent out fake messages asking the recipients to make a voluntary donation to help the victims of the earthquake in Nepal.



Ср 13.05.2015 22:31

[redacted] <[redacted]@[redacted]>

Relief Support for Nepal

Кому [redacted]

Greetings,

With a heavy heart, we are seeking your assistance for the Nepal Earthquake crisis that has thrown the country into a catastrophic state. A 7.8-magnitude earthquake just ripped through Nepal, devastating as it is, we experienced a second earthquake (7.3) which affected the people assisting survivors and stretched up to neighbouring countries.

According to local media reports, dozens of buildings, including historical landmarks, in the Nepalese capital of Kathmandu have been completely leveled. More than 8,000 people have been killed so far and tens of thousands injured and misplaced.

We have limited support from the government of Nepal as their resources are also being affected by the earthquake and the only resourceful remedy will be from individuals outside of Nepal.

You can find out further information about the Earthquake situation on the news or following the links below;

http://www.bbc.com/news/world-asia-32701385
http://www.aljazeera.com/news/2015/05/150512071622053.html

We humbly request your donation to initiate rescue operations to save victims and also provide aid for the rescued victims. Every Saturday for the next 2 months, relief items will be air-lifted from our base in China to Nepal.

Due to the immediate need of financial aid, donations will be accepted by our regional co-ordination agent in China via Western Union or Moneygram with details below;

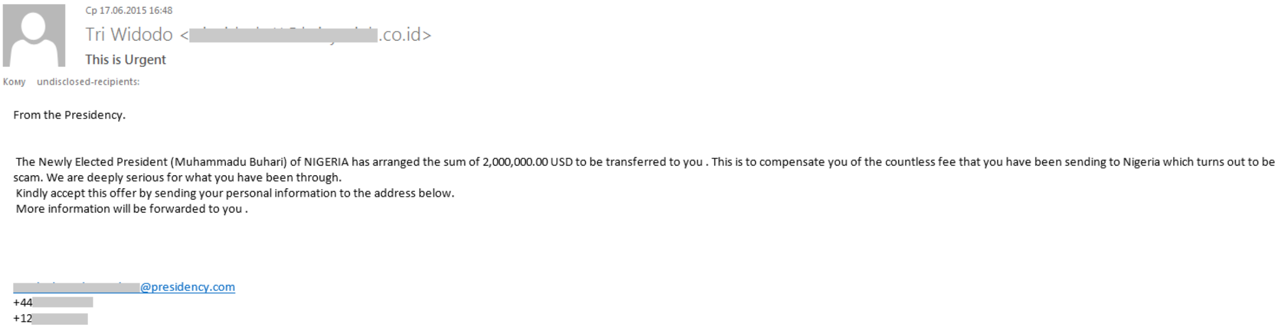
First Name: [redacted]
Last Name: [redacted]
City: Zhencheng
Country: China

Once donation is made, please send an e-mail to [redacted]@yahoo.com / [redacted]@sina.cn with receipt of payment and your information along with your phone number so we can extend our appreciation. We also respect your privacy if you want to remain anonymous regarding your donation..

However, for donations above $5,000, please send an e-mail to [redacted]@sina.cn to request for our banking details.

Thank you for your patronage and God bless you for your service to humanity.

"Nigerians" could not let political events go unnoticed. In one of the mass mailings, the fraudsters tried to lure the recipient with the sum of $2 million, which the newly elected President of Nigeria was allegedly ready to send to the user as compensation for the fraud committed by the citizens of his country.



Ср 17.06.2015 16:48

Tri Widodo <[redacted].co.id>

This is Urgent

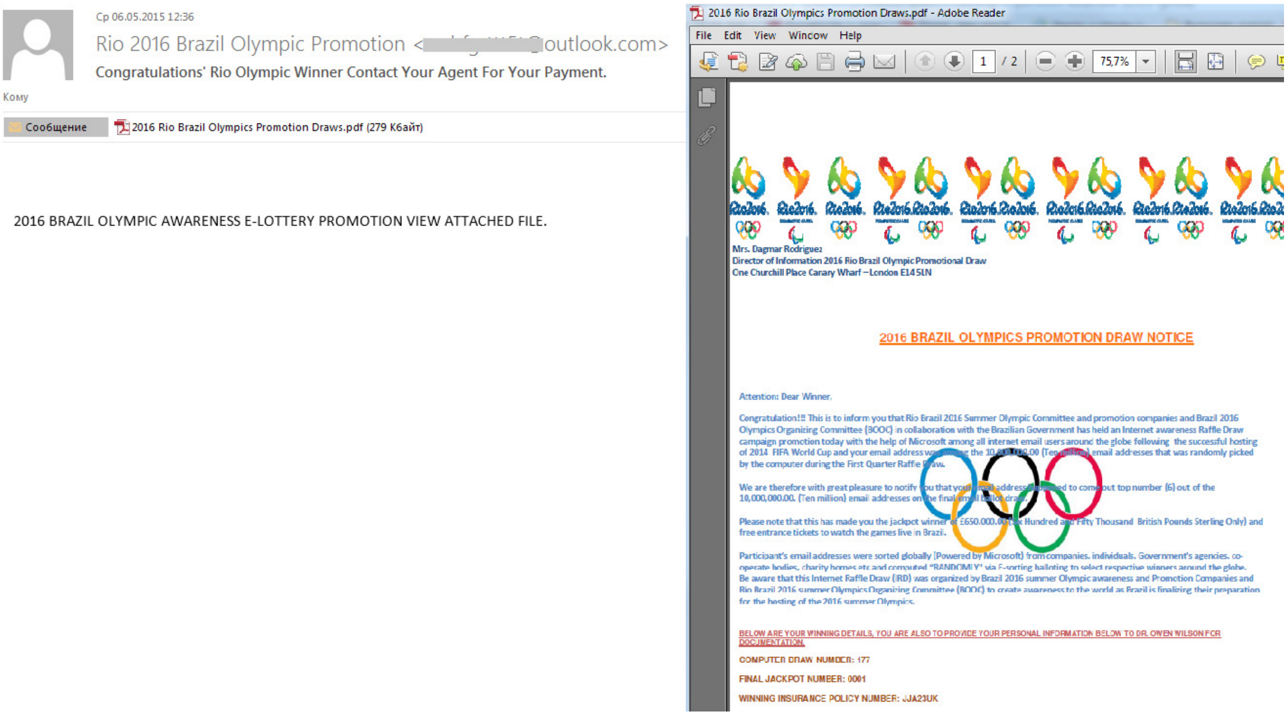
Кому undisclosed-recipients:

From the Presidency.

The Newly Elected President (Muhammadu Buhari) of NIGERIA has arranged the sum of 2,000,000.00 USD to be transferred to you . This is to compensate you of the countless fee that you have been sending to Nigeria which turns out to be scam. We are deeply serious for what you have been through.
Kindly accept this offer by sending your personal information to the address below.
More information will be forwarded to you .

[redacted]@presidency.com
+44[redacted]
+12[redacted]

The next Olympic Games in Brazil will not be held until 2016, but we are already registering fraudulent notifications of lottery wins dedicated to this popular sporting event. Interestingly, a large number of emails of this type was sent out in the run-up to the World Cup, while the Olympics were not mentioned. The content of the messages is standard: the lottery was held by the official organization, the recipient's address was randomly selected out of millions of email addresses, to receive the win it is necessary to respond to the email and provide the specified personal information.



Ср 06.05.2015 12:36

Rio 2016 Brazil Olympic Promotion <[redacted]outlook.com>

Congratulations' Rio Olympic Winner Contact Your Agent For Your Payment.

Кому

Сообщение | 2016 Rio Brazil Olympics Promotion Draws.pdf (279 Кбайт)

2016 BRAZIL OLYMPIC AWARENESS E-LOTTERY PROMOTION VIEW ATTACHED FILE.

2016 Rio Brazil Olympics Promotion Draws.pdf - Adobe Reader
File Edit View Window Help
1 / 2
75,7%

Mrs. Dagmar Rodriguez
Director of Information 2016 Rio Brazil Olympic Promotional Draw
One Churchill Place Carary Wharf – London E14 5LN

2016 BRAZIL OLYMPICS PROMOTION DRAW NOTICE

Attention: Dear Winner,

Congratulation!!! This is to inform you that Rio Brazil 2016 Summer Olympic Committee and promotion companies and Brazil 2016 Olympics Organizing Committee (BOOC) in collaboration with the Brazilian Government has held an Internet awareness Raffle Draw campaign promotion today with the help of Microsoft among all internet email users around the globe following the successful hosting of 2014 FIFA World Cup and your email address was among the 10,000,000.00 (Ten million) email addresses that was randomly picked by the computer during the First Quarter Raffle Draw.

We are therefore with great pleasure to notify you that your email address happened to come out top number (6) out of the 10,000,000.00. (Ten million) email addresses on the final email ballot draw.

Please note that this has made you the jackpot winner of £650.000.00 (Six Hundred and Fifty Thousand British Pounds Sterling Only) and free entrance tickets to watch 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) was organized by Brazil 2016 summer Olympic awareness and Promotion Companies and Rio Brazil 2016 summer Olympics Organizing Committee (BOOC) to create awareness to the world as Brazil is finalizing their preparation for the hosting of the 2016 summer Olympics.

BELOW ARE YOUR WINNING DETAILS, YOU ARE ALSO TO PROVIDE YOUR PERSONAL INFORMATION BELOW TO DR. OWEN WILSON FOR DOCUMENTATION.

COMPUTER DRAW NUMBER: 177

FINAL JACKPOT NUMBER: 0001

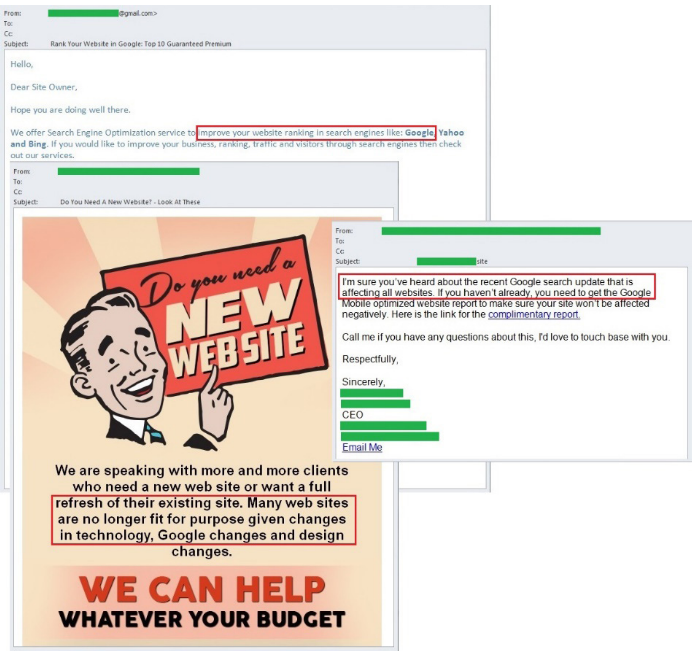
WINNING INSURANCE POLICY NUMBER: JJA23UK

Noticeably, emails containing a short text in the body of the message, with detailed information provided in an attached PDF or DOC file, are gaining popularity with spammers. This may be because an email with a short text has more chance of passing through a spam filter as legitimate. Emails with attached files are especially dangerous because a user is likely to open the attachment to learn about the the content, which can result in malware infection.

The Google search algorithm update

Yet another event exploited in spam in the second quarter of 2015 was the release of regular update to the Google search algorithm. This changed the mobile web search results so that the sites adapted for mobile phones were displayed on top positions.

This news resulted in a significant increase in the amount of spam relating to SEO (search engine optimization) and promotion of sites. Spammers sent out offers advertising the creation of sites of any complexity and purpose, as well as services to attract new customers. They emphasized the necessity to bring the site up-to-date by using the latest features of a popular search engine. Those site owners who still had doubts were threatened with ending up as the last pages in Google search results and the resulting loss of potential customers.



From: [redacted]@gmail.com>
To:
Cc:
Subject: Rank Your Website in Google: Top 10 Guaranteed Premium

Hello,

Dear Site Owner,

Hope you are doing well there.

We offer Search Engine Optimization service to improve your website ranking in search engines like: **Google**, **Yahoo and Bing**. If you would like to improve your business, ranking, traffic and visitors through search engines then check out our services.

From: [redacted]
To:
Cc:
Subject: Do You Need A New Website? - Look At These

We are speaking with more and more clients who need a new web site or want a full refresh of their existing site. Many web sites are no longer fit for purpose given changes in technology, Google changes and design changes.

From: [redacted]
To:
Cc:
Subject: [redacted]site

I'm sure you've heard about the recent Google search update that is affecting all websites. If you haven't already, you need to get the Google Mobile optimized website report to make sure your site won't be affected negatively. Here is the link for the complimentary report.

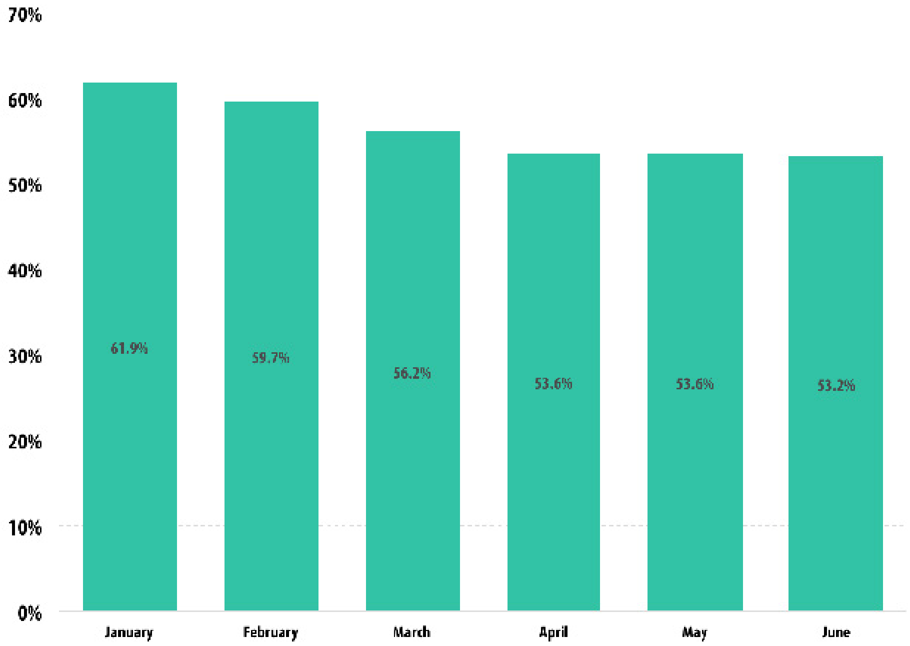
Call me if you have any questions about this, I'd love to touch base with you.

Respectfully,

Sincerely,
[redacted]
CEO
[redacted]
Email Me

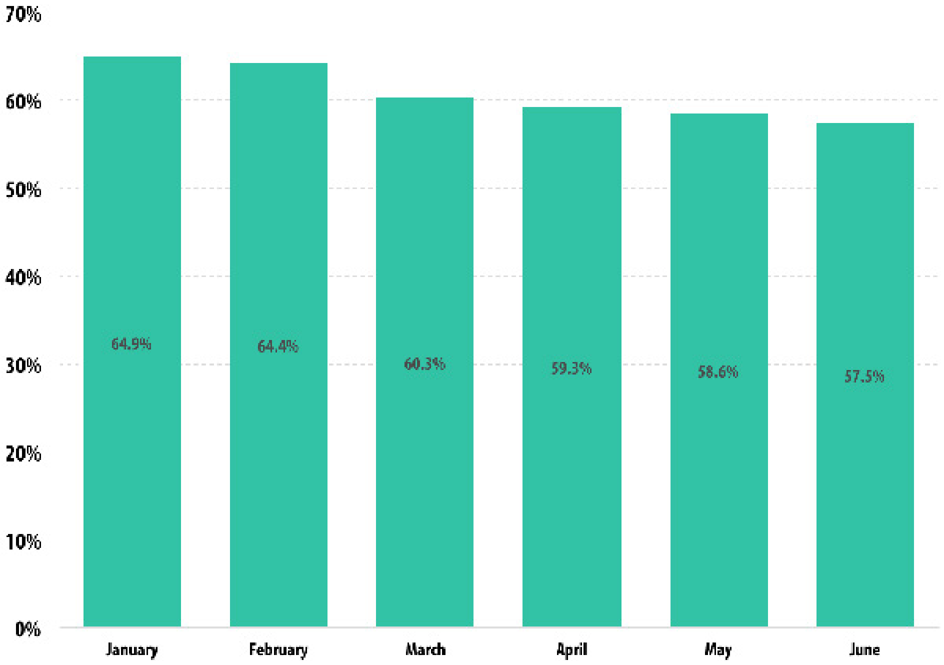
STATISTICS

Proportion of spam in email traffic



Proportion of spam in email traffic, January – June 2015

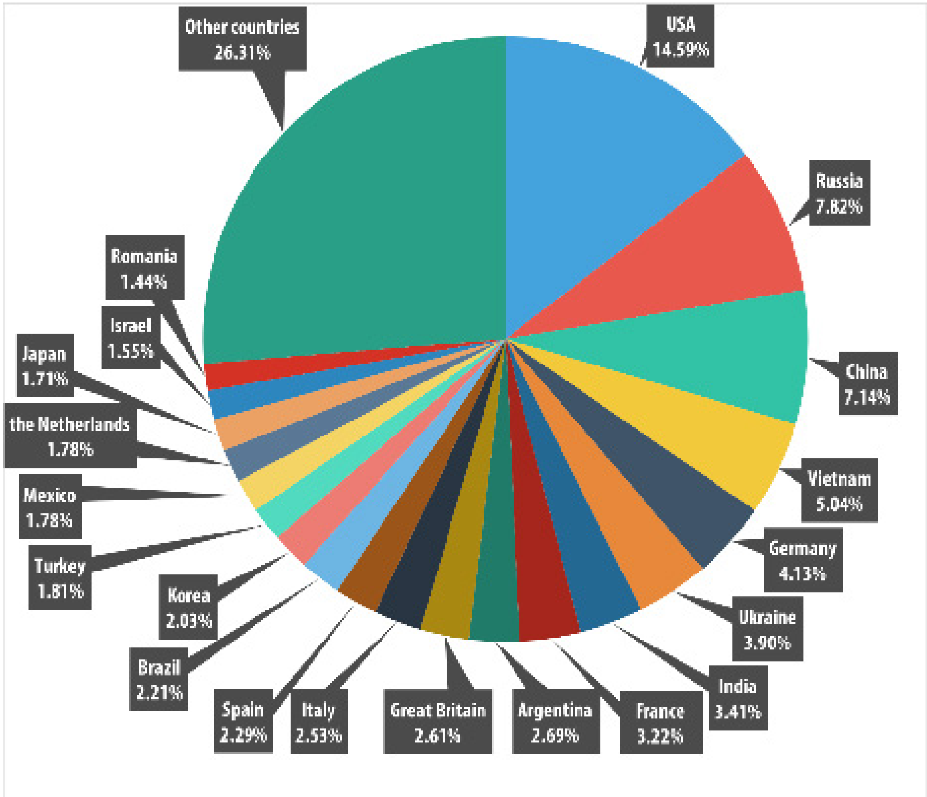
The worldwide decline in the share of spam in email traffic since the beginning of the year has almost stopped. In the second quarter of 2015 it stabilized, fluctuating between 53.5% in April and 53.23% in June.



Proportion of spam in email traffic in Russia, January – June 2015

The situation with spam in Russia is almost the same as for worldwide email traffic. During the second quarter, the share of spam traffic decreased by approximately 1 percentage point per month. Thus, the maximum quantity of spam emails in Q2 was sent in April (59.32%), while the minimum amount was distributed in June (57.47%).

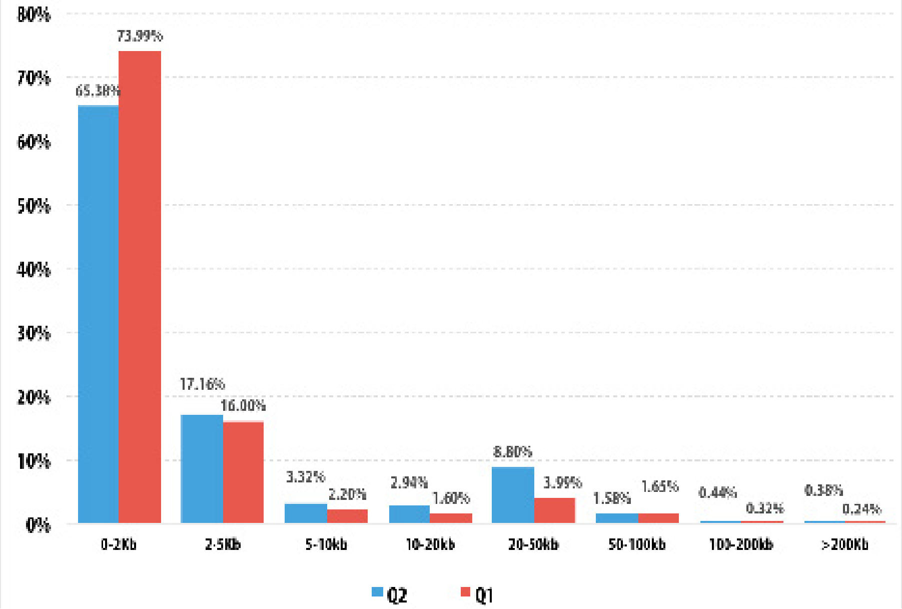
Spam sources by country



Countries that were sources of spam, Q2 2015

In the second quarter of 2015 the USA (14.59%) and Russia (7.82%) remained the biggest sources of spam. China came third with 7.14% of the world's spam, compared to 3.23% in the previous quarter. It was followed by Vietnam (5.04% compared to 4.82% in Q1), Germany (4.13% compared to 4.39% in Q1) and Ukraine (3.90% compared to 5.56% in Q1).

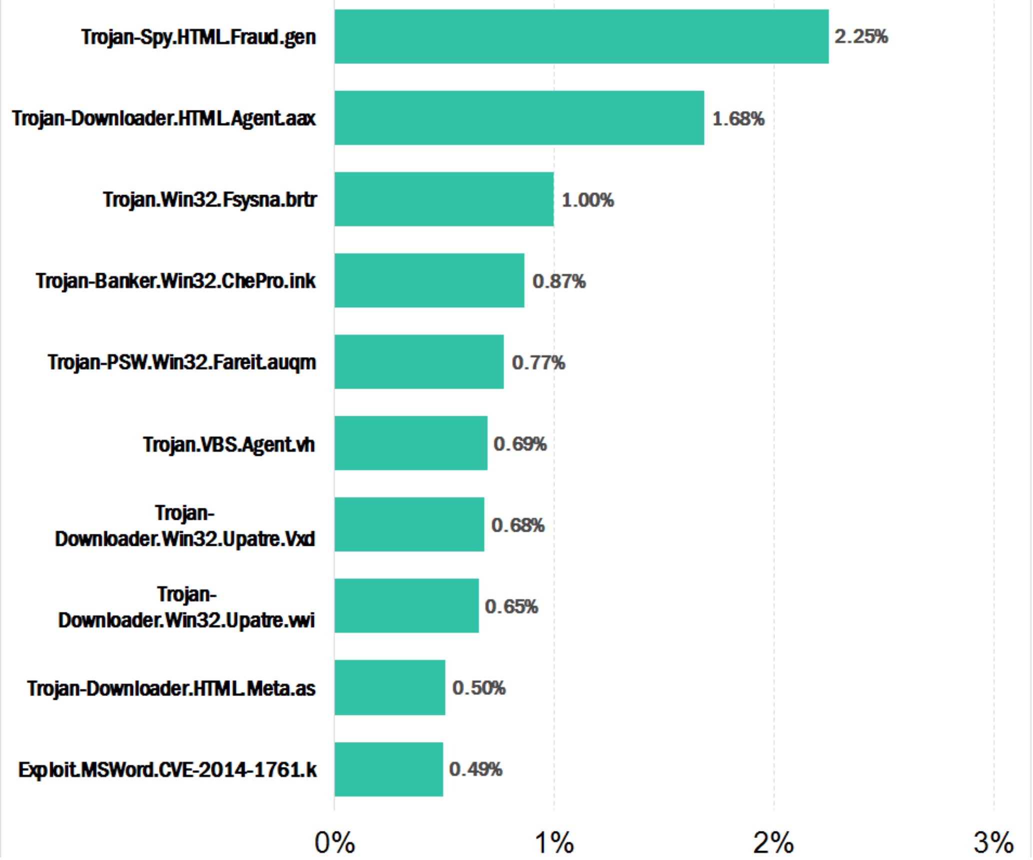
Spam email size



Spam email size distribution, Q1 2015 and Q2 2015

The distribution of spam emails by size saw little change from the previous quarter. The leaders were very small emails of up to 2 KB (65.38%), although the proportion of such emails has gradually decreased (it accounted for 73.99% in Q1). The share of emails sized 20-50 KB grew by 4.81 percentage points and reached 8.80%, while the percentage of emails in the size range of 2 KB-5 KB (17.16%), 5-10 KB (3.32%) and 10-20 KB (2.94%) increased slightly – by about 1 percentage point each.

MALICIOUS EMAIL ATTACHMENTS



Top 10 malicious programs sent by email, Q2 2015

The notorious Trojan-Spy.HTML.Fraud.gen topped the rating. As we have written before, this program is a fake HTML page which is sent via email, imitating an important notification from a large commercial bank, an online store, a software developer, etc. This threat appears as an HTML phishing website where a user has to enter his personal data which is then forwarded to cybercriminals.

Second and third positions are occupied by Trojan-Downloader.HTML.Agent.aax and Trojan-Downloader.HTML.Meta.as. Both are HTML pages which, when opened by users, redirect them to a rigged site. There, a victim is usually faced with a phishing page or is offered a download - Binbot, a binary option trading bot. The two malicious programs spread via email attachments and the only difference between them is the link which redirects users to rigged sites.

Trojan.Win32.Fsysna.brtr rounds off the Top3. It is just a common spam bot which redirects spam from the command center to the mail server on behalf of the infected machine.

Fourth is Trojan-Banker.Win32.ChePro.ink. This downloader, which was as low as sixth position in last year's ranking, is a CPL applet (a Control Panel component) that downloads Trojans designed to steal confidential financial information. Most malicious programs of this type are aimed at Brazilian and Portuguese banks.

It is followed by Trojan-PSW.Win32.Fareit.auqm. Fareit Trojans steal browser cookies and passwords from FTP clients and email programs and then send the data to a remote server run by the fraudsters.
Seventh and eight places are occupied by downloaders from the Upatre family – Trojan-Downloader.Win32.Upatre.fbq and Trojan-Downloader.Win32.Upatre.fca, respectively, which are usually disguised as PDF or RTF documents. Their main task is to download, unpack and run additional applications.

Exploit.MSWord.CVE-2014-1761.k. is tenth in the Q2 rating of the most popular malicious programs sent by email. It is a Word document containing an exploit which uses an appropriate vulnerability to download to the victim computer other malicious programs designed to steal user personal data.

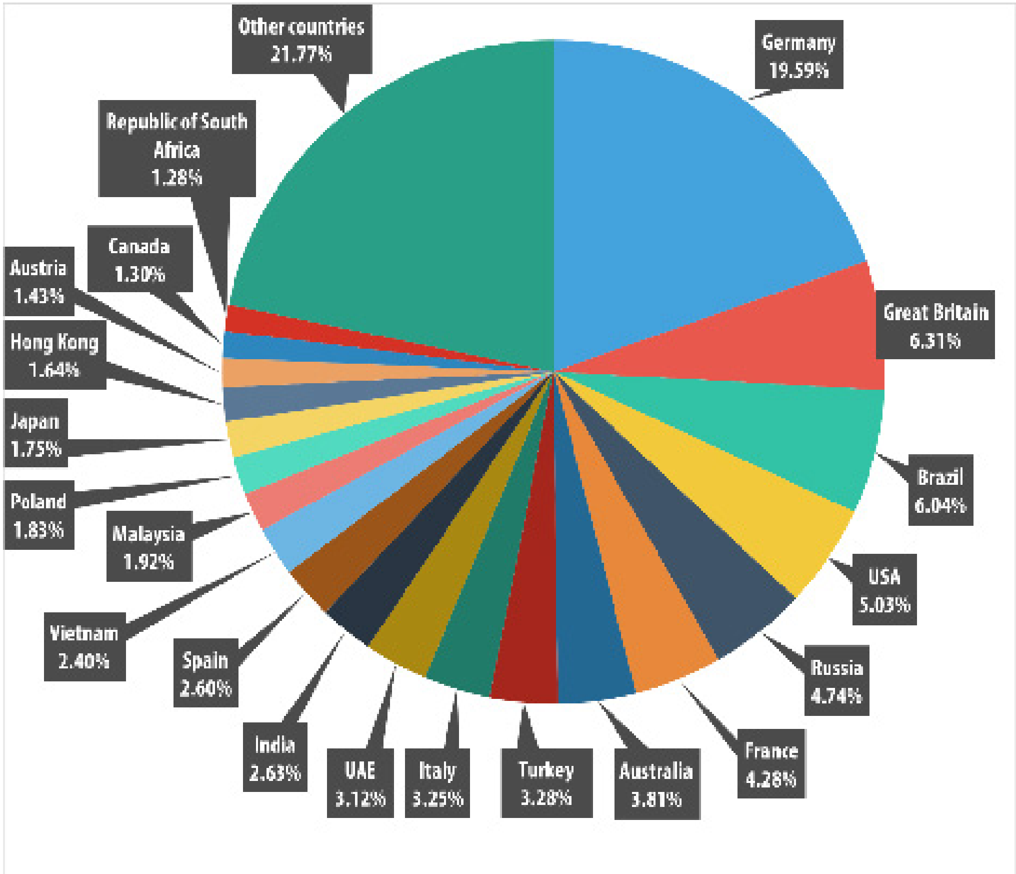
Malware families

If popular malware families, rather than specific malicious programs, are ranked, Upatre heads the Q2 rating. Malware from the Upatre family downloads the Dyre (aka Dyreza, Dyzap) Trojan banker. The list of financial organizations attacked by this banker depends on the configuration file which is loaded from the command center.

The MSWord.Agent family is gaining popularity, although in Q1 it only occupied third position in the Top 10. These malicious programs are DOC files with an embedded macro written in Visual Basic for Applications (VBA), which runs on opening the document. It downloads and runs other malware, such as malicious programs from the Andromeda family.

In Q2 2015, ZeuS/Zbot re-entered the Top 3. The members of this family are designed to carry out attacks on servers and users' computers and also for capturing data. Although ZeuS/Zbot is capable of carrying out various harmful actions, it is most often used to steal banking information. It can also install CryptoLocker – a malicious program that extorts money to decrypt the data that is has encrypted.

Countries targeted by malicious mailshots



Distribution of email antivirus verdicts by country, Q2 2015

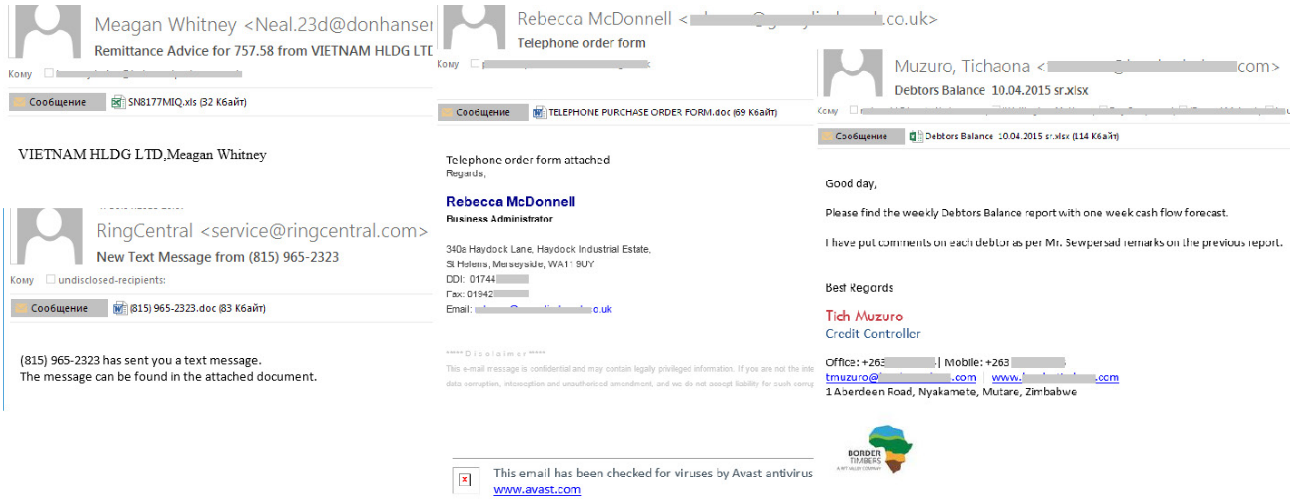
In the second quarter of 2015, there were major changes in the Top 3 countries most often targeted by mailshots. Germany (19.59%), which was only fourth in Q1, topped this quarter's rating: every fifth antivirus detection was registered on the territory of this country. Great Britain, which headed the rating in Q1 2015, moved down to second position (6.31%). Brazil settled in third (6.04%).

Special features of malicious spam

In the Q2 spam traffic we continued to register malicious emails with macro viruses, although the peak of distribution for these fell in the previous quarter. Although their number decreased, they still posed a serious threat: the macros we found belonged to the category of Trojan downloaders and were designed to download other malicious programs. Fraudsters trying to convince the recipient of the legitimacy of the email masked their messages as business correspondence and passed malicious attachments off as financial documents or orders.

In some emails the attackers specified the sender's contact details, inserted logos to make the email look official and took the email address indicated in the email from the "From" field. This made the fraudulent email look even more credible for the recipient.

In Q2 2015, we also came across emails imitating official messages from real companies, and the attackers matched the content of the message to the area of the company's activity. For example, the emails in one of the mass mailings notified the user about the alleged text message sent by the company providing telecommunications services. The recipient was told they could read it by opening the Microsoft Word attachment, but in fact the message contained Trojan-Downloader.VBS.Agent.amj.


Meagan Whitney <Neal.23d@donhanser
Remittance Advice for 757.58 from VIETNAM HLDG LTD
Кому □ [redacted]
Сообщение | SN8177MIQ.xls (32 Кбайт)

VIETNAM HLDG LTD,Meagan Whitney

RingCentral <service@ringcentral.com>
New Text Message from (815) 965-2323
Кому □ undisclosed-recipients:
Сообщение | (815) 965-2323.doc (83 Кбайт)

(815) 965-2323 has sent you a text message.
The message can be found in the attached document.

Rebecca McDonnell <[redacted].co.uk>
Telephone order form
Кому □ [redacted]
Сообщение | TELEPHONE PURCHASE ORDER FORM.doc (69 Кбайт)

Telephone order form attached
Regards,

Rebecca McDonnell
Business Administrator

340a Haydock Lane, Haydock Industrial Estate,
St Helens, Merseyside, WA11 9UY
DDI: 01744[redacted]
Fax: 01942[redacted]
Email: [redacted]o.uk

***** Disclaimer *****
This e-mail message is confidential and may contain legally privileged information. If you are not the inte
data corruption, interception and unauthorised amendment, and we do not accept liability for such corrup

This email has been checked for viruses by Avast antivirus
www.avast.com

Muzuro, Tichaona <[redacted]com>
Debtors Balance 10.04.2015 sr.xlsx
Кому □ [redacted]
Сообщение | Debtors Balance 10.04.2015 sr.xlsx (114 Кбайт)

Good day,

Please find the weekly Debtors Balance report with one week cash flow forecast.

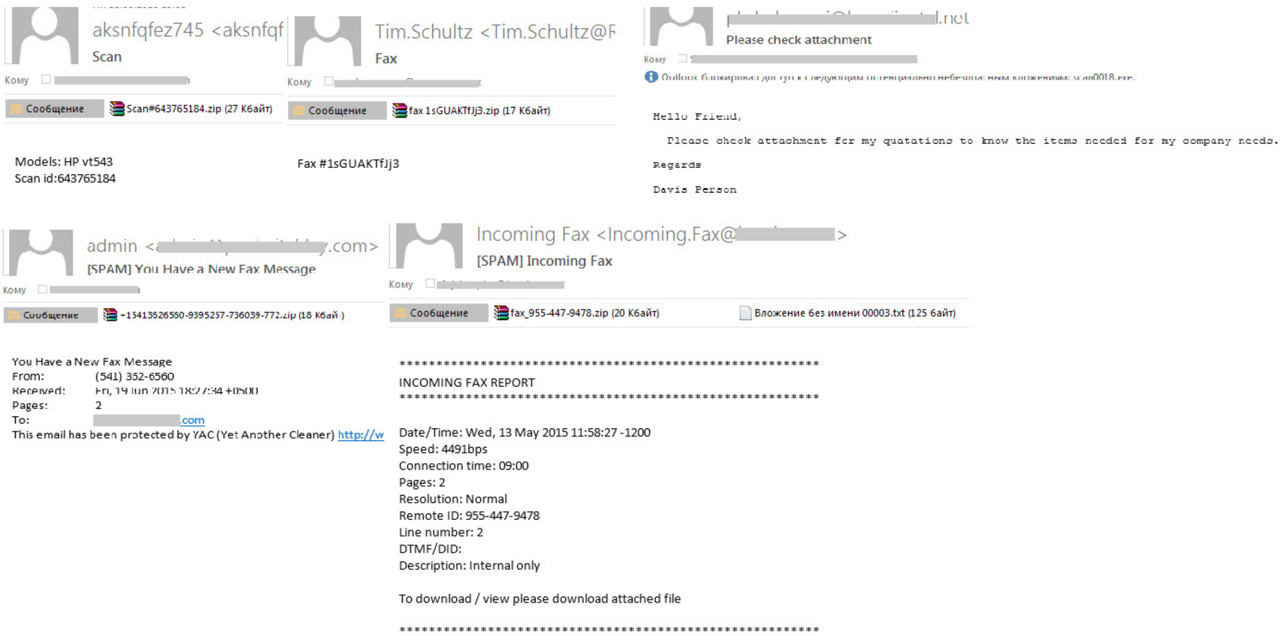
I have put comments on each debtor as per Mr. Sewpersad remarks on the previous report.

Best Regards

Tich Muzuro
Credit Controller

Office: +263[redacted] | Mobile: +263 [redacted]
tmuzuro@[redacted].com | www.[redacted].com
1 Aberdeen Road, Nyakamete, Mutare, Zimbabwe

Yet another trick which remained popular with cybercriminals who specialize in sending out malicious spam was masking messages s notifications of receipt of faxes or scans of various documents. These fake notifications are written mainly in English or German, and the attachments imitating the files with faxes or scans contain different types of malware: Trojan.Upatre, Trojan.Downloader and HawkEyePHPLogger. The text in the body of such emails could be brief or, by contrast, contain detailed information about the received document.


aksnfqfez745 <aksnfqf
Scan
Кому □ [redacted]
Сообщение | Scan#643765184.zip (27 Кбайт)

Models: HP vt543
Scan id:643765184

Tim.Schultz <Tim.Schultz@F
Fax
Кому □ [redacted]
Сообщение | fax 1sGUAKTfJj3.zip (17 Кбайт)

Fax #1sGUAKTfJj3

[redacted].net
Please check attachment
Кому □ [redacted]
Outlook блокировал доступ к следующим потенциально небезопасным вложениям: scan0018.exe.

```
Hello Friend,

  Please check attachment for my quatations to know the items needed for my company needs.

Regards

Davis Person
```

admin <[redacted].com>
[SPAM] You Have a New Fax Message
Кому □ [redacted]
Сообщение | +15413526560-9395257-736039-772.zip (18 Кбайт)

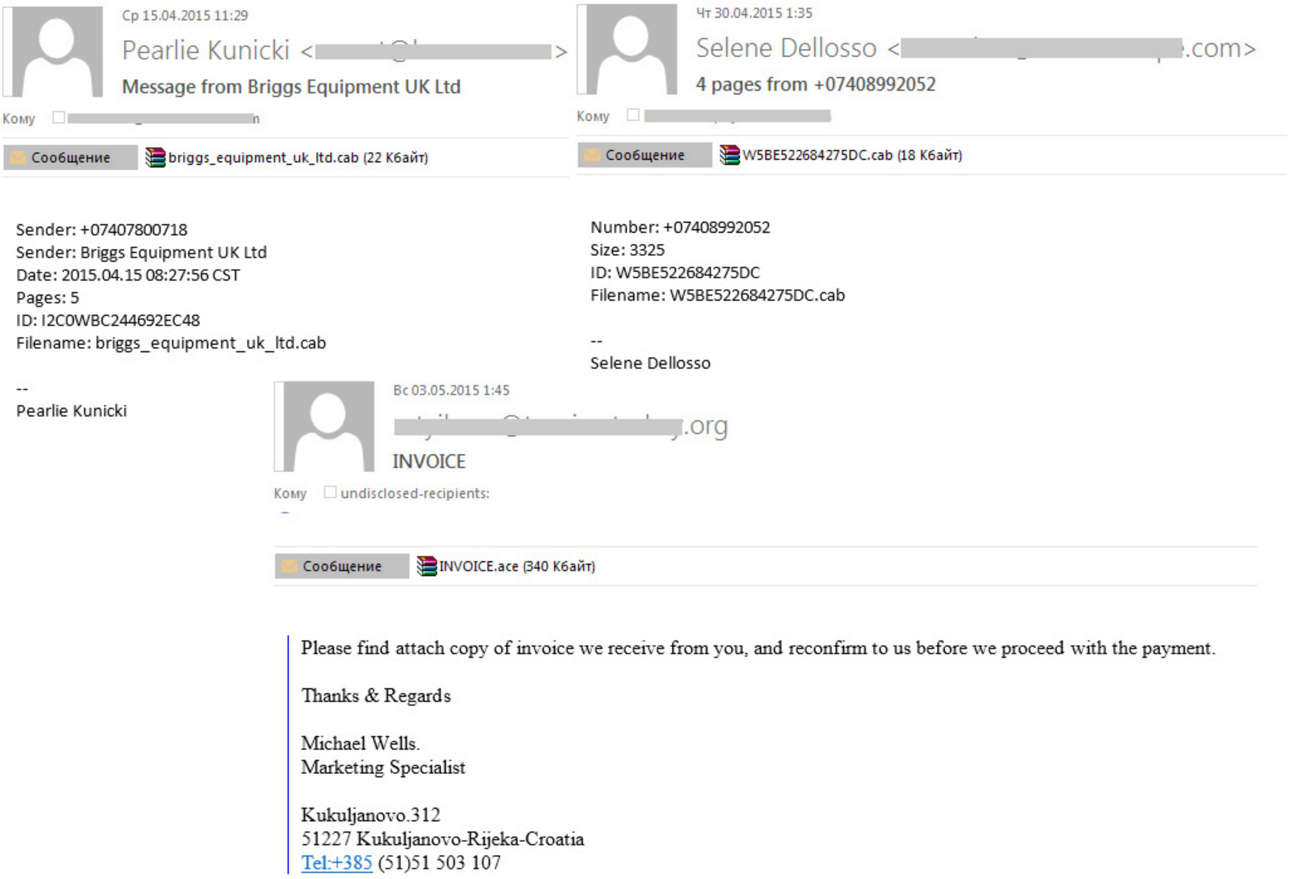
You Have a New Fax Message
From: (541) 352-6560
Received: Fri, 19 Jun 2015 18:27:34 +0500
Pages: 2
To: [redacted].com
This email has been protected by YAC (Yet Another Cleaner) http://w

Incoming Fax <Incoming.Fax@[redacted]>
[SPAM] Incoming Fax
Кому □ [redacted]
Сообщение | fax_955-447-9478.zip (20 Кбайт) | Вложение без имени 00003.txt (125 байт)

```
*************************************************************
INCOMING FAX REPORT
*************************************************************

Date/Time: Wed, 13 May 2015 11:58:27 -1200
Speed: 4491bps
Connection time: 09:00
Pages: 2
Resolution: Normal
Remote ID: 955-447-9478
Line number: 2
DTMF/DID:
Description: Internal only

To download / view please download attached file

*************************************************************
```

In September 2014, we registered a malicious mass mailing with an attachment that is not typical for spam – an archive in ARJ format. In 2015, fraudsters continue to use non-conventional archives to spread malware: April's and May's spam traffic distributed attached archives withCAB and ACE extensions, which are not common for today's spam.

The archives contained Trojan Trojan-Downloader.Win32.Cabby and HawkEye Keylogger. Unlike such popular spam extensions as ZIP and RAR, the CAB and ACE attachments may not always be recognized by users and thus cause less suspicion.



Ср 15.04.2015 11:29

Pearlie Kunicki <[redacted]>

Message from Briggs Equipment UK Ltd

Кому □ [redacted]

briggs_equipment_uk_ltd.cab (22 Кбайт)

Sender: +07407800718
Sender: Briggs Equipment UK Ltd
Date: 2015.04.15 08:27:56 CST
Pages: 5
ID: I2COWBC244692EC48
Filename: briggs_equipment_uk_ltd.cab

--
Pearlie Kunicki

Чт 30.04.2015 1:35

Selene Dellosso <[redacted].com>

4 pages from +07408992052

Кому □ [redacted]

W5BE522684275DC.cab (18 Кбайт)

Number: +07408992052
Size: 3325
ID: W5BE522684275DC
Filename: W5BE522684275DC.cab

--
Selene Dellosso

Вс 03.05.2015 1:45

[redacted].org

INVOICE

Кому □ undisclosed-recipients:

INVOICE.ace (340 Кбайт)

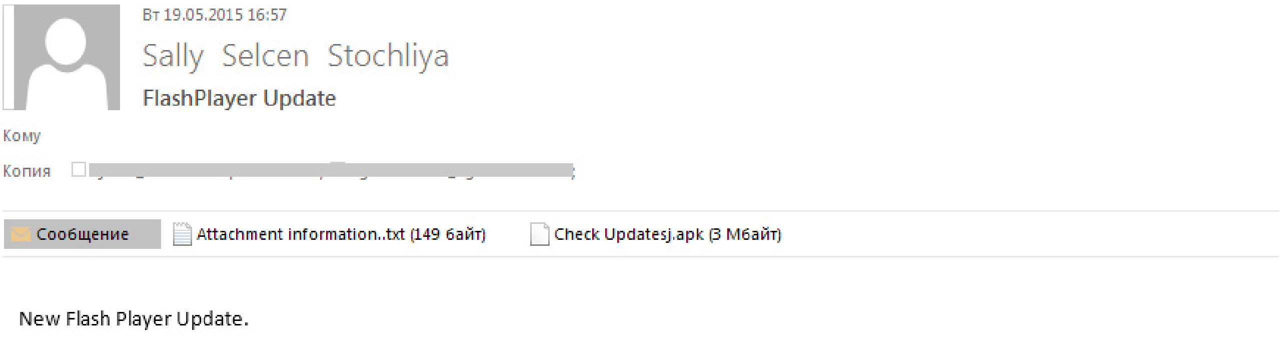
Please find attach copy of invoice we receive from you, and reconfirm to us before we proceed with the payment.

Thanks & Regards

Michael Wells.
Marketing Specialist

Kukuljanovo.312
51227 Kukuljanovo-Rijeka-Croatia
Tel:+385 (51)51 503 107

In Q2 2015, scammers distributed attached malicious ZIP and APK files within the framework of one mass mailing. If ZIP files are found in the majority of spam messages, APK files are relatively rare because they are archived executable application files for Android. The ZIP archives contained the Upatre family Trojan, while the file Check_Updatesj.apk was detected as the encryption Trojan SLocker for Android: when run, it encrypts images, documents and video files stored on the device. After that, the message is displayed to the user asking him to pay for decrypting the files. In sending malware in attached malicious ZIP and APK files, within the framework of one mass mailing, the scammers may have thought that they could trap not only PC users but the owners of Android-based smartphones and tablets working with e-mail from these devices.



Вт 19.05.2015 16:57

Sally Selcen Stochliya

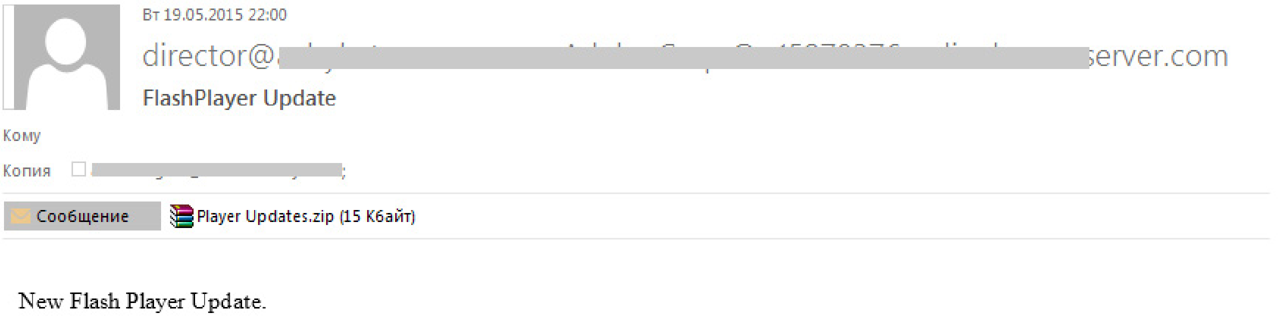
FlashPlayer Update

Кому

Копия □ [redacted]

Сообщение Attachment information..txt (149 байт) Check Updatesj.apk (3 Мбайт)

New Flash Player Update.



Вт 19.05.2015 22:00

director@[redacted]server.com

FlashPlayer Update

Кому

Копия □ [redacted]

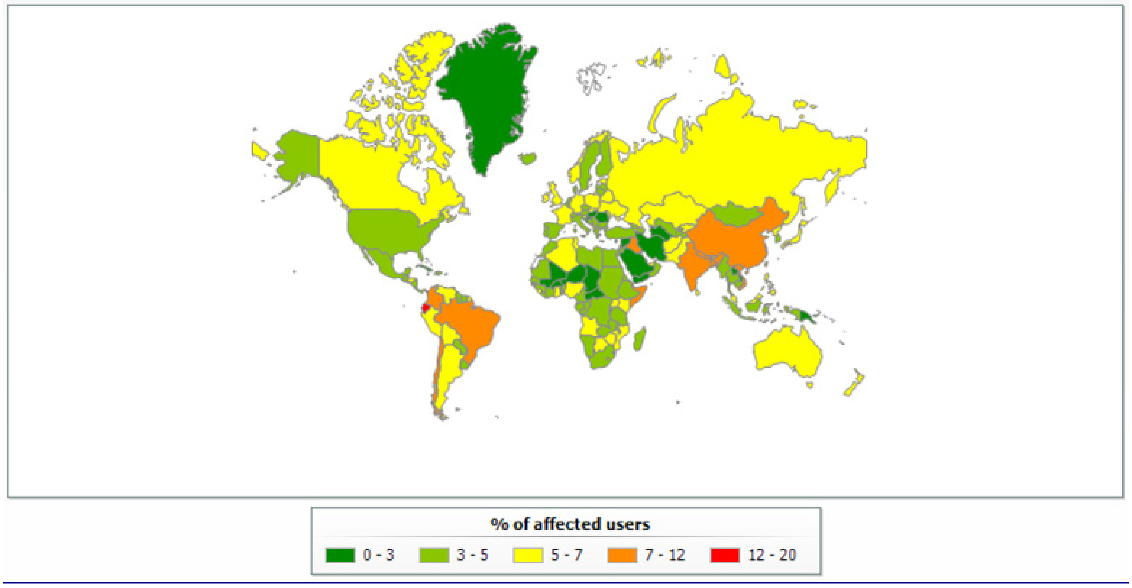
Сообщение Player Updates.zip (15 Кбайт)

New Flash Player Update.

PHISHING

In Q2 2015, the Anti-Phishing system was triggered 30,807,071 times on computers of Kaspersky Lab users. 509,905 masks of phishing URLs were added to the Kaspersky Lab databases over this period.

For several quarters in a row, the largest percentage of users affected by phishing attacks was in Brazil, although in Q2 2015 the number fell by half compared to the previous quarter. The same thing happened to the phishing numbers in many other countries.



Geography of phishing attacks, Q2 2015*

* Number of users on whose computers the Anti-Phishing system was triggered as a percentage of the total number of Kaspersky Lab users in the country

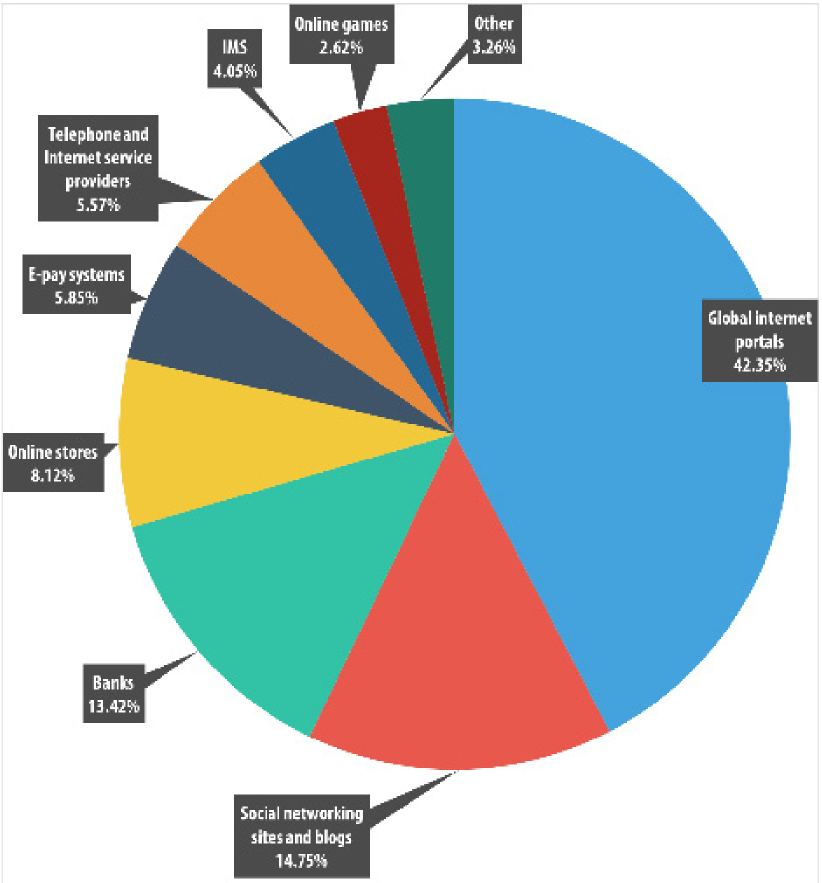
Top 10 countries by percentage of users attacked:

	Country	% of users
1	Brazil	9.74
2	India	8.3
3	China	7.23
	Россия	6,78
4	Russia	6.78
	Япония	5,93
5	France	6.54
6	Japan	5.93
	Казахстан	5,79
7	Malaysia	5.92
8	Poland	5.81
9	Kazakhstan	5.79
10	UAE	5.75

Organisations under attack

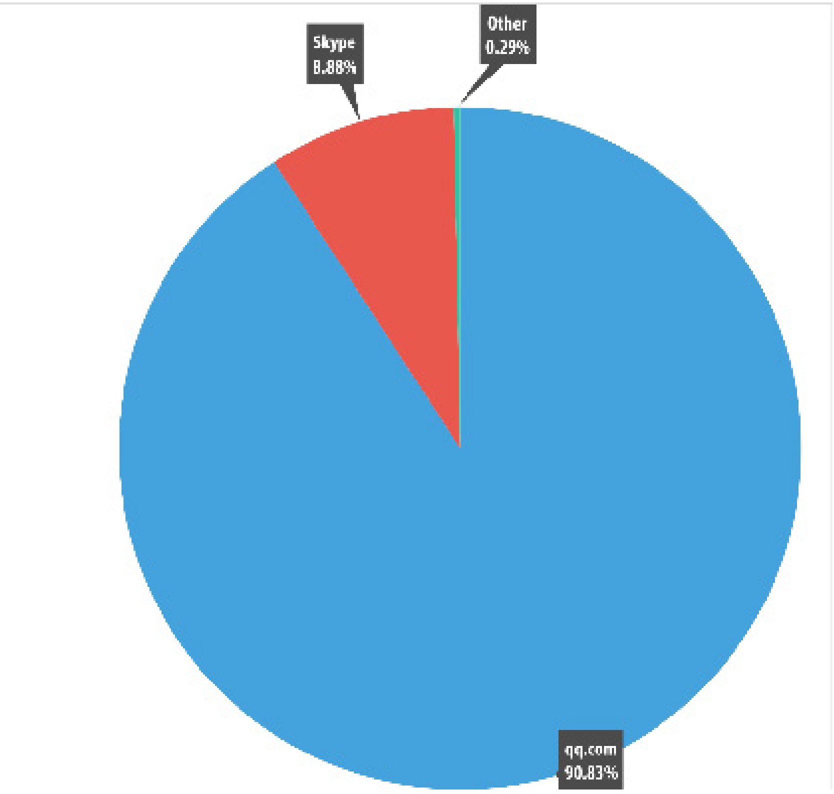
The statistics on phishing attack targets are based on the heuristic component of the Anti-Phishing system being triggered. The heuristic component of Anti-Phishing is triggered when the user follows a link to a phishing page information on which is not yet included in Kaspersky Lab databases, regardless of the way in which the page was reached – as a result of clicking on a link in a phishing email, a message on a social network or, for example, as a result of a malicious program's operation. When the component is triggered, it displays a banner in the browser, warning the user of a possible threat.

In the second quarter of 2015, the "Global Internet portals" category topped the rating of organizations attacked by phishers – its share increased by 2.78 percentage points from the previous quarter and accounted for 42.35%. The percentage of the "IMS" category (4.05%) also grew slightly (+0.13 percentage points) while the other categories showed a decline: "Social networking sites" lost 2.6 percentage points, "Banks" – 5.56 percentage points, "Online stores" – 1.56 percentage points, "E-pay systems" – 2.84 peercentage points, "Telephone and Internet service providers" – 1.33 percentage points, "Online games" – 0.78 percentage points.



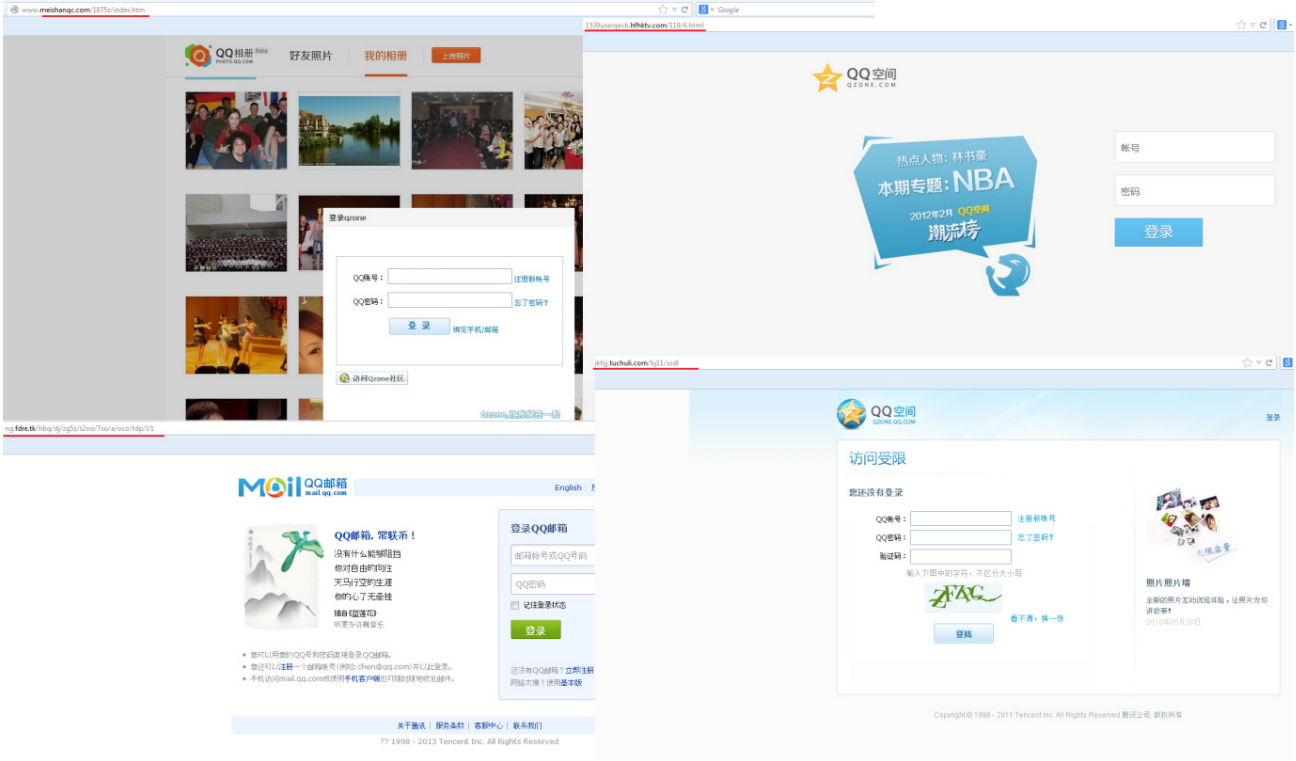
Distribution of organizations affected by phishing attacks, by category, Q2 2015

Instant messaging services are popular with fraudsters for many reasons. For example, cybercriminals often use stolen accounts for sending out phishing emails or links to malicious programs to the email addresses registered in the victim's list of contacts, distributing spam, extorting money and other fraudulent schemes.



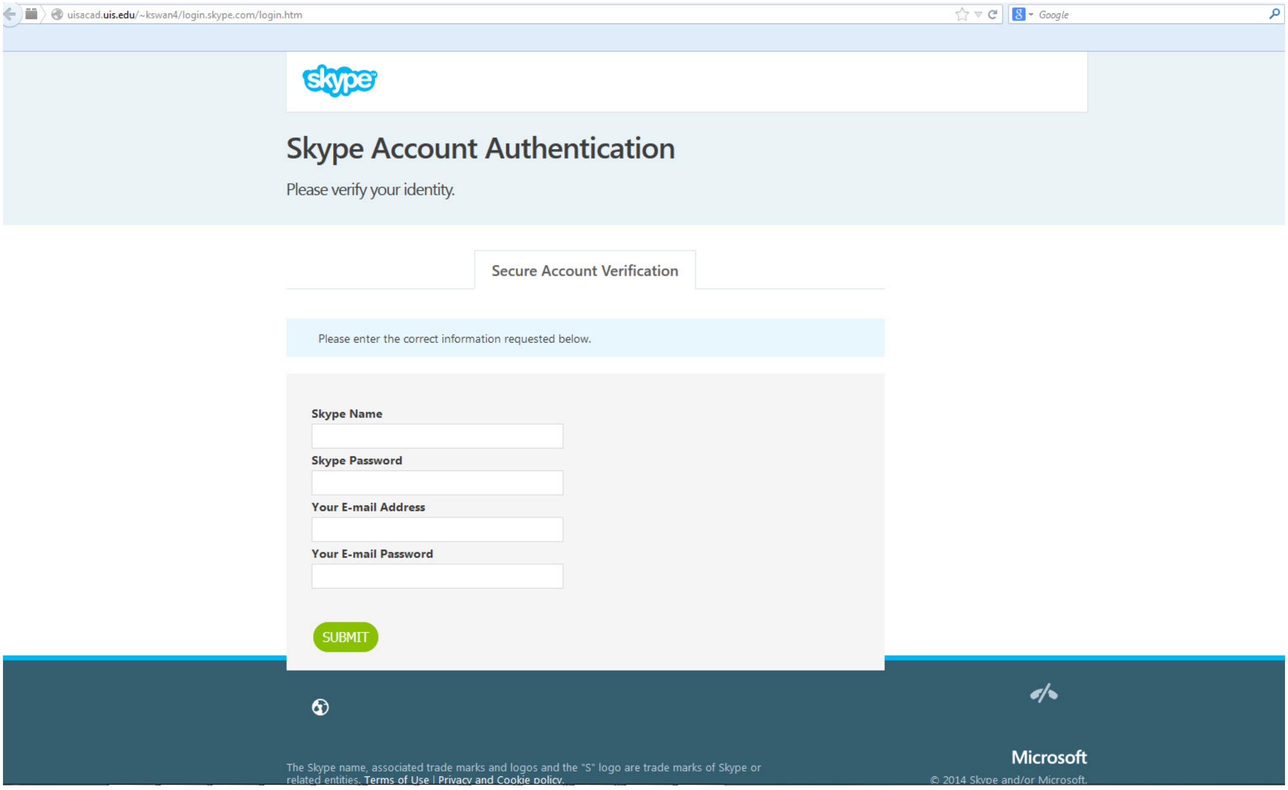
Distribution of phishing attacks on IMS, Q2 2015

Most of the Anti-Phishing system activations in this category fall on the popular Chinese instant messaging service QQ, supported by the Tencent telecommunications company.



Phishing pages imitating QQ personal account login pages.

Second comes Skype (8.88%) owned by Microsoft. Its share is incomparably smaller than that of the leader in this category.


uisacad.uis.edu/~kswan4/login.skype.com/login.htm

Google

skype

Skype Account Authentication

Please verify your identity.

Secure Account Verification

Please enter the correct information requested below.

Skype Name

Skype Password

Your E-mail Address

Your E-mail Password

SUBMIT

The Skype name, associated trade marks and logos and the "S" logo are trade marks of Skype or related entities. Terms of Use | Privacy and Cookie policy.

Microsoft

© 2014 Skype and/or Microsoft.

Phishing page inviting Skype users to verify their personal account

Top 3 organizations attacked

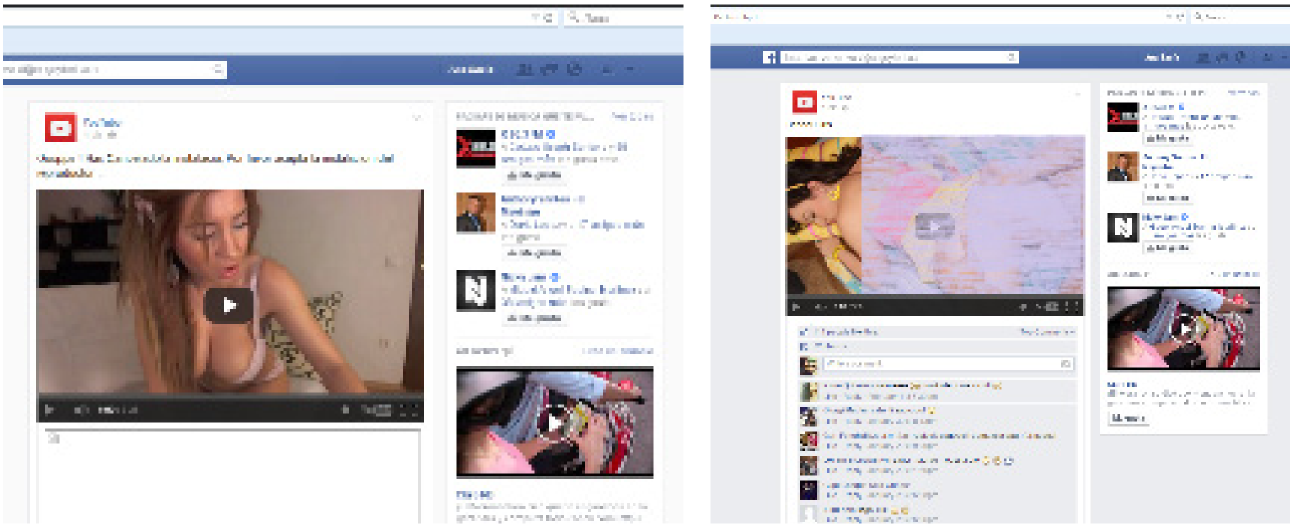
As we have written in our previous reports, the biggest part of non-spear phishing attacks targets the users of a small group of popular companies with many customers around the world. In this way fraudsters are trying to increase their chances of hitting the target by organizing yet another phishing attack.

The Top 3 organizations most often attacked by phishers accounts for 45.14% of all detected phishing links.

	Organization	% of all detected phishing links
1	Yahoo!	29.03%
2	Facebook	10.44%
3	Google	5.67%

The top three organizations targeted by phishers remained unchanged from the previous quarter. It includes Yahoo! (+23.82 percentage points), Facebook (-0.53 percentage points) and Google (-2.44 percentage points). A considerable increase in the proportion of detections of fake Yahoo! pages became possible due to the general decrease in the number of detections; in terms of numbers, the quantity of fake Yahoo! page detections increased only insignificantly.

In Q2 2015, we came across a huge number of phishing pages which imitated the publication of a Facebook page containing an intimate YouTube video. When trying to play the video, a malicious program was downloaded to the victim's computer.



Fake Facebook pages distributing malicious files

CONCLUSION

In Q2 2015, the percentage of spam in email traffic accounted for 53.4%, a drop of 5.8 percentage points from the previous quarter.

In the second quarter the stories contained in "Nigerian" letters were based on real events: the upcoming Olympic Games in Rio de Janeiro, the presidential elections in Nigeria, as well as the earthquake in Nepal. Fraudsters lured the recipients not only by promising rewards or compensation, but by mentioning lottery wins and asking for a donation for the victims of the earthquake in Nepal.

The increase in the amount of SEO spam was caused by the release of the Google Search algorithm update. The purpose of the update was to raise the sites adapted to mobile phones to a higher position in mobile search results.

In the second quarter of 2015 the top three sources of spam were the USA (14.59%), Russia (7.82%) and China (7.14%).

Trojan-Spy.HTML.Fraud.gen topped the rating of malicious programs sent by email. If popular malware families, rather than specific malicious programs, are ranked, Upatre headed the Q2 rating. Germany (19.59%) was the quarter's leader as the country most often targeted by mailshots.

Fraudsters continued to pass off attached malicious files as faxes and scans, Flash Player updates and business correspondence. They also continued to send out macro viruses in Word and Excel documents and they used CAB and ACE archives and APK files which are not typical for spam.

In Q2 2015, the Anti-Phishing system was triggered more than 30 million times on computers of Kaspersky Lab users. The largest percentage of users affected by phishing attacks was in Brazil, although the number fell by half from the previous quarter.

Securelist the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

Tel: +7-495-797-8700
+7-495-737-3412
Fax: +7-495-797-8709