KASPERSKY lab

SPAM AND PHISHING IN Q2 2016

By Darya Gudkova, Maria Vergelis, Nadezhda Demidova, Tatyana Shcherbakova

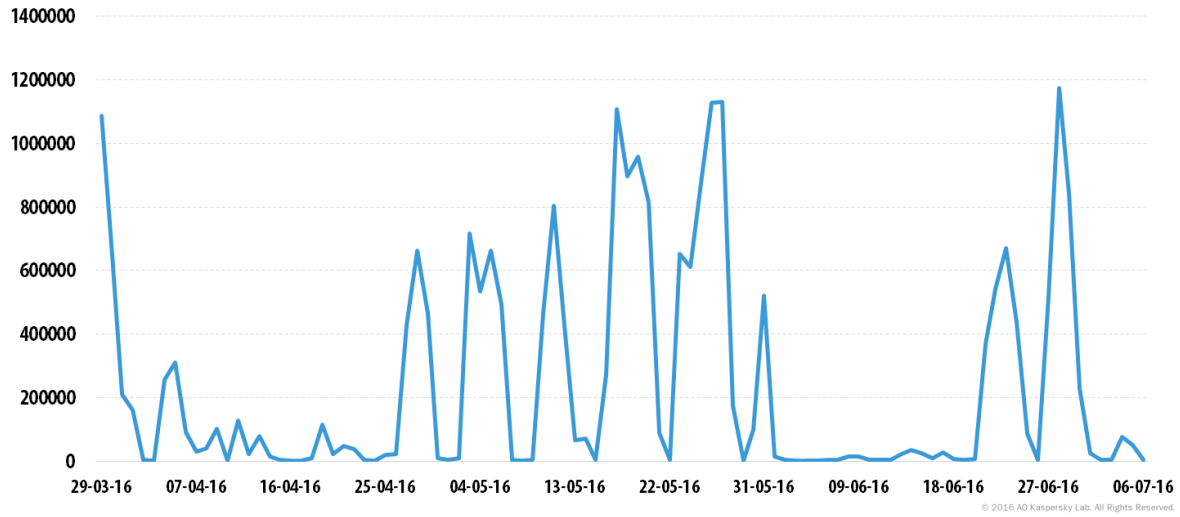
Contents

Spam: quarterly highlights

The year of ransomware in spam

Although the second quarter of 2016 has only just finished, it's safe to say that this is already the year of ransomware Trojans. By the end of Q2 there was still a large number of emails with malicious attachments, most of which download ransomware in one way or other to a victim's computer. However, in the period between 1 June and 21 June the proportion of these emails decreased dramatically.

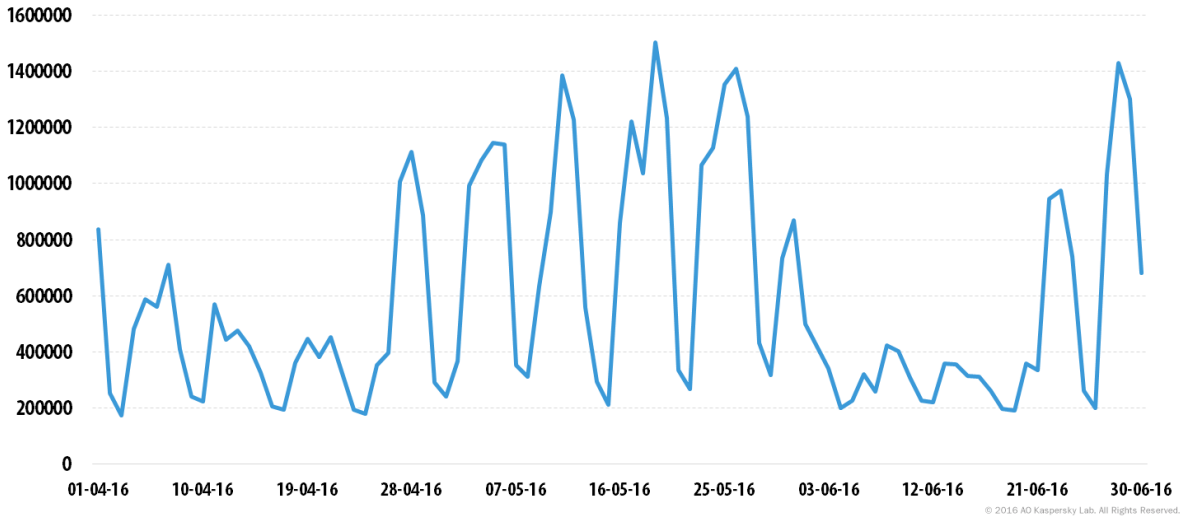
The majority of malicious attachments were distributed in ZIP archives. The decline can therefore be clearly seen in the following graph showing spam with ZIP attachments that arrived in our traps:



Number of emails with malicious ZIP archives, Q2 2016

In addition to the decline, June saw another interesting feature: this sort of spam was not sent out on Saturdays or Sundays.

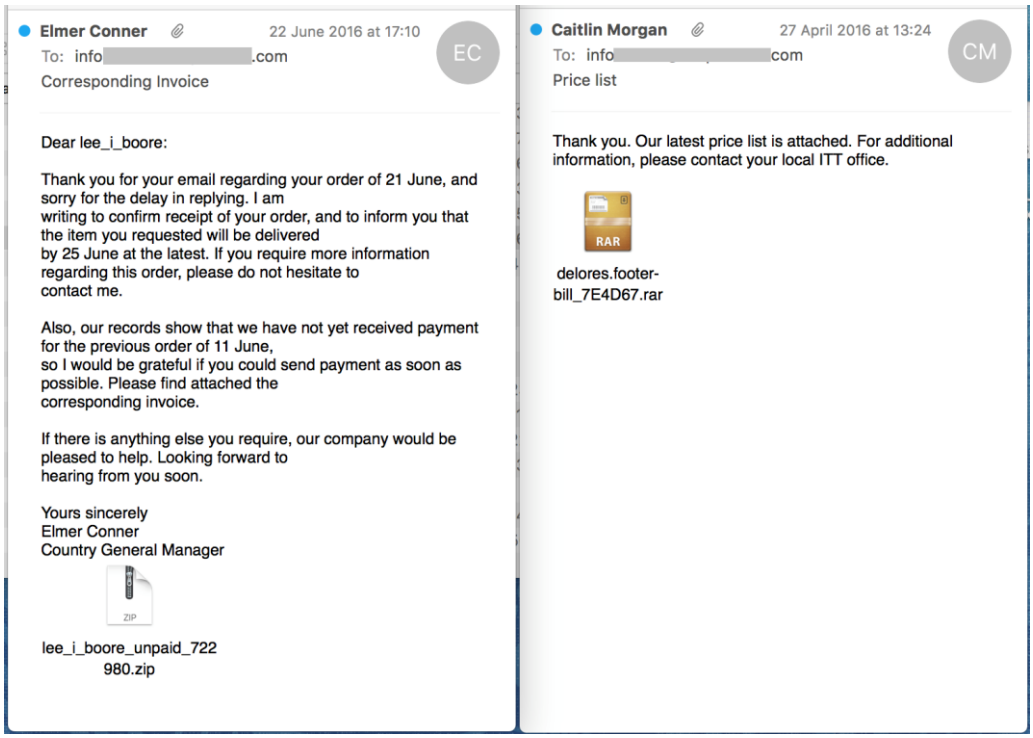
The same situation could be observed in KSN: the number of email antivirus detections dropped sharply on 1 June and grew on 22 June.



Number of email antivirus detections by day, Q2 2016

This decline was caused by a temporary lull in activity by the Necurs botnet, which is mostly used to distribute this type of malicious spam. After the botnet resumed its activity, the spam email template changed, and the malicious attachments became even more sophisticated.

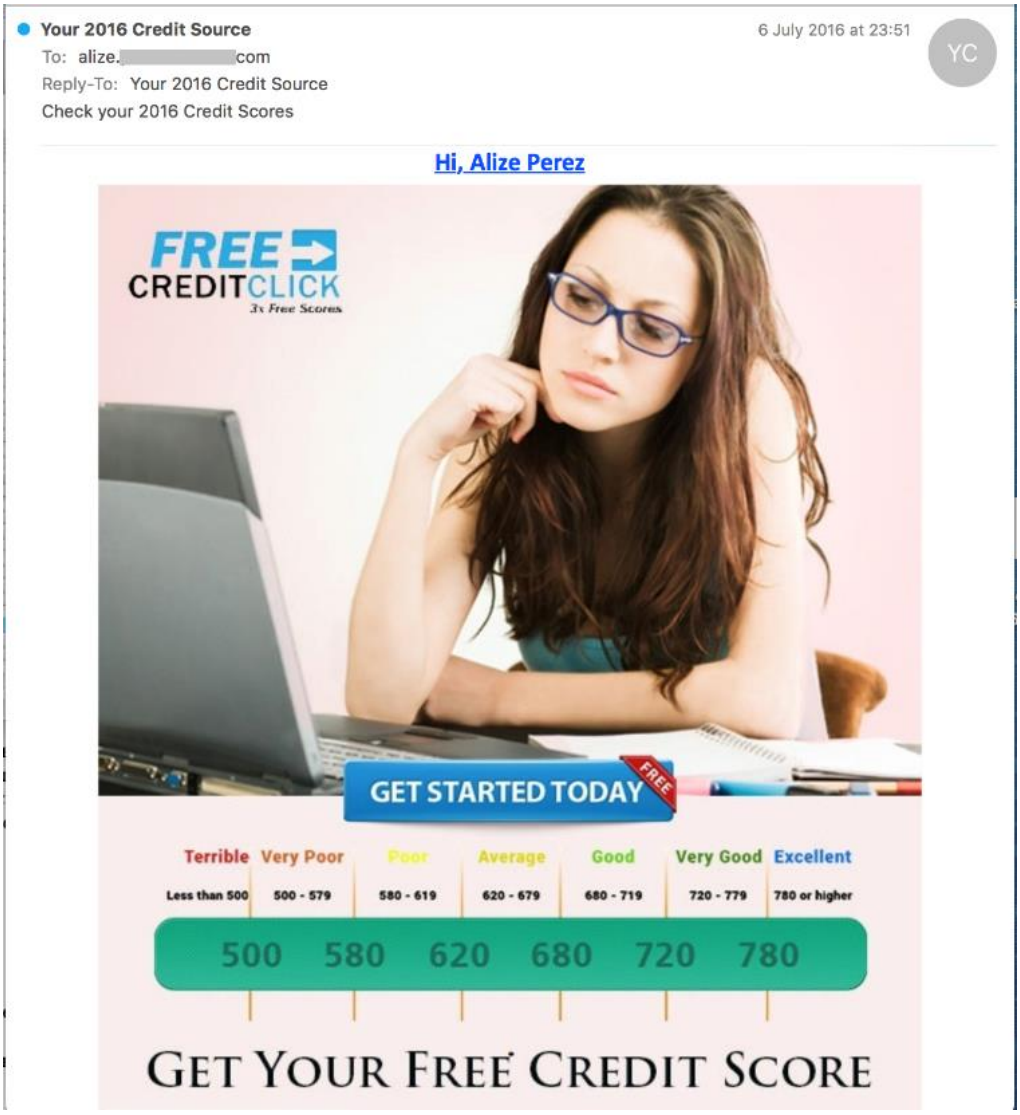
As in the previous quarter, the spam messages were mainly notifications about bills, invoices or price lists that were supposedly attached to the email. The attachments actually contained a Trojan downloader written in Javascript, and in most cases the malware loaded the Locky encryptor.



For example, some emails (see the screenshot above) contained an attachment with a Trojan downloader. When run, it downloaded Trojan-Ransom.Win32.Locky.agn, which encrypts the data on a victim's computer and demands a ransom, to be paid in bitcoin.

Obfuscation

The second quarter saw spammers continue to mask links using various Unicode ranges designed for specific purposes. This tactic became especially popular in 2015, and is still widely used by spammers.



The link in this example looks like this:

```
<A href=3D"http://=F0=9D=9A=96=F0=9D=9A=8A=F0=9D=9A=9B=F0=9D=9A=94=F0=9D=9A=
=8E=F0=9D=9A=9D=F0=9D=9A=9C=F0=9D=9A=9D=F0=9D=9A=8A=F0=9D=9A=97=F0=9D=9A=8D=
=F0=9D=9A=8A=F0=9D=9A=9B=F0=9D=9A=8D=F0=9D=9A=9C=EF=BC=8E=F0=9D=9A=98=F0=9D=
=9A=9B=F0=9D=9A=90/so31e.OP784QEVH?cDMjZTccvz8Dcvqwvcyczqckcfb91cmmc"><IMG =
```

If you transfer the domain from UTF-8 into the more familiar HTML, it becomes "marketstandards.org". The characters, which look quite ordinary, in fact belong to the Mathematical Alphanumeric Symbols UTF range used in highly specific mathematical formulas, and are not intended for use in plain text or hyperlinks. The dot in the domain is also unusual: it is the fullwidth full stop used in hieroglyphic languages. The rest of the hyperlink, as well as the rest of the text in these spam messages, is written using the Latin alphabet.

Spam in APT attacks

In Q2, we came across a number of APT attacks in the corporate sector. Emails were made to look as if they came from representatives of the targeted company, and contained a request to immediately transfer money to a specific account. The text was fairly plausible and hinted at a personal acquaintance and previous communication. In some cases, the emails included the logo of the attacked company. All the messages conveyed a sense of urgency ("ASAP", "urgent", "must be completed today") – scammers often use this trick in an attempt to catch people off guard, so that they act rather than think.

Below is an example:

Hello NNNNN,

How are you doing! Are you available at the office? I need you to process an overdue payment that needs to be paid today.

Thanks,

XXXXX

The emails were sent selectively – to individual employees, usually connected to the finance department. The knowledge shown by the scammers suggests the attack was carefully prepared.

The most suspicious aspect of the attack was the domain used in the 'From' field – myfirm.moby – that differed from the corporate one. Perhaps the attackers hope that some email clients only show the sender's name by default, while concealing the address.

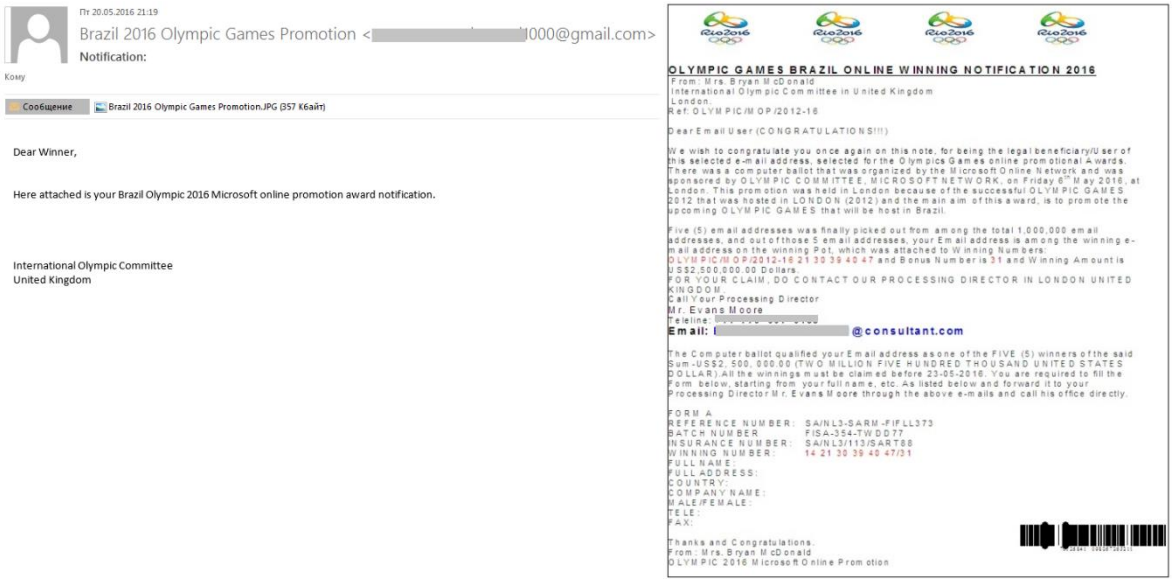
It is not that difficult to write any domain in the 'From' field, and in the future we can expect more well-prepared attacks.

Sporting events in spam

Spam mailings exploiting real-life events have long become an integral part of junk email. Sporting events are not as popular among spammers as political events, although their use is increasing with every year. There is a continuous stream of emails mentioning various political figures, while sport-related spam messages usually only appear in the run-up to an event. However, we have noticed that mass mailings can now be launched long before an event starts. For instance, emails exploiting the Olympic Games in Brazil were discovered over a year ago, in the second quarter of 2015. The majority of them were fraudulent emails designed to trick recipients and steal their personal information and money.

The classic scenario involves false notifications about lottery wins related to 2016 Olympics. The messages claim that the lottery was held by the official organizers of the games and the recipient was

selected at random from millions of addresses. In order to claim the cash, the recipient has to reply to the email and provide some personal information.



Пт 20.05.2016 21:19
Brazil 2016 Olympic Games Promotion <[redacted]000@gmail.com>
Notification:
Кому
Сообщение Brazil 2016 Olympic Games Promotion.JPG (357 Кбайт)

Dear Winner,

Here attached is your Brazil Olympic 2016 Microsoft online promotion award notification.

International Olympic Committee
United Kingdom

OLYMPIC GAMES BRAZIL ONLINE WINNING NOTIFICATION 2016

From: Mrs. Bryan McDonald
International Olympic Committee in United Kingdom
London.
Ref: OLYMPIC/MOP/2012-16

Dear Email User (CONGRATULATIONS!!!)

We wish to congratulate you once again on this note, for being the legal beneficiary/User of this selected e-mail address, selected for the Olympics Games online promotional Awards. There was a computer ballot that was organized by the Microsoft Online Network and was sponsored by OLYMPIC COMMITTEE, MICROSOFT NETWORK, on Friday 6TH May 2016, at London. This promotion was held in London because of the successful OLYMPIC GAMES 2012 that was hosted in LONDON (2012) and the main aim of this award, is to promote the upcoming OLYMPIC GAMES that will be host in Brazil.

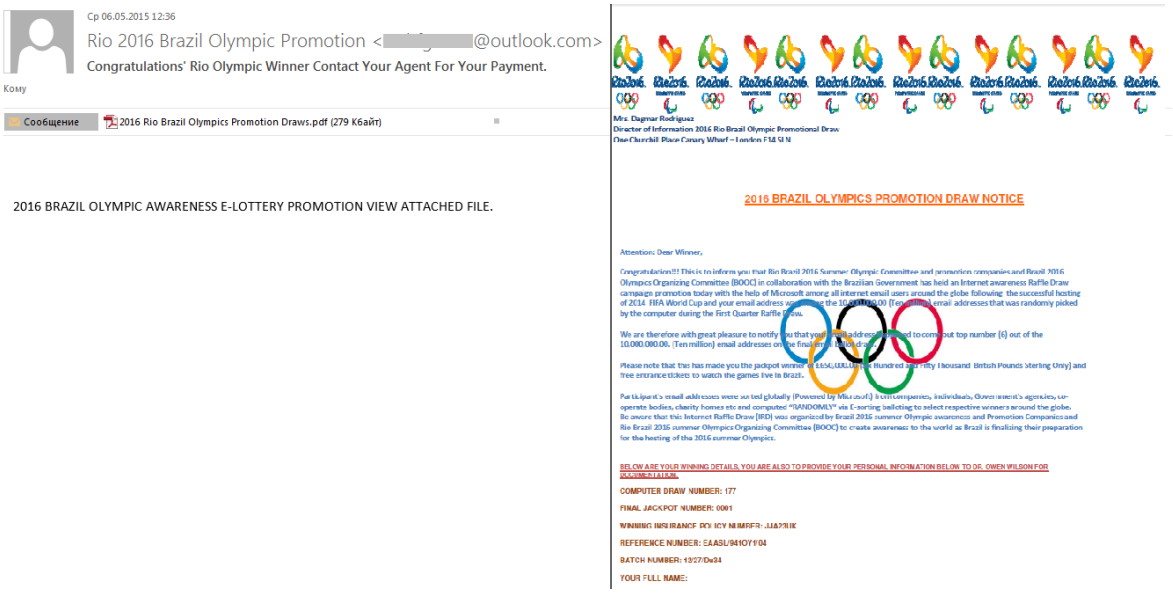
Five (5) email addresses was finally picked out from among the total 1,000,000 email addresses, and out of those 5 email addresses, your Email address is among the winning e-mail address on the winning Pot, which was attached to Winning Numbers:
OLYMPIC/MOP/2012-16 21 30 39 40 47 and Bonus Number is 31 and Winning Amount is US$2,500,000.00 Dollars.
FOR YOUR CLAIM, DO CONTACT OUR PROCESSING DIRECTOR IN LONDON UNITED KINGDOM.
Call Your Processing Director
Mr. Evans Moore
Teleline: [redacted]
Email: [redacted]@consultant.com

The Computer ballot qualified your Email address as one of the FIVE (5) winners of the said Sum-US$2, 500, 000.00 (TWO MILLION FIVE HUNDRED THOUSAND UNITED STATES DOLLAR). All the winnings must be claimed before 23-05-2016. You are required to fill the Form below, starting from your full name, etc. As listed below and forward it to your Processing Director Mr. Evans Moore through the above e-mails and call his office directly.

FORM A
REFERENCE NUMBER: SA/NL3-SARM-FIFLL373
BATCH NUMBER: FISA-354-TWDD77
INSURANCE NUMBER: SA/NL3/113/SART88
WINNING NUMBER: 14 21 30 39 40 47/31
FULL NAME:
FULL ADDRESS:
COUNTRY:
COMPANY NAME:
MALE/FEMALE:
TELE:
FAX:

Thanks and Congratulations.
From: Mrs. Bryan McDonald
OLYMPIC 2016 Microsoft Online Promotion

The text of the message was often contained in an attached file (.pdf, .doc, .jpg), while the body of the message only displayed a short text prompting the recipient to open the attachment.



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.

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

2016 BRAZIL OLYMPICS PROMOTION DRAW NOTICE

Attention: Dear Winner,

Congratulations!!! 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 [redacted] 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 [redacted] matched to come out top number (6) out of the 10,000,000.00. (Ten million) email addresses on the final [redacted]

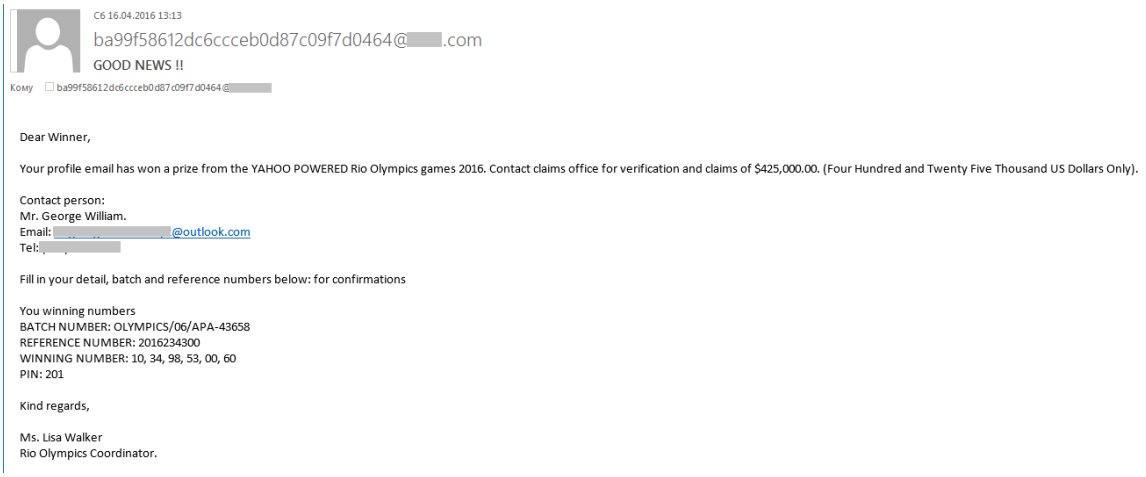
Please note that this has made you the jackpot winner of [redacted] Hundred and Fifty Thousand British Pounds Sterling Only) and free entrance tickets to watch the games live in Brazil.

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: JJA27UK
REFERENCE NUMBER: EAASL/941OY/104
BATCH NUMBER: 13/27/De34
YOUR FULL NAME:

There were also more traditional messages where the spammer text was included directly in the body of the message.



Сб 16.04.2016 13:13
ba99f58612dc6ccceb0d87c09f7d0464@[redacted].com
GOOD NEWS !!
Кому ba99f58612dc6ccceb0d87c09f7d0464@[redacted]

Dear Winner,

Your profile email has won a prize from the YAHOO POWERED Rio Olympics games 2016. Contact claims office for verification and claims of $425,000.00. (Four Hundred and Twenty Five Thousand US Dollars Only).

Contact person:
Mr. George William.
Email: [redacted]@outlook.com
Tel:[redacted]

Fill in your detail, batch and reference numbers below: for confirmations

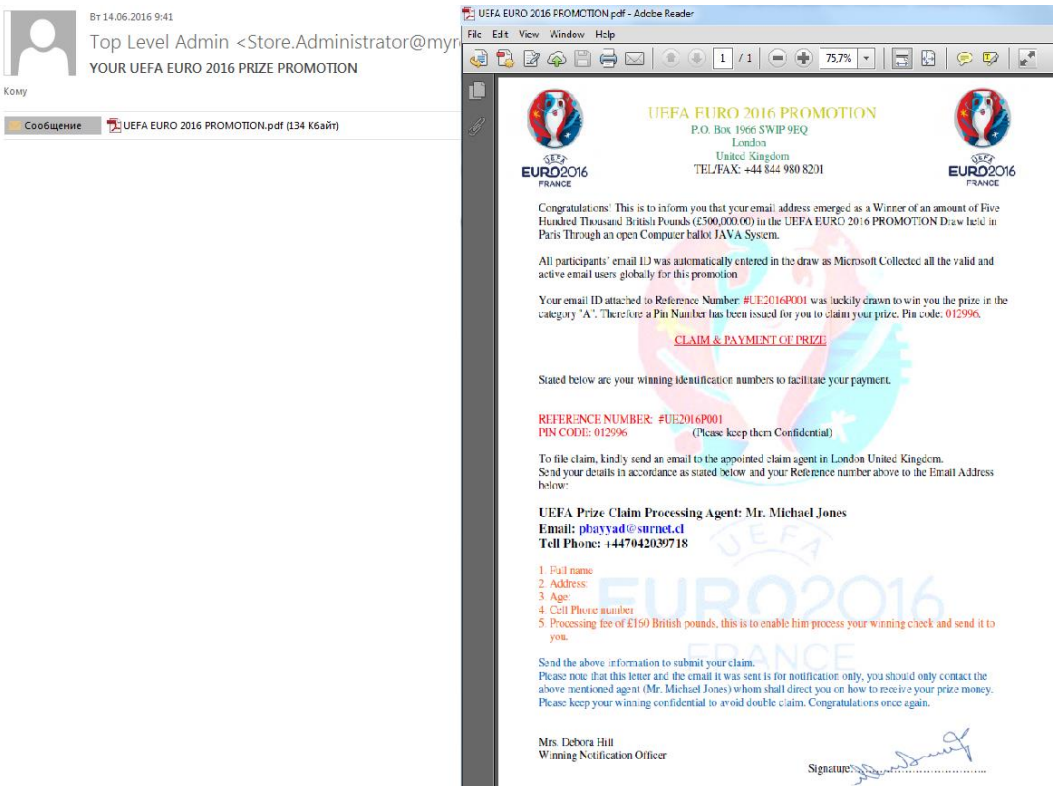
You winning numbers
BATCH NUMBER: OLYMPICS/06/APA-43658
REFERENCE NUMBER: 2016234300
WINNING NUMBER: 10, 34, 98, 53, 00, 60
PIN: 201

Kind regards,

Ms. Lisa Walker
Rio Olympics Coordinator.

In addition to fraudulent messages, advertising spam was also sent out.

Unlike the Olympics, football tournaments have long been used by scammers to grab people's attention to their spam. Q2 2016 saw the long-awaited UEFA European Championship, and in the run-up to the tournament spam traffic included fake notifications of lottery wins. The content was no different from that dedicated to the Olympic Games, and the emails also contained attachments explaining why the message was sent.



Вт 14.06.2016 9:41
Top Level Admin <Store.Administrator@myr[redacted]
YOUR UEFA EURO 2016 PRIZE PROMOTION
Кому
Сообщение UEFA EURO 2016 PROMOTION.pdf (134 Кбайт)

UEFA EURO 2016 PROMOTION.pdf - Adobe Reader
File Edit View Window Help

UEFA EURO 2016 PROMOTION
P.O. Box 1966 SW1P 9EQ
London
United Kingdom
TEL/FAX: +44 844 980 8201

Congratulations! This is to inform you that your email address emerged as a Winner of an amount of Five Hundred Thousand British Pounds (£500,000.00) in the UEFA EURO 2016 PROMOTION Draw held in Paris Through an open Computer ballot JAVA System.

All participants' email ID was automatically entered in the draw as Microsoft Collected all the valid and active email users globally for this promotion

Your email ID attached to Reference Number: #UE2016P001 was luckily drawn to win you the prize in the category "A". Therefore a Pin Number has been issued for you to claim your prize. Pin code: 012996.

CLAIM & PAYMENT OF PRIZE

Stated below are your winning identification numbers to facilitate your payment.

REFERENCE NUMBER: #UE2016P001
PIN CODE: 012996 (Please keep them Confidential)

To file claim, kindly send an email to the appointed claim agent in London United Kingdom.
Send your details in accordance as stated below and your Reference number above to the Email Address below:

UEFA Prize Claim Processing Agent: Mr. Michael Jones
Email: pbayyad@surnet.cl
Tell Phone: +447042039718

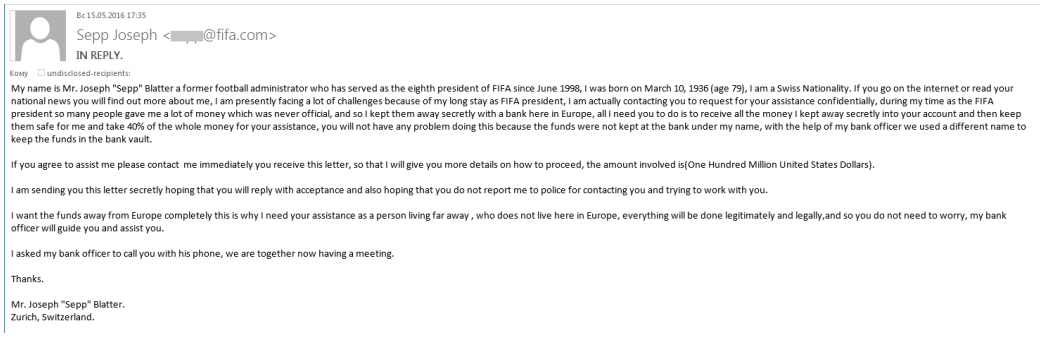
1. Full name
2. Address:
3. Age
4. Cell Phone number
5. Processing fee of £150 British pounds, this is to enable him process your winning check and send it to you.

Send the above information to submit your claim.
Please note that this letter and the email it was sent is for notification only, you should only contact the above mentioned agent (Mr. Michael Jones) whom shall direct you on how to receive your prize money.
Please keep your winning confidential to avoid double claim. Congratulations once again.

Mrs. Debora Hill
Winning Notification Officer
Signature:

The football theme was also exploited by 'Nigerian' scammers. They sent out emails supposedly on behalf of the former FIFA president, and used the infamous corruption scandal associated with his name to make their messages look more realistic. They believed that a fabricated story about how Sepp Blatter had supposedly received money and secretly transferred it to an account in a European

bank would not arouse suspicion. In return for keeping the money in their bank accounts, the recipients were promised a 40% cut of the total sum.



Вс 15.05.2016 17:35

Sepp Joseph <[redacted]@fifa.com>

IN REPLY.

Кому undisclosed-recipients:

My name is Mr. Joseph "Sepp" Blatter a former football administrator who has served as the eighth president of FIFA since June 1998, I was born on March 10, 1936 (age 79), I am a Swiss Nationality. If you go on the internet or read your national news you will find out more about me, I am presently facing a lot of challenges because of my long stay as FIFA president, I am actually contacting you to request for your assistance confidentially, during my time as the FIFA president so many people gave me a lot of money which was never official, and so I kept them away secretly with a bank here in Europe, all I need you to do is to receive all the money I kept away secretly into your account and then keep them safe for me and take 40% of the whole money for your assistance, you will not have any problem doing this because the funds were not kept at the bank under my name, with the help of my bank officer we used a different name to keep the funds in the bank vault.

If you agree to assist me please contact me immediately you receive this letter, so that I will give you more details on how to proceed, the amount involved is(One Hundred Million United States Dollars).

I am sending you this letter secretly hoping that you will reply with acceptance and also hoping that you do not report me to police for contacting you and trying to work with you.

I want the funds away from Europe completely this is why I need your assistance as a person living far away , who does not live here in Europe, everything will be done legitimately and legally,and so you do not need to worry, my bank officer will guide you and assist you.

I asked my bank officer to call you with his phone, we are together now having a meeting.

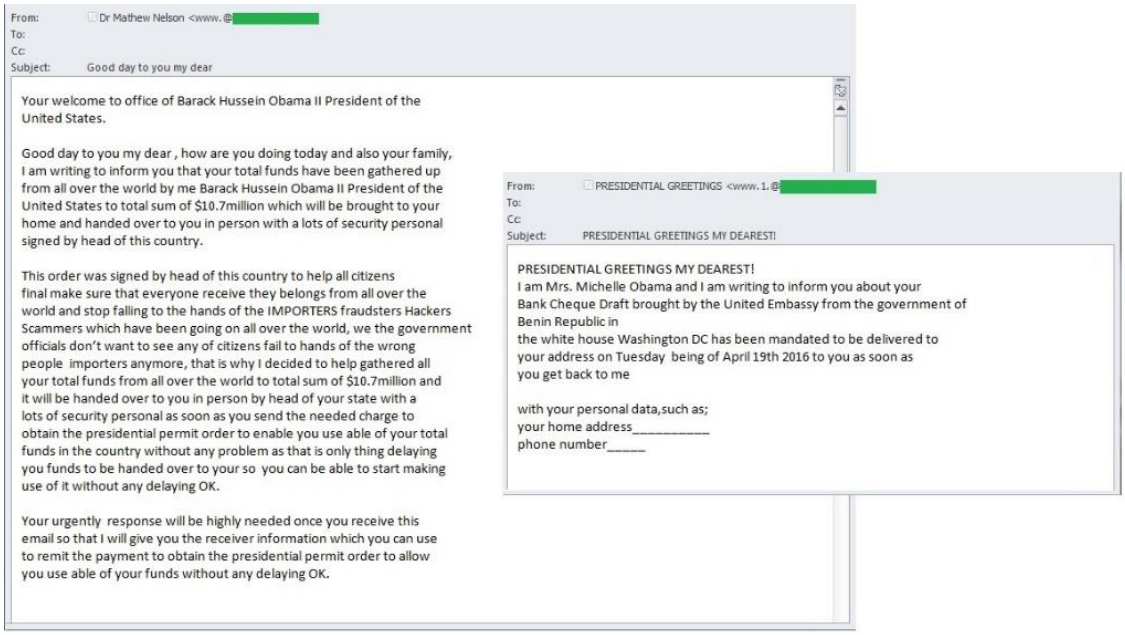
Thanks.

Mr. Joseph "Sepp" Blatter.
Zurich, Switzerland.

In order to convince recipients that the message was genuine, the authors even went to the trouble of using the correct name and domain in the 'From' field.

US politicians in spam

The presidential election campaign is now in full swing in the United States and the nominees and their entourages are under close media scrutiny. Of course, spammers couldn't resist using the names of high-profile politicians in their advertising and fraudulent emails. For example, numerous 'Nigerian' letters were sent in the name of current president Barack Obama and his wife Michelle. In their 'official' emails, the 'President' and the 'First lady' assured the recipient that a bank card or a check for a very large sum of money had already been issued in their name. The only thing the recipient had to do was complete some formalities, and the money would be delivered shortly afterwards. In order to get the instructions from the White House the recipient had to send some personal information, including their email address and the password for their email account, as well as detailed passport information to spoofed email addresses.



From: Dr Mathew Nelson <www.@[redacted]
To:
Cc:
Subject: Good day to you my dear

Your welcome to office of Barack Hussein Obama II President of the United States.

Good day to you my dear , how are you doing today and also your family, I am writing to inform you that your total funds have been gathered up from all over the world by me Barack Hussein Obama II President of the United States to total sum of $10.7million which will be brought to your home and handed over to you in person with a lots of security personal signed by head of this country.

This order was signed by head of this country to help all citizens final make sure that everyone receive they belongs from all over the world and stop falling to the hands of the IMPORTERS fraudsters Hackers Scammers which have been going on all over the world, we the government officials don't want to see any of citizens fail to hands of the wrong people importers anymore, that is why I decided to help gathered all your total funds from all over the world to total sum of $10.7million and it will be handed over to you in person by head of your state with a lots of security personal as soon as you send the needed charge to obtain the presidential permit order to enable you use able of your total funds in the country without any problem as that is only thing delaying you funds to be handed over to your so you can be able to start making use of it without any delaying OK.

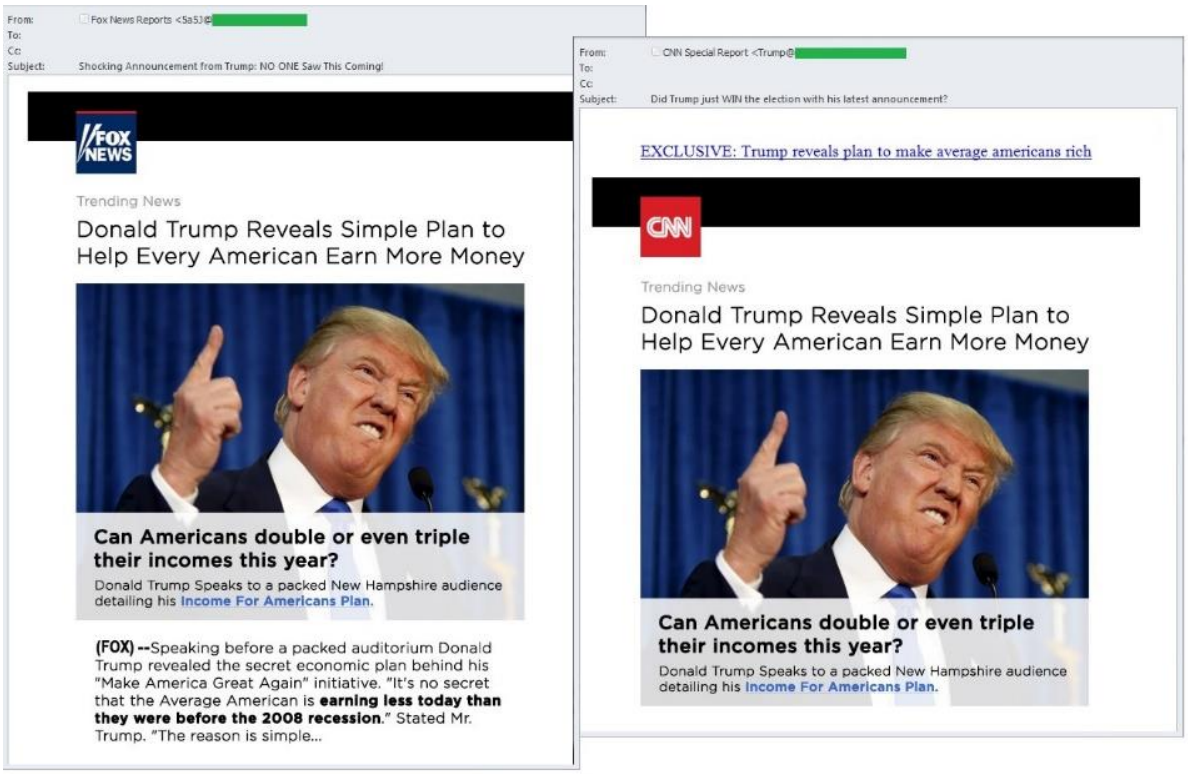
Your urgently response will be highly needed once you receive this email so that I will give you the receiver information which you can use to remit the payment to obtain the presidential permit order to allow you use able of your funds without any delaying OK.

From: PRESIDENTIAL GREETINGS <www.1.@[redacted]
To:
Cc:
Subject: PRESIDENTIAL GREETINGS MY DEAREST!

PRESIDENTIAL GREETINGS MY DEAREST!
I am Mrs. Michelle Obama and I am writing to inform you about your Bank Cheque Draft brought by the United Embassy from the government of Benin Republic in
the white house Washington DC has been mandated to be delivered to your address on Tuesday being of April 19th 2016 to you as soon as you get back to me

with your personal data,such as;
your home address_____
phone number_____

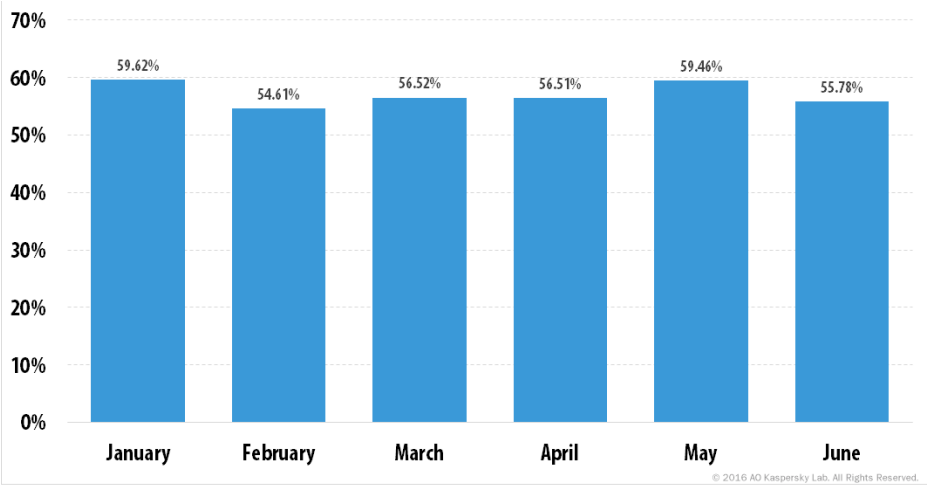
Another politician whose name regularly cropped up in spam was Donald Trump, one of the contenders for the US presidency. Spammers offered a unique Trump technique for earning money online: anyone who wanted to know how to get rich, had to click a link in the emails which were designed to look like news reports from CNN and Fox News.



The links led to fake news sites also in the style of major media outlets and news networks. The sites contained a story about a simple method for earning money – the publication of links, which is basically another kind of spam distribution. In order to participate in the program, a user had to register by providing their phone number and email address.

Statistics

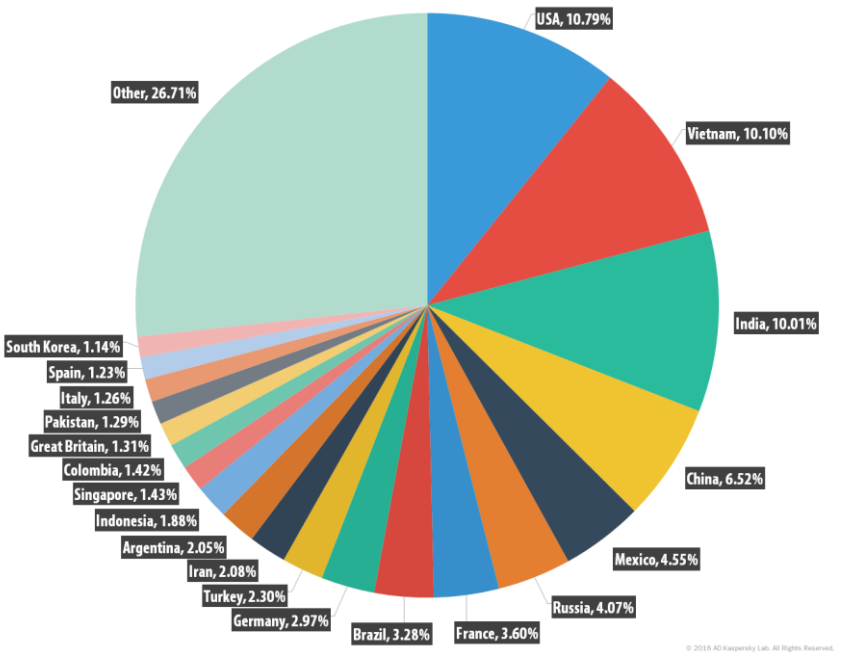
Proportion of spam in email traffic



Percentage of spam in global email traffic, Q2 2016

The largest percentage of spam in the second quarter – 59.46% – was registered in May and was 3 p.p. more than in April. The average percentage of spam in global email traffic for Q2 amounted to 57.25%.

Sources of spam by country

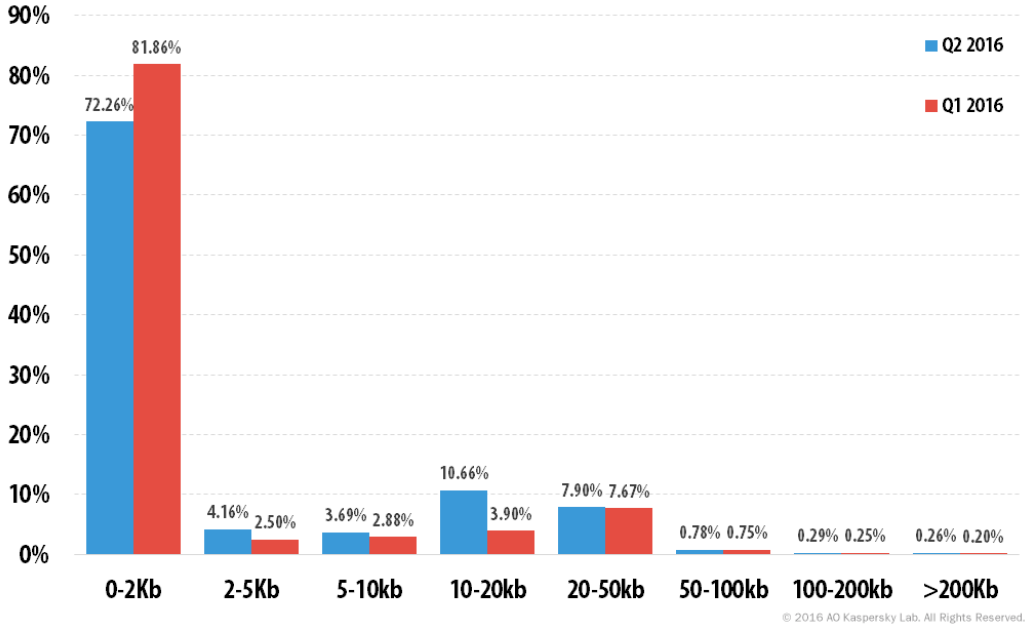


Sources of spam by country, Q2 2016

In Q2 2016, the biggest three sources of spam remained the same as in the previous quarter – the US (10.79%), Vietnam (10.10%) and India (10.01%). However, the figures for each country changed: the gap between them narrowed to within a single percentage point.

China (6.52%) moved up to fourth with an increase of 1.43 p. p. compared to Q1. Mexico (4.55%) came fifth, followed by Russia (4.07%) and France (3.60%). Brazil (3.28%), which was fourth in the previous quarter, lost 2.2 p.p. and dropped to eighth place. Germany (2.97%) and Turkey (2.30%) completed the TOP 10.

Spam email size



Breakdown of spam emails by size, Q1 and Q2 2016

Traditionally, the most commonly distributed emails are very small – up to 2 KB (72.26%), although the proportion of these emails dropped by 9.6 p.p. compared to the previous quarter. Meanwhile, the share of emails sized 10-20 KB increased by 6.76 p.p. The other categories saw minimal changes.

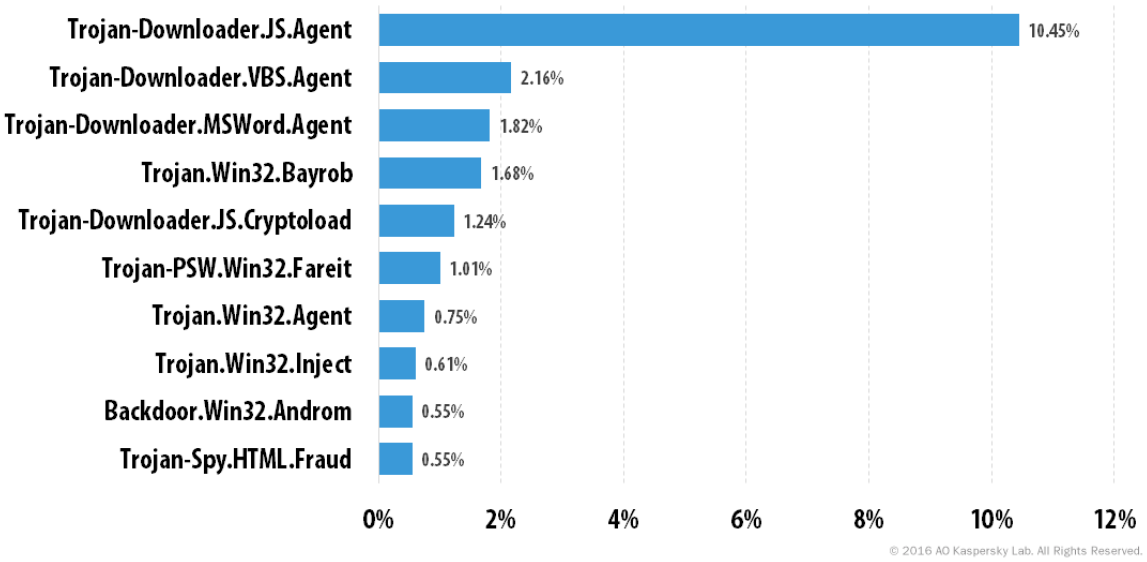
Malicious email attachments

Currently, the majority of malicious programs are detected proactively by automatic means, which makes it very difficult to gather statistics on specific malware modifications. So we have decided to turn to the more informative statistics of the TOP 10 malware families.

TOP 10 malware families

The three most popular malware families remained unchanged from the previous quarter – Trojan-Downloader.JS.Agent (10.45%), Trojan-Downloader.VBS.Agent (2.16%) and Trojan-Downloader.MSWord.Agent (1.82%).

The Trojan.Win32.Bayrob family moved up to fourth place (1.68%), while the Backdoor.Win32.Androm family fell from fourth to ninth place with 0.6%.

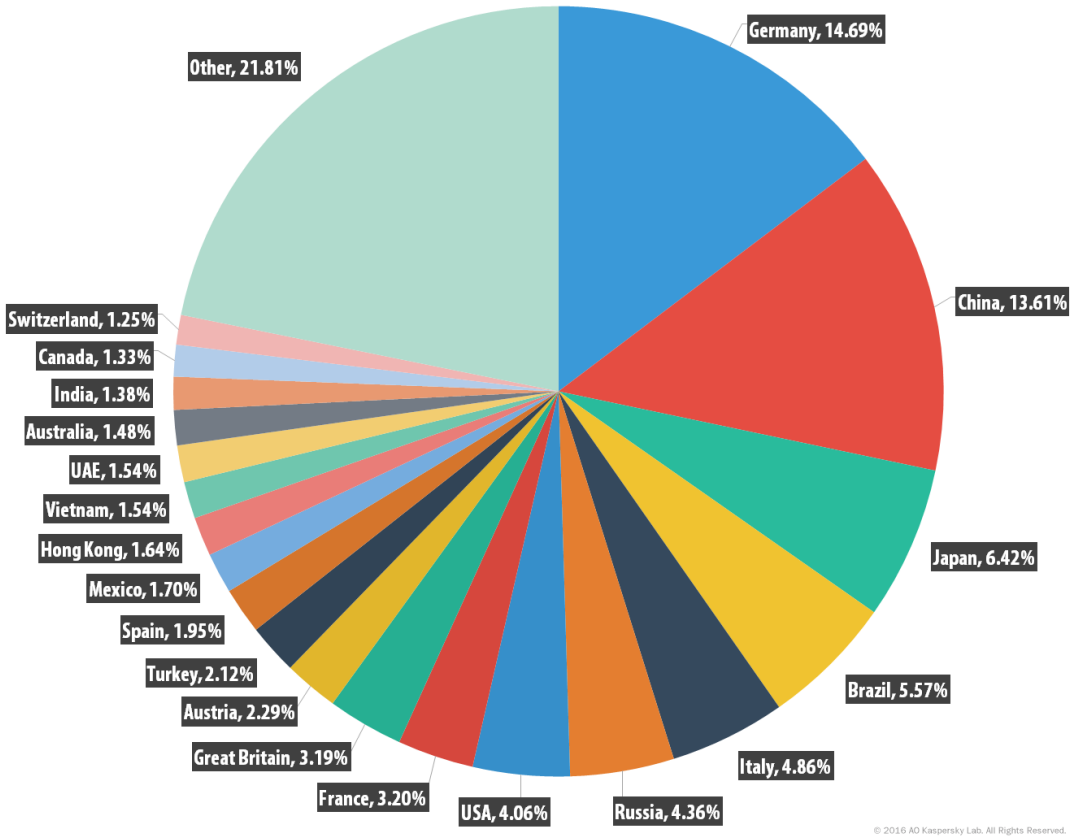


TOP 10 malware families in Q2 2016

A newcomer to this ranking was the Trojan.Win32.Inject family (0.61%). The malicious programs from this family embed their code in the address space of other processes.

The Trojan-Spy.HTML.Fraud family (0.55%) rounded off the TOP 10 in Q2 2016.

Countries targeted by malicious mailshots



Distribution of email antivirus verdicts by country, Q2 2016

Germany (14.69%) topped the ranking of countries targeted by malicious mailshots, although its share decreased 4.24 p.p. It was followed by China (13.61%) whose contribution grew 4.18 p.p. Japan (6.42%) came third after ending the previous quarter in seventh with a share of 4.29%.

Fourth place was occupied by Brazil (5.57%). Italy claimed fifth with a share of 4.9% and Russia remained in sixth (4.36%).

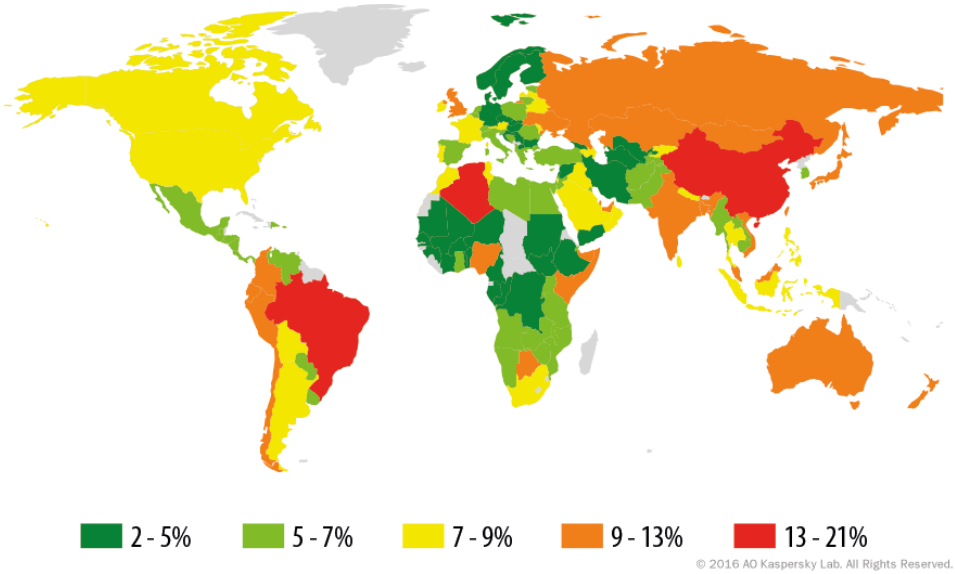
The US (4.06%) was the seventh most popular target of malicious mailshots. Austria (2.29%) rounded off this TOP 10.

Phishing

In Q2 2016, the Anti-Phishing system was triggered 32,363,492 times on the computers of Kaspersky Lab users, which is 2.6 million less than the previous quarter. Overall, 8.7% of unique users of Kaspersky Lab products were attacked by phishers in Q2 of 2016.

Geography of attacks

The country where the largest percentage of users is affected by phishing attacks was China (20.22%). In Q2 2016, the proportion of those attacked increased by 3.52 p.p.



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*

The percentage of attacked users in Brazil decreased by 2.87 p.p. and accounted for 18.63%, placing the country second in this ranking. Algeria (14.3%) came third following a 2.92 p.p. increase in its share compared to the previous quarter.

TOP 10 countries by percentage of users attacked:

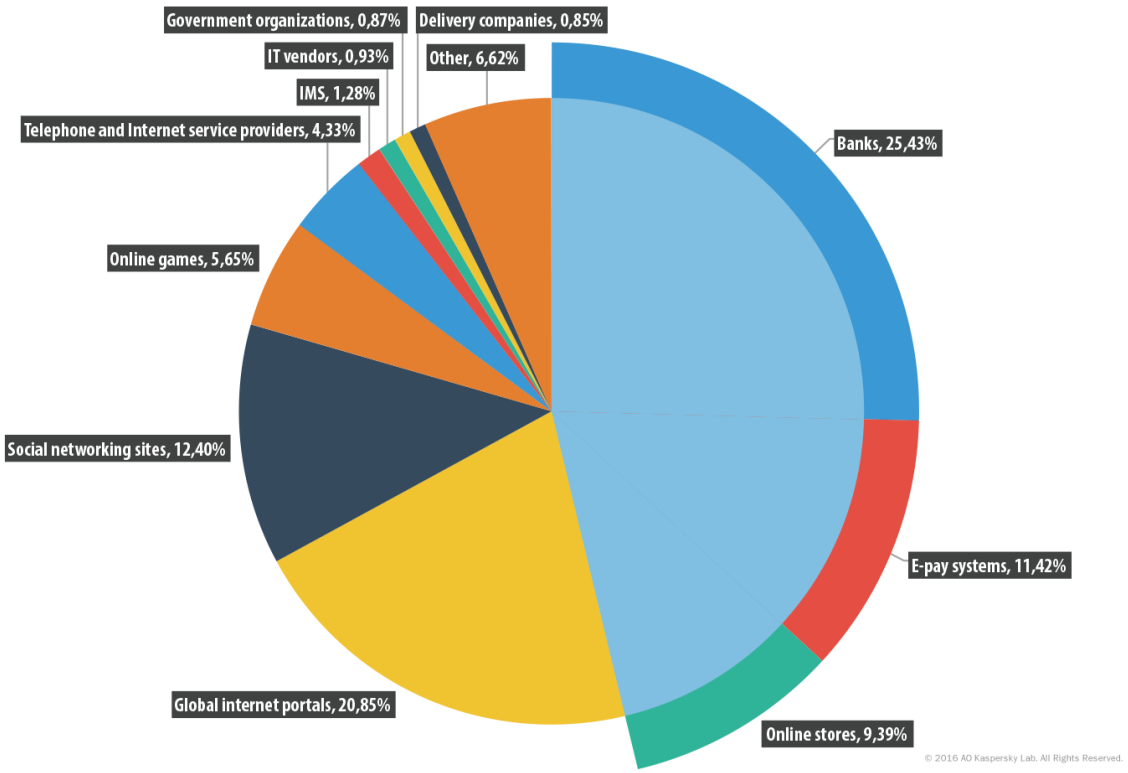
China	20.22%
Brazil	18.63%
Algeria	14.3%
United Kingdom	12.95%
Australia	12.77%

Vietnam	11.46%
Ecuador	11.14%
Chile	11.08%
Qatar	10.97%
Maldives	10.94%

Organizations under attack

The statistics on phishing targets are based on detections of Kaspersky Lab's heuristic anti-phishing component. It is activated every time a user attempts to open a phishing page while information about it has not yet been included in Kaspersky Lab's databases. It does not matter how the user attempts to open the page – by clicking a link in a phishing email or in a message on a social network or, for example, as a result of malware activity. After the security system is activated, a banner is displayed in the browser warning the user about a potential threat.

In Q2 of 2016, the share of the 'Global Internet portals' category (20.85%), which topped the rating in the first quarter, decreased considerably – by 7.84 p.p. The share of the 'Financial organizations' category grew 2.07 p.p. and accounted for 46.23%. This category covers 'Banks' (25.43%, +1.51 p.p.), 'Payment systems' (11.42%, -0.42 p.p.) and 'Online stores' (9.39%, +0.99 p.p.).



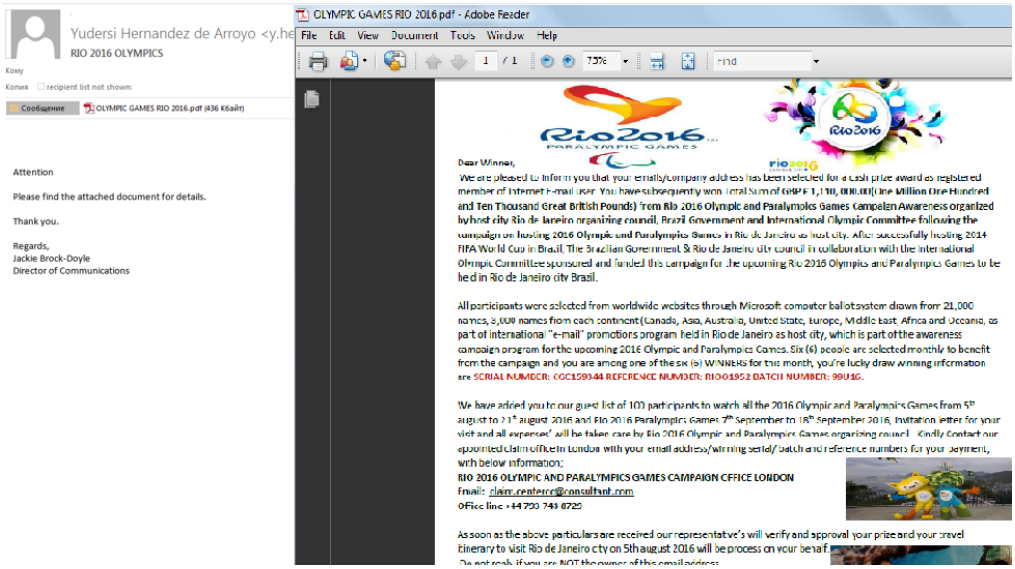
Distribution of organizations affected by phishing attacks by category, Q2 2016

The share of attacks on the 'Social networking sites' category increased by 2.65 p.p. and reached 12.4%. The 'Online games' category was also attacked more often (5.65%, + 1.96 p.p.). Meanwhile, the 'Telephone and Internet service providers' (4.33%) and the 'IMS' (1.28%) categories lost 1.17 p.p. and 2.15 p.p. respectively.

Hot topics this quarter

The Olympics in Brazil

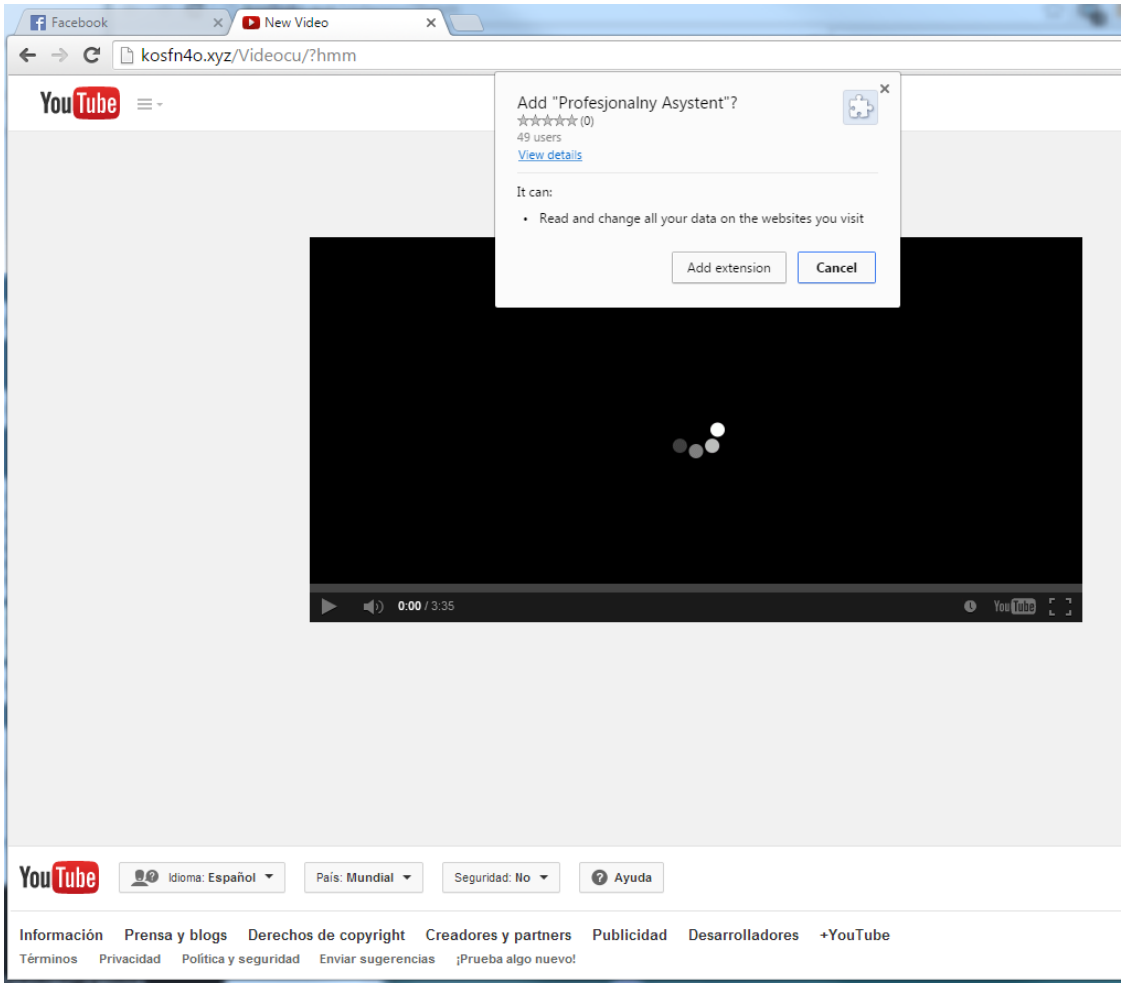
For a number of years now Brazil has been among the countries with the highest proportion of users targeted by phishing. In 2015 and 2016 phishers have focused on the Rio Olympic Games in Brazil. Last quarter showed that as well as ordinary users, the potential victims of phishing included the organizers of the Olympic Games.



The Olympic theme remained popular in Q2, with phishers working overtime to send out fake notifications about big cash wins in a lottery that was supposedly organized by the Brazilian government and the Olympic Committee.

'Porn virus' for Facebook users

Facebook users are often subjected to phishing attacks. During one attack in the second quarter, a provocative video was used as bait. To view it, the user was directed to a fake page imitating the popular YouTube video portal, and told to install a browser extension.

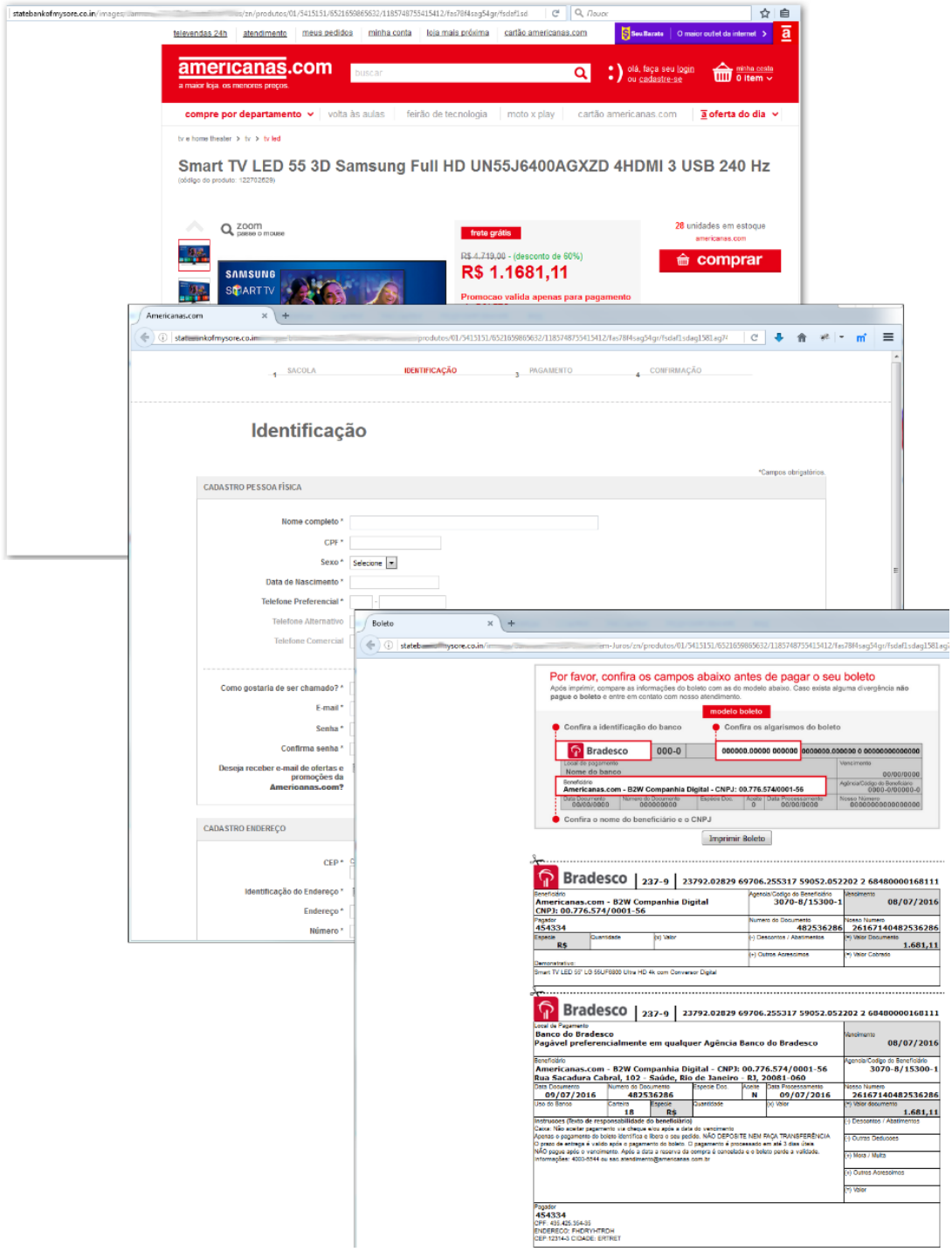


This extension requested rights to read all the data in the browser, potentially giving the cybercriminals access to passwords, logins, credit card details and other confidential user information. The extension also distributed more links on Facebook that directed to itself, but which were sent using the victim's name.

Phisher tricks

Compromising domains with good reputation

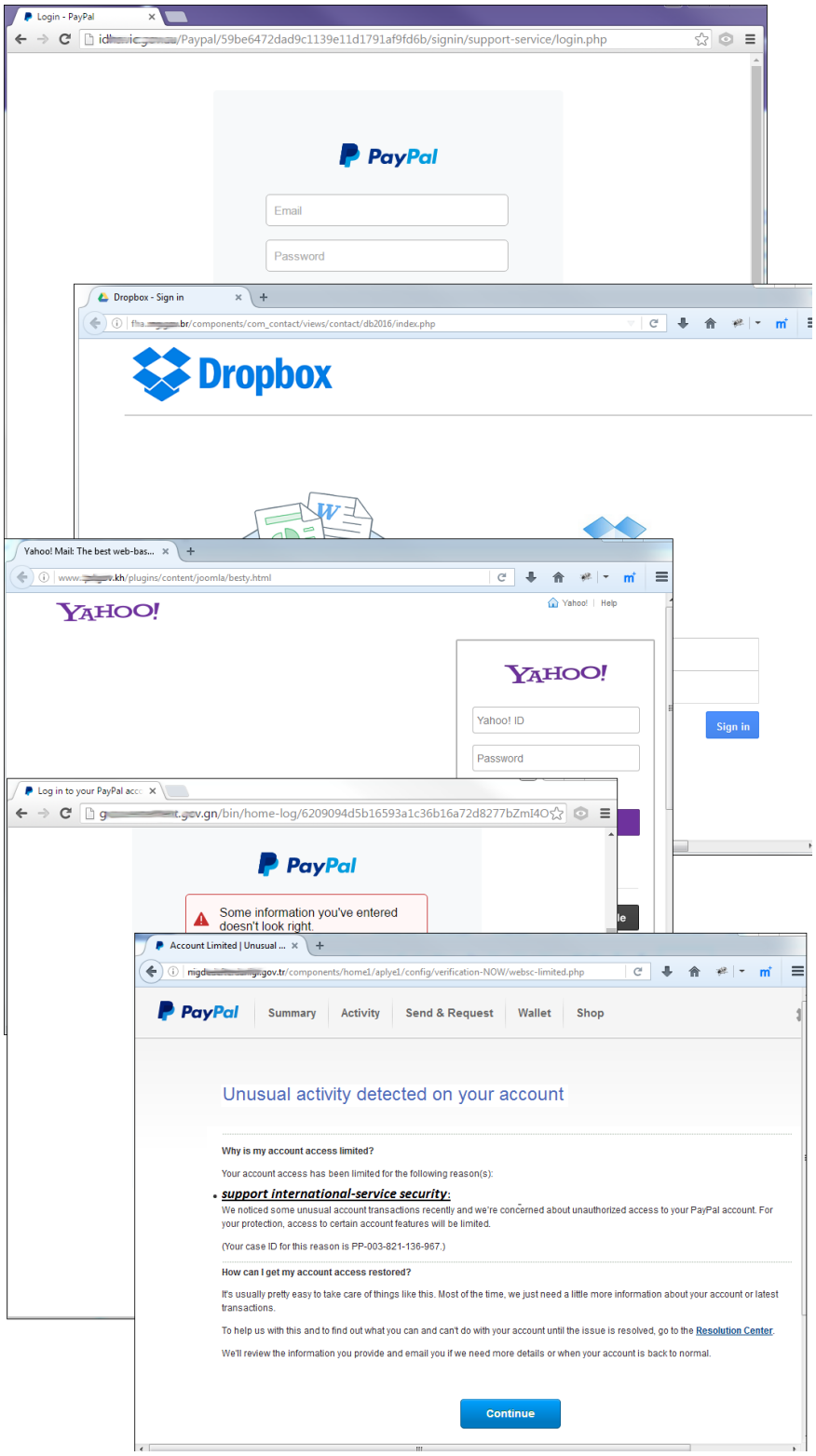
To bypass security software filters, fraudsters try to place phishing pages on domains with good reputations. This significantly reduces the probability of them being blocked and means potential victims are more trusting. The phishers can strike it big if they can use a bank or a government agency domain for their purposes. In Q2, we came across a phishing attack targeting the visitors of a popular Brazilian e-commerce site: the fake page was located on the domain of a major Indian bank. This is not the first time fraudsters have compromised the domain of a large bank and placed their content on it.



Phishing pages targeting the users of the Brazilian store americanas.com

When trying to purchase goods on the fake pages of the store, the victim is asked to enter lots of personal information. When it's time to pay, the victim is prompted to print out a receipt that now shows the logo of a Brazilian bank.

The domains of state structures are hacked much more frequently by phishers. In Q2 2016, we registered numerous cases where phishing pages were located on the domains belonging to the governments of various countries. Here are just a few of them:



Phishing pages located on the domains of government authorities

The probability of these links being placed on blacklists is negligible thanks to the reputation of the domain.

TOP 3 organizations attacked

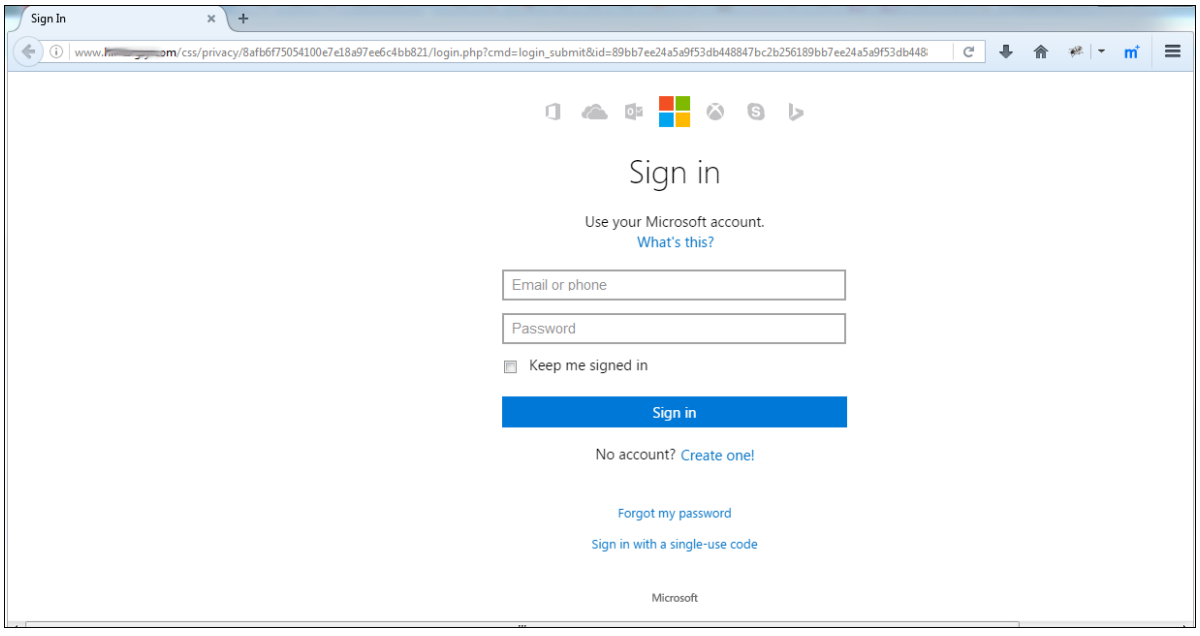
Fraudsters continue to focus most of their attention on the most popular brands, enhancing their chances of a successful phishing attack. More than half of all detections of Kaspersky Lab's heuristic anti-phishing component fall on phishing pages hiding behind the names of fewer than 15 companies.

The TOP 3 organizations attacked most frequently by phishers accounted for 23% of all phishing links detected in Q2 2016.

	Organization	% of detected phishing links
1	Microsoft	8.1
2	Facebook	8.03
3	Yahoo!	6.87

In Q2 2016, this TOP 3 ranking saw a few changes. Microsoft was the new leader with 8.1% (+0.61 p.p.), while Facebook (8.03%, +2.32 p.p.) came second. The share of attacks targeting Yahoo! (6.87%) fell 1.46 p.p., leaving last quarter's leader in third.

Q2 leader Microsoft is included in the 'Global Internet portals' category because the user can access a variety of the company's services from a single account. This is what attracts the fraudsters: in the event of a successful attack, they gain access to a number of services used by the victim.



Example of phishing on Live.com, a Microsoft service

Conclusion

In the second quarter of 2016, the proportion of spam in email traffic increased insignificantly – by 0.33 p.p. – compared to the previous quarter and accounted for 57.25%. The US remained the biggest source of spam. As in the previous quarter, the top three sources also included Vietnam and India.

Germany was once again the country targeted most by malicious mailshots, followed closely by China. Japan, which was seventh in the previous quarter's ranking, completed the TOP 3 in Q2.

Trojan-Downloader.JS.Agent remained the most popular malware family distributed via email. Next came Trojan-Downloader.VBS.Agent and Trojan-Downloader.MSWord.Agent. A significant amount of malicious spam was used to spread ransomware Trojans such as Locky. For almost a month, however, cybercriminals did not distribute their malicious spam, but then the Necurs botnet began working again. We don't expect to see any significant reduction in the volume of malicious spam in the near future, although there may be changes in email patterns, the complexity of the malware, as well as the social engineering methods used by attackers to encourage a user to launch a malicious attachment.

The focus of phishing attacks shifted slightly from the 'Global Internet portals' to the 'Financial organizations' category.

The theme of the Olympic Games was exploited by both phishers and spammers to make users visit fake pages with the aim of acquiring their confidential information or simply to get their money.

Events in the political arena, such as the presidential election in the US, also attracted spammers, while the sites of government agencies were compromised in phishing attacks.

As we can see, the overriding trend of the quarter is that of fraud and making quick money from victims using direct methods such as Trojan cryptors that force unprotected users to pay a ransom, or phishing attacks that target financial organizations, rather than long drawn-out scams. All of this once again highlights the need for both comprehensive protection on computers and increased vigilance by Internet users.

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