KASPERSKY lab

Kaspersky Security Bulletin

SPAM AND PHISHING IN 2015

Maria Vergelis, Tatyana Shcherbakova, Nadezhda Demidova, Darya Loseva

#KLReport

CONTENT

THE YEAR IN FIGURES 3
NEW DOMAIN ZONES IN SPAM 4
SPAMMER TRICKS: METHODS FOR EXPRESSING DOMAIN NAMES 5
- Special features of the IP protocol: different IP formats 5
- Obfuscation of an IP address, or how many ways can a number be written in Unicode 6
- Interpreting URL symbols 7
- Reiteration of a popular domain name 9
- Emails without a URL 9

WORLD EVENTS IN SPAM 11
STATISTICS 12
- Proportion of spam in email traffic 12
- Sources of spam by country 13
- The size of spam emails 14

MALICIOUS ATTACHMENTS IN EMAIL 15
- Malware families 16
- Countries targeted by malicious mailshots 17
- Special features of malicious spam 17

PHISHING 20
- Main trends 20
- The geography of attacks 24
- Organizations under attack 26

CONCLUSION AND FORECASTS 27

THE YEAR IN FIGURES

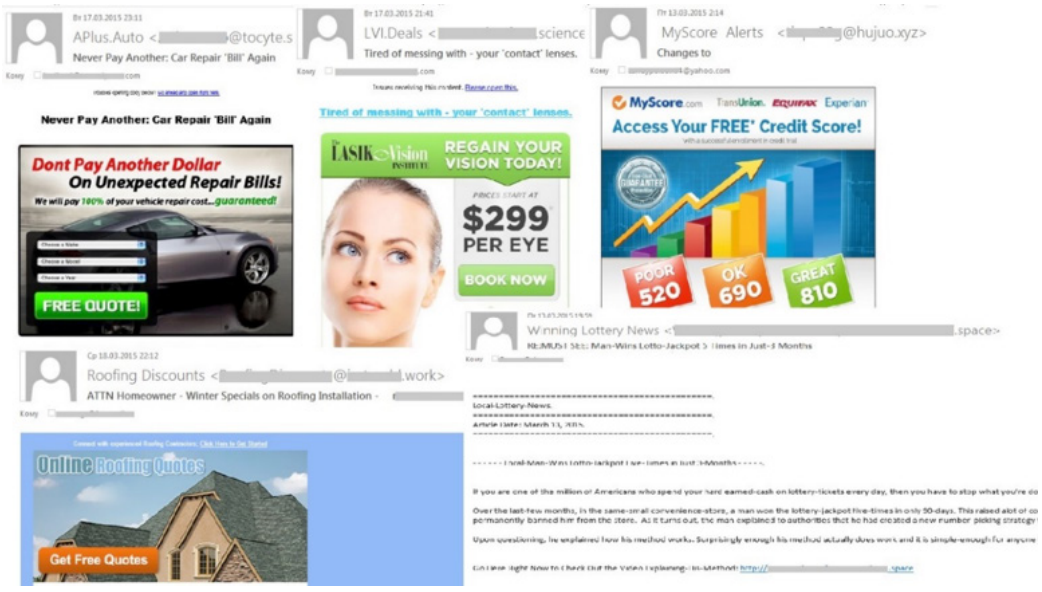
According to Kaspersky Lab, in 2015

- The proportion of spam in email flows was 55.28%, which is 11.48 percentage points lower than in 2014.
- 79% of spam emails were no more than 2 KB in size.
- 15.2% of spam was sent from the US.
- Users in Germany were targeted by 19% of malicious emails, the largest share of any country.
- 146,692,256 instances that triggered the 'Antiphishing' system were recorded.
- Russia suffered the highest number of phishing attacks, with 17.8% of the global total.
- Japan (21.68 %) took the lead in the ranking of unique users attacked by phishers.
- 34.33% of phishing attacks targeted online financial organizations (banks, payment systems and online stores).

NEW DOMAIN ZONES IN SPAM

In early 2015, we registered a surge in the number of new top-level domains used for distributing mass mailings. This was caused by the growth in interest among spammers for the New gTLD program launched in 2014. The main aim of this program is to provide organizations with the opportunity to choose a domain zone that is consistent with their activities and the themes of their sites. The business opportunities provided by New gTLD were enthusiastically endorsed by the Internet community, and active registration of new domain names is still ongoing.

However, new domain zones almost immediately became an arena for the large-scale distribution of spam, as cybercriminals registered domains to spread mass mailings. At first, there was some logical connection between the theme of the spam and the domain name, but this changed as the year went on and the domain names used in mass mailings were, on the whole, not related to the subject of the spam. However, even now we still come across isolated cases where the connection is noticeable. For example, online dating sites are often placed in the *.date* zone.



This lack of any connection between the domain name and spam theme was mainly caused by the cost of new domains. The attackers try to choose the cheapest possible hosting because the sites will often be used just once for a specific spam mass mailing, so the domain name does not play a major role. Instead, the deciding factors tend to be the cost of the domains and the discounts that small registrars are willing to provide for bulk purchases.

SPAMMER TRICKS: METHODS FOR EXPRESSING DOMAIN NAMES

Scammers try to make every email unique in order to bypass mass filtering and complicate the work of content filters. It is quite easy to make each text different by using similar characters from other alphabets, or by changing the word and sentence order, etc. But there is always the address of the spammer site – it can't be changed so easily, and the whole point of sending out spam is for users to click a link to the advertised site. Over the years, spammers have come up with numerous ways to hide the spammer site from anti-spam filters: redirects to hacked sites, generation of unique links to short URL services, the use of popular cloud services as redirects, etc.

In 2015, in addition to the methods mentioned above, spammers also focused on ways of expressing domain names and IP addresses. Here we take a closer look at these tricks by studying examples taken from a variety of spam messages.

Special features of the IP protocol: different IP formats

The standard method of writing IP addresses IPv4 is the dotted-decimal format where the value of each byte is given as a decimal number from 0 to 255, and each byte is separated by a dot. However, there are other formats that browsers will interpret correctly. These are binary, octal, hexadecimal formats, and the format dword/Undotted Integer when every IP byte is first converted to a hexadecimal format, then all the bytes are written in one number in the order they were written in the IP address, and then this number is converted into the decimal system. All these formats can be combined by writing each part of the IP in a different way, and the browser will still interpret it correctly!

These techniques are exploited by spammers. They write the same IP addresses in many different ways, including the method of combining different formats:

- oct – hex

```
http://0056.0004.0x5774
http://0242.0336.0xC122
```

- oct – dword

```
http://0037.0200.15567
```

- hex – dword

```
http://0xC2.2188528
http://0x5B.15319812
```

- Addresses in hexadecimal format can be written with and without dots separating the numbers:

```
http://0x6C.0x3B.0x9.0xBC/
http://0x45a27efd/
```

Additionally, 4294967296 (256^4) can be added any number of times to the number in the Integer format, and the result will still be interpreted as the same IP address.

In the decimal format, the number 256 can be added to each part of the IP address any amount of times – as long as there is a three-digit result, the address will be interpreted correctly.

In the octal format, any number of leading zeros can be added to the IP address, and it will remain valid:

```
http://000000000000271.00000000000000000053.000000000000000000000000000000317.00000000
000000000/

http://000000000000000000000000000000316.000000000000000000000000000000375.0000000000
000000000000000304.00000000000000000000016
```

You can also insert any number of forward slashes in the address:

```
http://////////////////////////////////////////////////////0x4A3FC3D2

http://////////////////////////////////////////////////////////////0x4A3FC3E2
```

Although in some legal libraries IP addresses can be stored in different formats, it is prohibited to use any format other than the standard dotted-decimal in the URL (i.e., in the links being referred to).

Obfuscation of an IP address, or how many ways can a number be written in Unicode

We have already written about the obfuscation of key words in spam using various Unicode ranges.

The same tricks can be applied when writing IP addresses and domain names. With regards to an IP, in 2015 spammers often used Unicode numbers from the so-called full-size range. Normally, it is used with hieroglyphic languages so that Latin letters and numbers do not look too small and narrow compared to the hieroglyphics.

http://６７．１５８．６０．５

We also came across figures from other ranges – figures in a circle, figures that are underscored, etc.:

http://④⑥.④.⑧⑤.②⓪①

Obfuscation of domains

As mentioned above, this trick also works with domains. Unicode has even more letter ranges than numerical. Spammers often used multiple ranges in a single link (changing them randomly in every email, thereby increasing the variability within a single mass mailing).

To make the links even more unique, rather than obfuscating the spammer site itself the scammers obfuscated short URL services where the links to the main site were generated in large quantities:

http://pIXｅｅｌ.me
http://wes.ℑN
http://Dºℑº P．cºm
http://U𝔶x3. n U
http://𝔣𝔲𝔯.ly

Interpreting URL symbols

URLs contain special symbols that spammers use to add 'noise'. Primarily, it is the @ symbol which is intended for user authentication on the site. A link such as http://login:password@domain.com means that the user wants to enter the site domain.com using a specific username (login) and password. If the site does not require authentication, everything that precedes the @ symbol, will simply be ignored. We came across mass mailings where spammers simply inserted the @ symbol in front of the domain name and mass mailings where the @ symbol was preceded with a random (or non-random) sequence:

http://@landbridges.net
http://send.com%2D%2D%3A%3A-:@g.ua/DU9F

It is interesting that this technique was used to obfuscate links; that is usually the prerogative of phishers. This method of presenting URLs can be used by fraudsters to trick users into thinking that a link leads to a

legitimate site. For example, in the link http://google.com@spamdomain.com/anything the domain that the browser accepts is spamdomain.com, not google.com. However, in order to trick users, spammers have used another domain-related technique: they registered lots of domains beginning with com-. With third-level domains the links in emails looked like this: http://learnmore.com-eurekastep.eu/find

If you don't look carefully, you might think that the main domain is learnmore.com, whereas it is in fact com-eurekastep.eu.

In addition to the @ symbol, scammers filled links with other symbols: www.goo&zwj.g&zwjl/0Gsylm.

For example, in the case above the "&zwj" fragment in the goo.gl domain has been inserted randomly in different parts of the domain making the link unique in each email. This insertion is called a zero-width joiner; it is used to combine several individual symbols in the Hindi languages as well as emoticons in one symbol. Within the domain, it obviously carries no semantic meaning; it simply obfuscates the link.

Yet another method of obscuring links is the use of a "soft hyphen" (SHY). In HTML, SHY is a special symbol that is not visible in the text, but if a word containing a special symbol doesn't fit in at the end of a line, the part after the special symbol is moved to the next line, while a hyphen is added to the first part. Typically, browsers and email clients ignore this symbol inside links, so spammers can embed it anywhere in a URL and as often as they like. We came across a mass mailing where soft hyphens had been inserted in the domain more than 200 times (hexadecimal encoding):

```
http://a&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#x
AD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;a&#xAD;&#xAD;&#xAD;&#xAD;y&#xAD
;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;a&#xAD;&#
xAD;&#xAD;&sup1;&#xAD;&#xAD;&#xAD;&#xAD;&sup1;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&
#xAD;&sup2;&#xAD;&#xAD;&#xAD;&ordm;&#xAD;&#xAD;&#xAD;&#xAD;d&#xAD;&#xAD;&#xA
D;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;et&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;
&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;e&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#x
AD;&#xAD;&#xAD;r&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;
&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;r&#xAD;&#x
AD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;e&#xAD;&#xAD;&#xAD;
&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xA
D;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;n&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&
#xAD;&#xAD;&#xAD;&#xAD;&#xAD;t&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xA
D;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;.&#xAD;&#xAD;&#xAD;&#
xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;c&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;
&#xAD;&#xAD;&#xAD;&ordm;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xA
D;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#
xAD;&#xAD;&#xAD;&#xAD;m&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;&#xA
D;&#xAD;&#xAD;&#xAD;&#xAD;&#xAD;/
```

As well as the soft hyphen there are other special symbols used in domains – the sequence indicator (& ordm;), the superscripts 1 and 2 (& sup1 ;, & sup2;) – that can be interpreted by some browsers as the letter "o" and the figures "1" and "2" respectively.

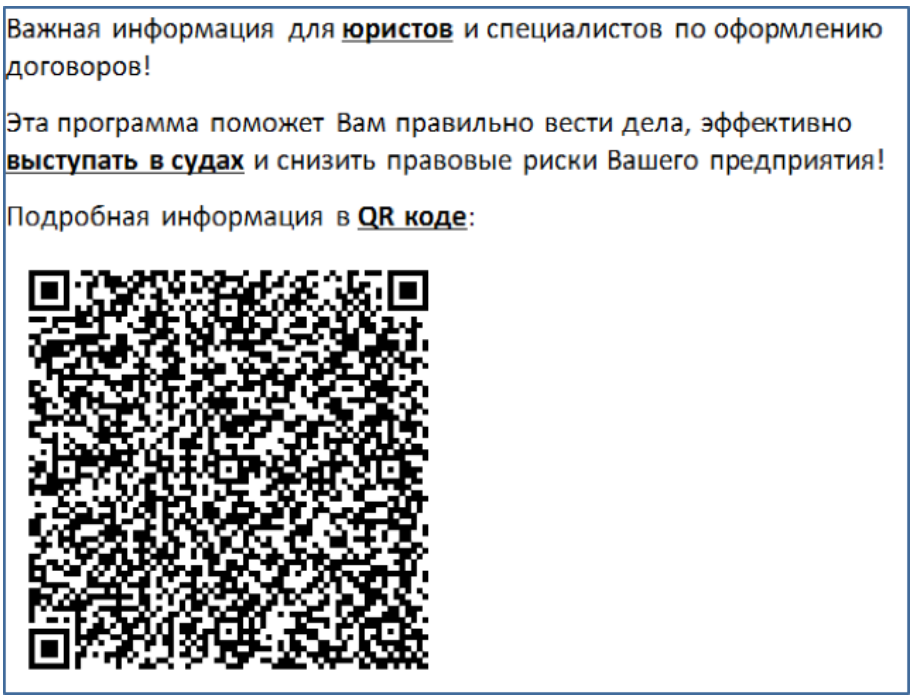
Reiteration of a popular domain name

Another original way of adding noise to links used by spammers in 2015 was the use of a well-known domain as a redirect. This trick is not new, but this time the fraudsters added the same well-known domain several times

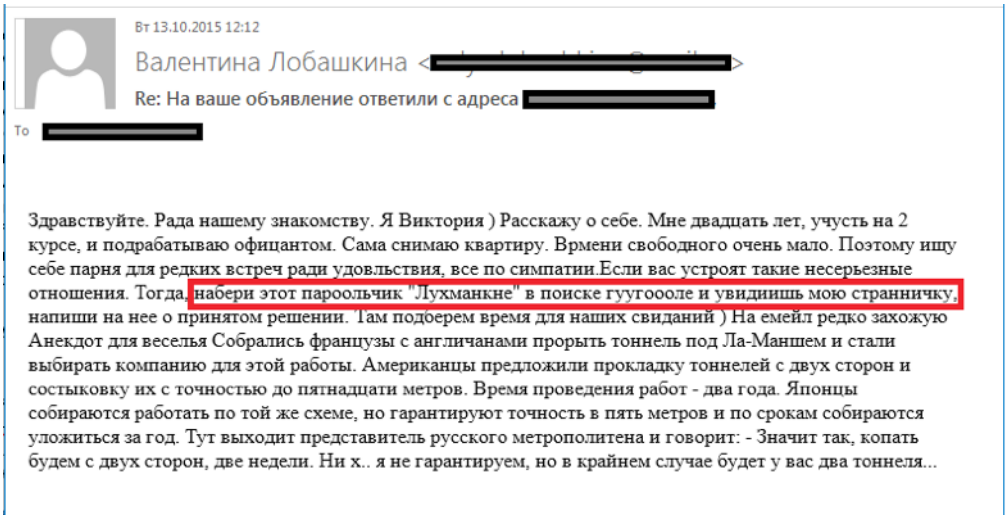
```
https://www.google.com/url?sa=D&q=https://www.google.com/accounts/Logout?continue=https:/
/appengine.google.com/_ah/logout%3Fcontinue%3Dhttp://www.rpp.uk.com/faq.php&service=ah&
usg=AFQjCNEcIQfFfP7TESslKSTQ9omhRbsDAA
https://vk.com/away.php?https://vk.com/away.php?https://vk.com/away.php?https://seminar-
practicum.ru/&to=https://shar.es/1cVuWm/kseniyamail2009
```

Emails without a URL

It is also worth mentioning those cases where no domains were used at all. Instead of a URL, a number of spam mailings contained a QR-code.



Other mass mailings prompted the user to enter a random sequence in a search engine; the link to the site appeared at the top of the search results:



Вт 13.10.2015 12:12

Валентина Лобашкина <[redacted]>

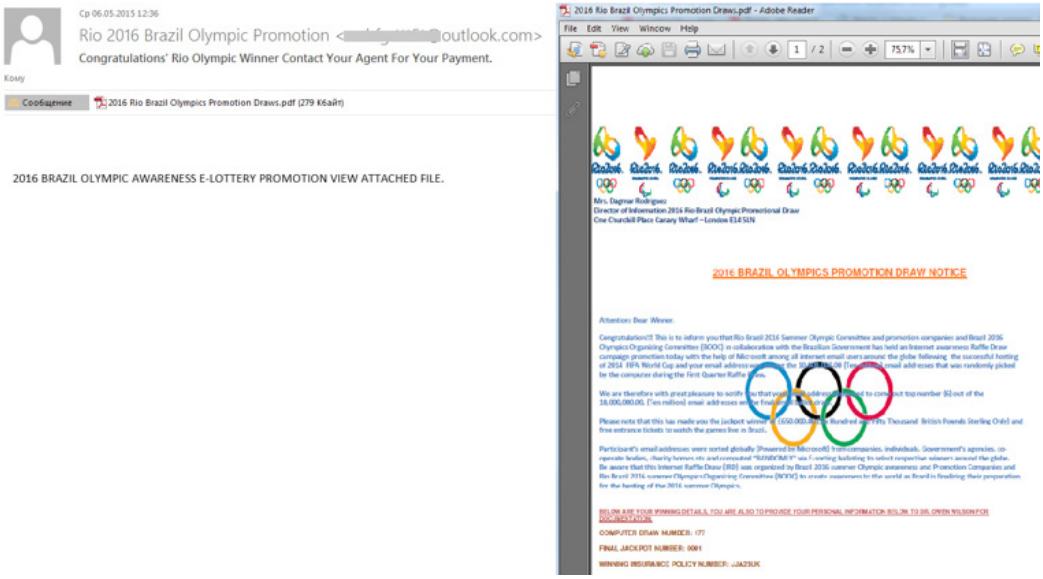
Re: На ваше объявление ответили с адреса [redacted]

To [redacted]

Здравствуйте. Рада нашему знакомству. Я Виктория) Расскажу о себе. Мне двадцать лет, учусь на 2 курсе, и подрабатываю официантом. Сама снимаю квартиру. Врмени свободного очень мало. Поэтому ищу себе парня для редких встреч ради удовльствия, все по симпатии.Если вас устроят такие несерьезные отношения. Тогда, набери этот пароольчик "Лухманкне" в поиске гуугоооле и увидиишь мою странничку, напиши на нее о принятом решении. Там подберем время для наших свиданий) На емейл редко захожую Анекдот для веселья Собрались французы с англичанами прорыть тоннель под Ла-Маншем и стали выбирать компанию для этой работы. Американцы предложили прокладку тоннелей с двух сторон и состыковку их с точностью до пятнадцати метров. Время проведения работ - два года. Японцы собираются работать по той же схеме, но гарантируют точность в пять метров и по срокам собираются уложиться за год. Тут выходит представитель русского метрополитена и говорит: - Значит так, копать будем с двух сторон, две недели. Ни х.. я не гарантируем, но в крайнем случае будет у вас два тоннеля...

WORLD EVENTS IN SPAM

The next Olympic Games in Brazil only take place in the summer of 2016, but already in 2015 fraudulent notifications of lottery wins dedicated to this popular sporting event were being registered. These included emails containing an attached PDF file that informed recipients that their address had been randomly selected out of millions of email addresses. In order to claim the prize it was necessary to respond to the email and provide specific personal information. In addition to the text, the attachments contained different graphical elements (logos, photos, etc.). The fake lottery win notifications, which were of a considerable length, were often sent out with attachments to bypass spam filtering.



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)

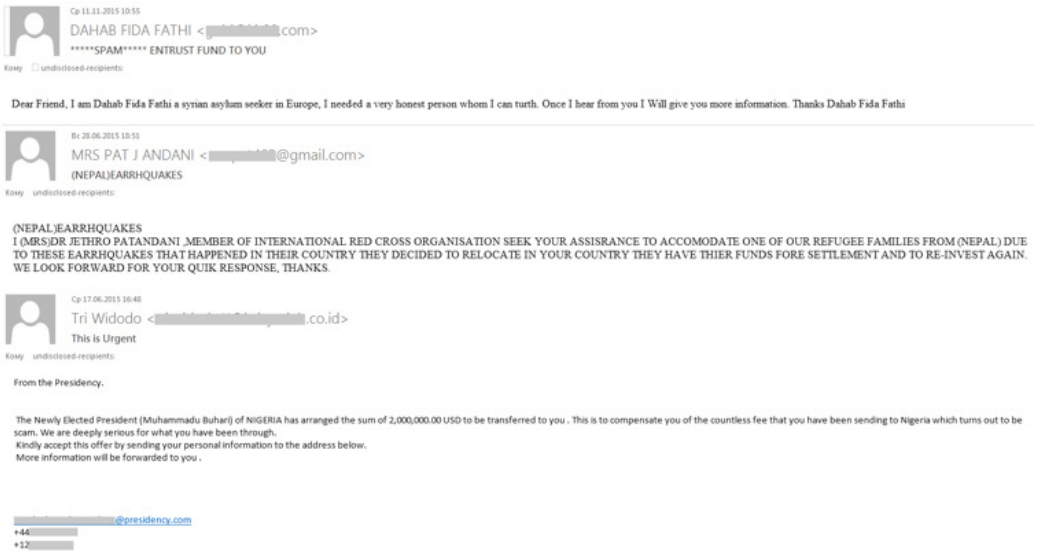
2016 BRAZIL OLYMPIC AWARENESS E-LOTTERY PROMOTION VIEW ATTACHED FILE.

2016 Rio Brazil Olympics Promotion Draws.pdf - Adobe Reader

File Edit View Window Help

2016 BRAZIL OLYMPICS PROMOTION DRAW NOTICE

In 2015, 'Nigerian' scammers exploited political events in Ukraine, the war in Syria, the presidential elections in Nigeria and earthquake in Nepal to convince recipients that their stories were genuine. The authors primarily sought help to invest huge sums of money or asked for financial assistance. These so-called Nigerian letters made use of the customary tricks to deceive recipients and extort money from them.



Cp 11.11.2015 10:55
DAHAB FIDA FATHI <[redacted].com>
*****SPAM***** ENTRUST FUND TO YOU
Кому undisclosed-recipients:

Dear Friend, I am Dahab Fida Fathi a syrian asylum seeker in Europe, I needed a very honest person whom I can turth. Once I hear from you I Will give you more information. Thanks Dahab Fida Fathi

Вс 28.06.2015 10:51
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.

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 .

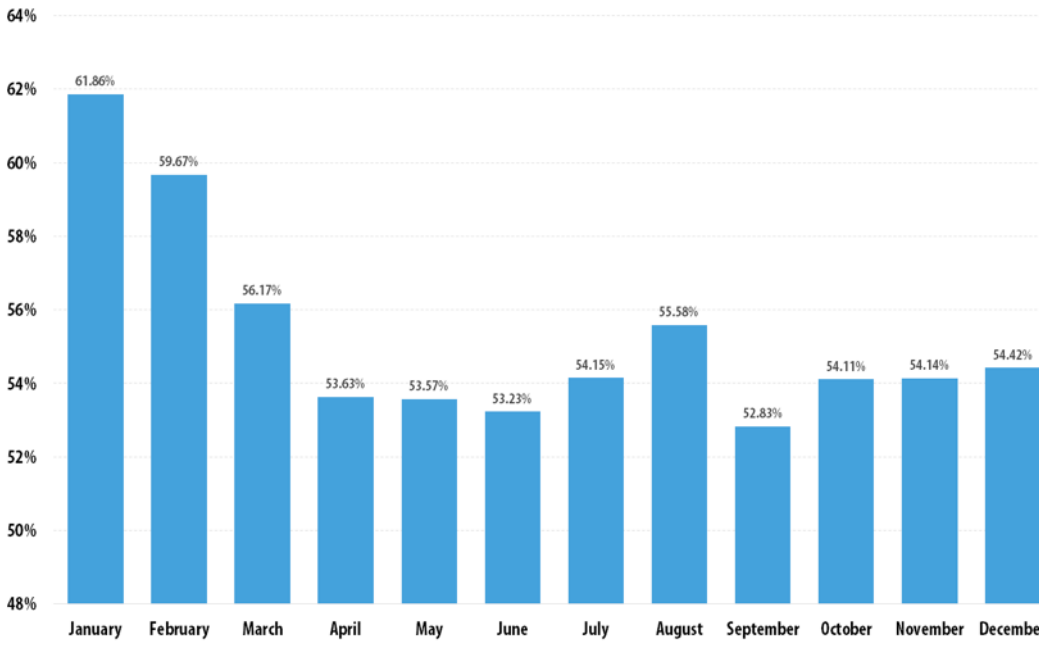
[redacted]@presidency.com
+44[redacted]
+12[redacted]

Emails about the war in Syria often mentioned refugees and Syrian citizens seeking asylum in Europe. Some emails were made to look as if they had been sent directly from refugee camps and contained complaints about the poor conditions.

STATISTICS

Proportion of spam in email traffic

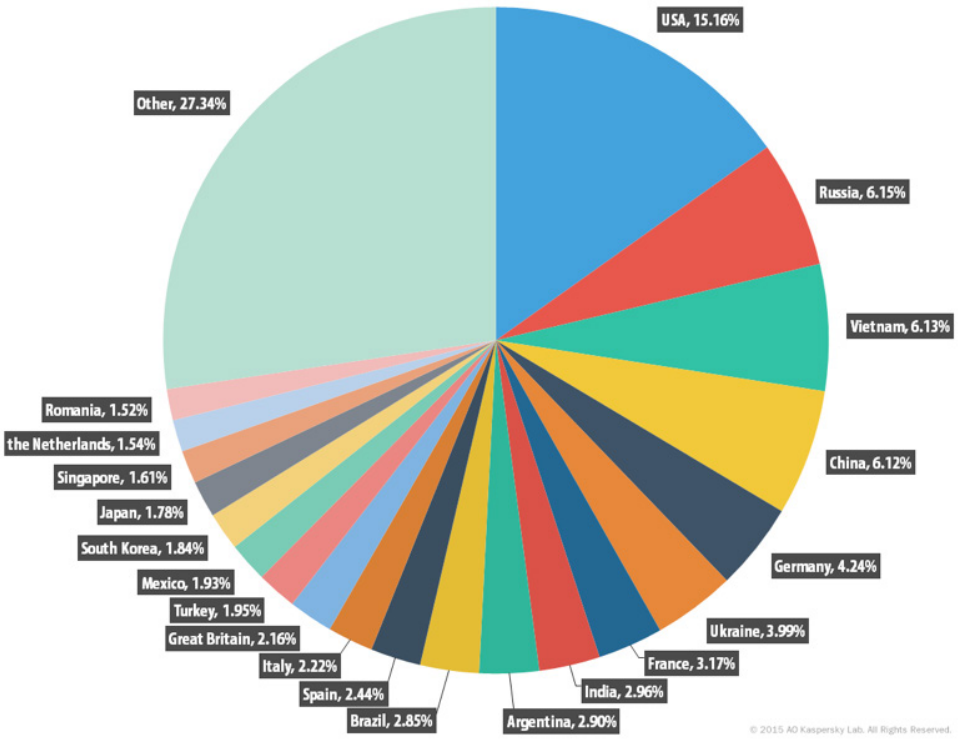
In 2015, the proportion of spam in email traffic was 55.28%, which is 11.48 percentage points lower than the previous year.



The proportion of spam in email traffic, 2015

The most noticeable drop was registered in the first months of 2015 – from 61.86% in January to 53.63% in April. The fluctuations throughout the rest of the year were inconsiderable – within 1-2 percentage points.

Sources of spam by country

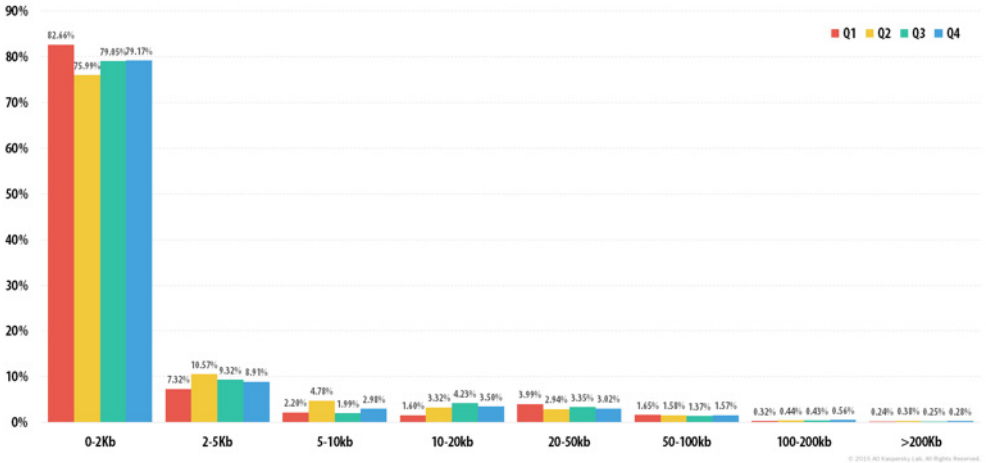


Sources of spam by country, 2015

In 2015, there was a slight change to the top three sources of spam: China (6.12%) dropped to fourth although the proportion of spam distributed from that country actually increased by 0.59 percentage points. Replacing it in third place was Vietnam (6.13%), which saw 1.92 percentage points added to its share. Russia (6.15%) remained in second place with an increase of 0.22 percentage points, while the US (15.16%) remained the undisputed leader despite a decrease of 1.5 percentage points.

As was the case in 2014 Germany came fifth (4.24%), with its contribution increasing by 0.24 percentage points. The rest of the Top 10 consisted of Ukraine (3.99%, +0.99 p.p.), France (3.17%, +0.62 p.p.), India (2.96%, no change), Argentina (2.90%, -0.65 p.p.) and Brazil (2.85%, +0.42 p.p.).

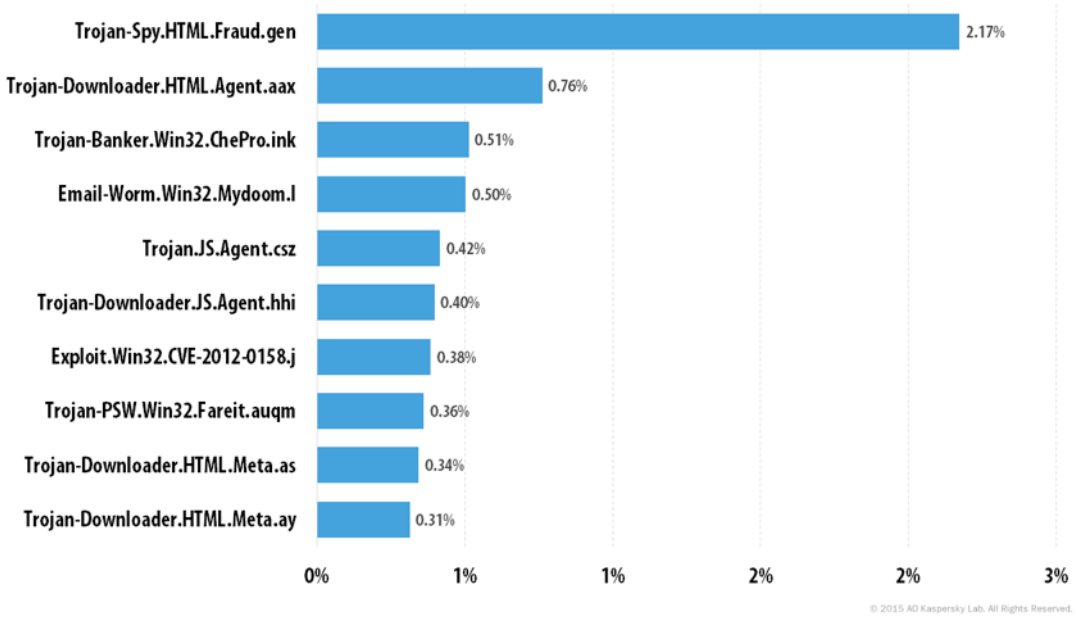
The size of spam emails



The size of spam emails in 2015

The proportion of super-short spam emails (under 2 KB) grew in 2015 and averaged 77.26%, while the share of emails sized 2-5 KB fell to 9.08%. The general trend of 2015 was a reduction in the size of emails.

MALICIOUS ATTACHMENTS IN EMAIL



The Top 10 malicious programs spread by email in 2015

The notorious Trojan-Spy.HTML.Fraud.gen remained the most popular malicious program sent by email. This program is a fake HTML page sent via email that imitates an important notification from a large commercial bank, online store, or 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.

Trojan-Downloader.HTML.Agent.aax was in second, while ninth and tenth positions were occupied by Trojan-Downloader.HTML.Meta.as. and Trojan-Downloader.HTML.Meta.ay respectively. All three are HTML pages that, when opened by users, redirect them to a malicious site. Once there, a victim usually encounters a phishing page or is offered a download – Binbot, a binary option trading bot. These malicious programs spread via email attachments and the only difference between them is the link that redirects users to the rigged sites.

Third was Trojan-Banker.Win32.ChePro.ink. This downloader 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.

Email-Worm.Win32.Mydoom.l was in fourth place. This network worm spreads as an email attachment via file-sharing services and writable network resources. It harvests email addresses from infected computers so they can be used for further mass mailings. To send the email, the worm directly connects to the SMTP server of the recipient.

Next came Trojan.JS.Agent.csz and Trojan-Downloader.JS.Agent.hhi, which are downloaders written in JavaScript. These malicious programs may contain several addresses (domains) which the infected computer consecutively calls. If the call is successful, a malicious EXE file is downloaded in the temp folder and run.

Trojan-PSW.Win32.Fareit.auqm was in eighth position. Fareit Trojans steal browser cookies and passwords from FTP clients and email programs and then send the data to a remote server run by cybercriminals.

Malware families

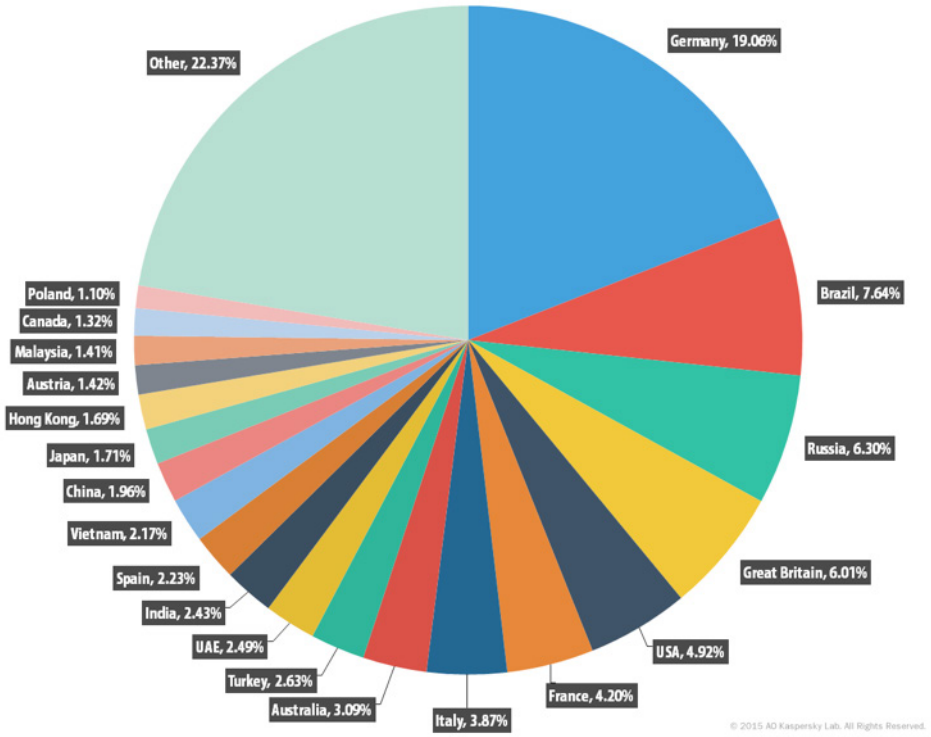
Throughout the year, Upatre remained the most widespread malware family. Malware from this family downloads the Trojan banker known as Dyre/Dyreza/Dyzap.

MSWord.Agent and VBS.Agent occupied second and third places respectively. To recap, 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 Andromeda.VBS.Agent. As the name suggests, it uses the embedded VBS script. To download and run other malware on the user's computer the malicious programs of this family utilize the ADODB.Stream technology.

The Andromeda family came fourth. These programs allow the attackers to secretly control infected computers, which often become part of a botnet. Noticeably, in 2014 Andromeda topped the rating of the most widespread malware families.

The Zbot family came fifth. Representatives of this family are designed to carry out attacks on servers and user 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.

Countries targeted by malicious mailshots



Distribution of email antivirus verdicts by country, 2015

For the previous three years, the Top 3 countries most often targeted by mailshots has remained unchanged – the US, the UK and Germany. However, in 2015, spammers altered their tactics and targets. As a result, Germany came first (19.06%, +9.84 p.p.) followed by Brazil (7.64%, +4.09 p.p.), which was only sixth in 2014.

The biggest surprise in Q3, and the whole of 2015, was Russia's rise to third place (6.30%, +3.06 p.p.). To recap, in 2014 Russia was ranked eighth with no more than 3.24% of all malicious spam being sent to the country.

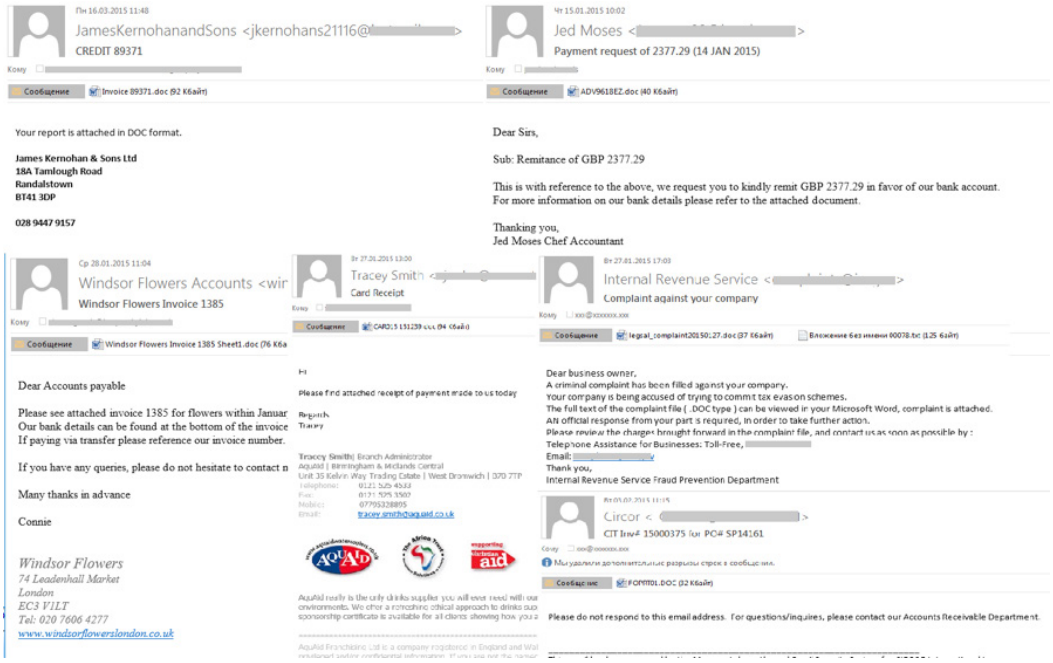
We would like to believe that despite the trend seen in recent quarters, the number of malicious mass mailings sent to Russia will decrease. As for the total number of malicious attachments sent via email, their number is likely to grow in 2016 and the theft of personal information and Trojan ransomware will occupy the top places.

Special features of malicious spam

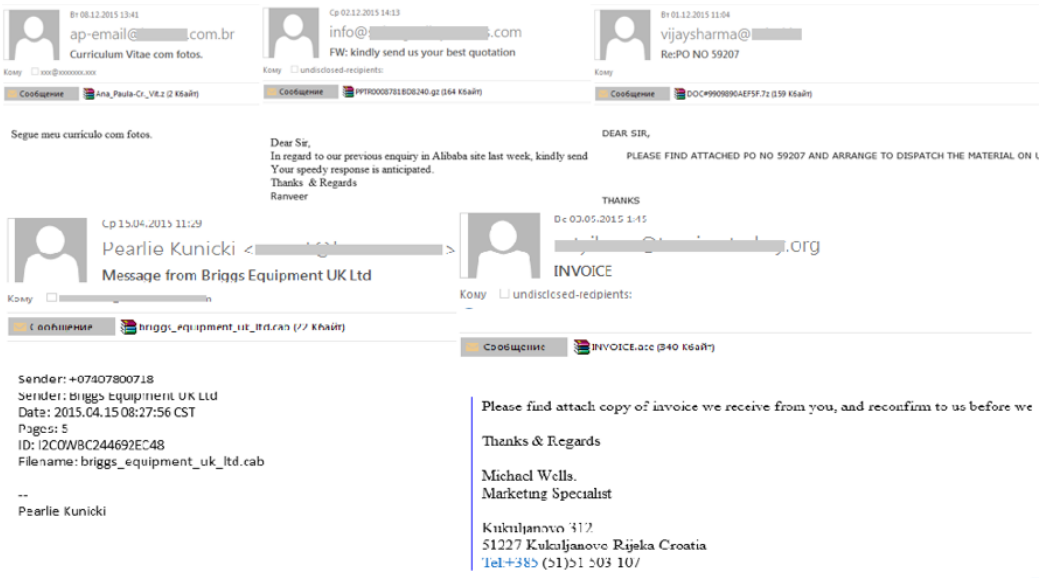
In spam traffic for 2015 we registered a burst of mass mailings with macro viruses. The majority of emails containing macro viruses in Q1 were sent in attachments with a .doc or .xls extension and belonged to the Trojan downloader category designed to download other malicious programs.

As a rule, the malicious attachments imitated various financial documents: notifications about fines or money transfers, unpaid bills, payments, complaints, e-tickets, etc. They were often sent on behalf of employees from real companies and organizations.

The danger posed by macro viruses is not restricted to their availability and ease of creation. A macro virus can infect not only the document that is opened initially but also a global macro common to all similar documents and consequently all the user's documents that use global macros. Moreover, the VBA language is sufficiently functional to be used for writing malicious code of all kinds.



In 2015, cybercriminals specializing in malicious spam continued to distribute malware in non-standard archive formats (.cab, .ace, .7z, .z, .gz). These formats were introduced long ago and are used by specialists in software development and installation, but they are largely unknown to ordinary users, unlike ZIP and RAR. Another difference is the high degree of file compression. These malicious archives were passed off as a variety of attachments (orders, invoices, photographs, reports, etc.) and contained different malicious programs (Trojan-Downloader.Win32.Cabby, Trojan-Downloader.VBS.Agent.azx, Trojan-Spy.Win32.Zbot .iuk, HawkEye Keylogger, etc.). The vast majority of emails were in English, though there were messages in other languages.



In 2014, cybercriminals were particularly active in sending out fake emails from mobile devices and notifications from mobile apps containing malware and adverts. In 2015, the mobile theme continued: malicious programs were distributed in the form of .apk and .jar files, which are in fact archived executable application files for mobile devices. Files with the .jar extension are usually ZIP archives containing a program in Java, and they are primarily intended to be launched from a mobile phone, while .apk files are used to install applications on Android.

In particular, cybercriminals masked the mobile encryption Trojan SLocker behind a file containing updates for Flash Player: when run, it encrypts images, documents and video files stored on the device. After launching, a message is displayed telling the user to pay a fee in order to decrypt his files. Another .jar archive contained Backdoor.Adwind written in Java. This multi-platform malicious program can be installed not only on mobile devices but also on Windows, Mac and Linux.

The attackers who send out malware in files for mobile devices are most probably hoping that recipients using email on a mobile device will install the malicious attachment.

With every year, cybercriminals are becoming more interested in mobile devices. This is primarily due to the constant increase in activity by mobile users (using messengers and other methods of exchanging data) and the migration of different services (e.g., financial transactions) to mobile platforms, and of course, one user may have several mobile devices. Secondly, it is due to the emergence of various popular apps that can be used by cybercriminals both directly (for sending out spam, including malicious spam) and indirectly (in phishing emails). For example, users of the popular messenger WhatsApp fall victim to not only traditional

advertising spam but also virus writers. Mobile users should be especially careful because cybercriminal activity in this sphere is only likely to increase.

PHISHING

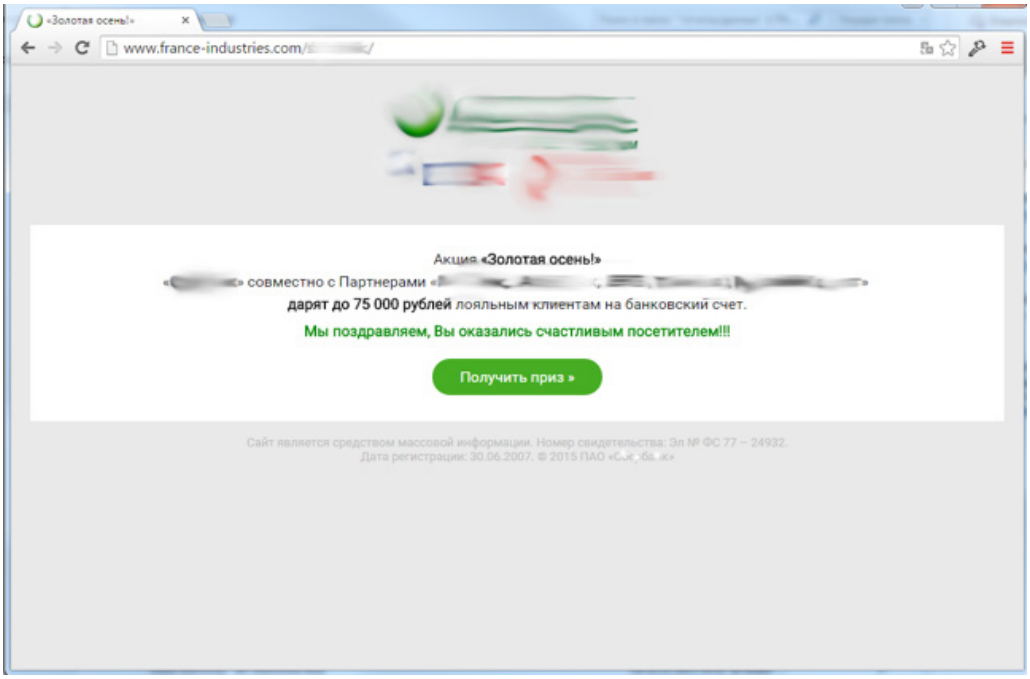
Main trends

In 2015, the Anti-Phishing system was triggered 148,395,446 times on computers of Kaspersky Lab users. 60% (89,947,439) of those incidents were blocked by deterministic components and 40% (58,448,007) by heuristic detection components.

Methods of distributing phishing content

The methods used by cybercriminals to spread phishing content have long gone beyond the framework of email clients. For example, one of the most popular ways of distributing phishing pages is pop-up ads. In 2015, we came across a variety of fraudulent schemes utilizing this simple trick: the fake page automatically opens in the browser when a user visits certain sites, including legitimate ones, but uses pop-up advertising.

Cybercriminals used this technique to attack customers of Russian banks in the third and fourth quarters of 2015.

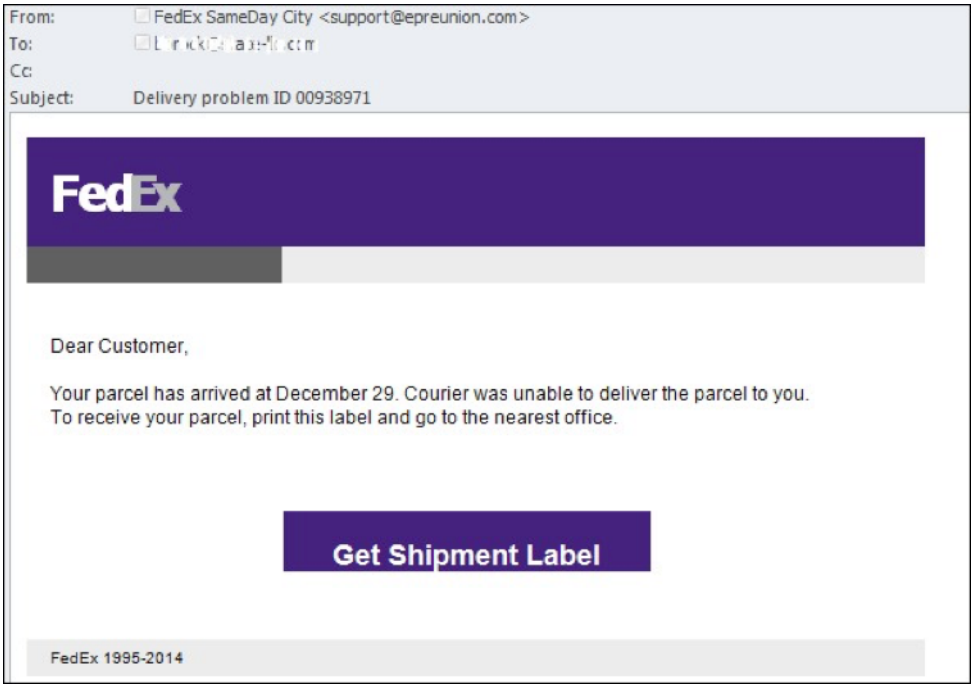


The fraudulent page to which the victim is redirected by a pop-up advert

Other popular themes of the year

As we mentioned in Q1, the contribution of the 'Delivery company' category is very small (0.23%), but it has recently experienced a slight increase (+0.04 p.p.). In addition, DHL, one of the companies in this category, was among the Top 100 organizations most often targeted by phishers.

This method – an email sent on behalf of a delivery firm – is often used by fraudsters to distribute malicious attachments, gather personal information and even collect money.



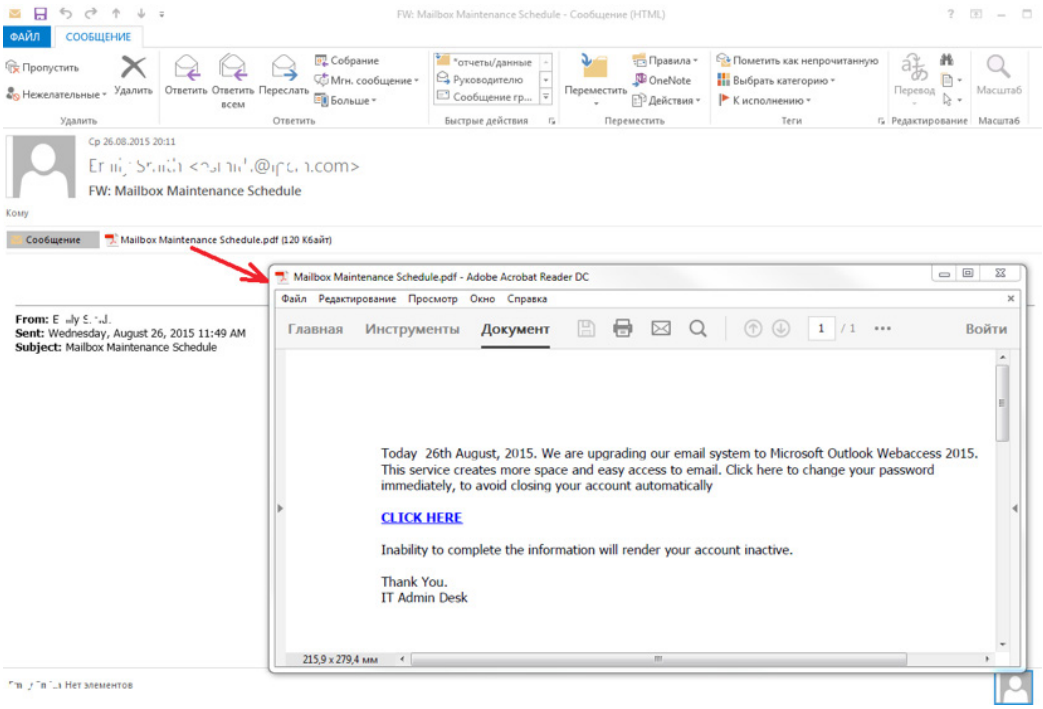
Phishing email sent on behalf of FedEx

The attackers are especially active in this category in the run-up to holidays when people tend to buy presents using popular delivery services.

Email tricks

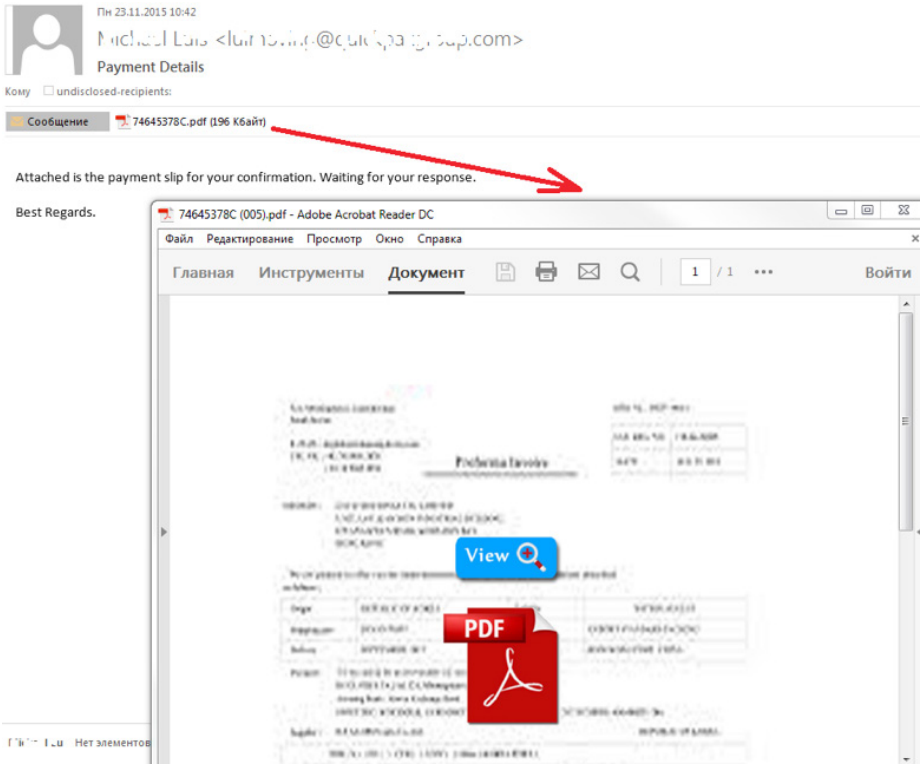
Scammers have long made successful use of PDF attachments in phishing attacks. These files are usually a form for entering personal information that is sent to the fraudsters by pressing a button in the file. However, in 2015 we saw a surge of emails in which the text message and the link to the phishing page were included in the PDF document. The text in the body of the message was reduced to a minimum to bypass spam filtering.

These tricks are used against organizations in all categories. In 2015, many attacks of this type targeted banking and mail organizations.



Example of a phishing email. The body of the message contains only the text imitating the heading of the email to which this email is allegedly responding. The email has an attached PDF file that contains the link to the phishing page.

We came across numerous PDF files that redirected victims to phishing websites. The fraudsters encouraged the user to click on 'View pdf File' to read the contents of the file.

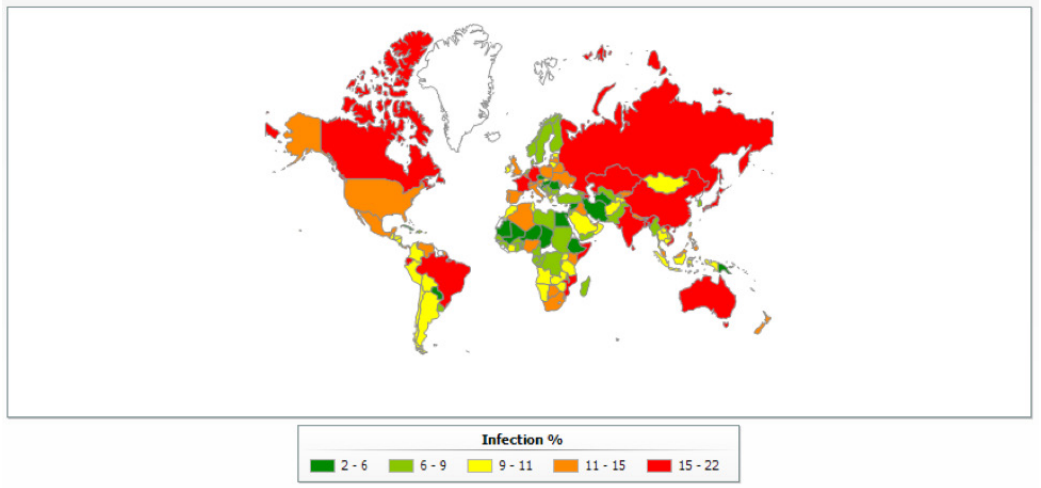


A phishing email with an attached PDF file containing a redirect to a phishing website

The geography of attacks

Top 10 countries by percentage of attacked users

Japan had the highest proportion of users subjected to phishing attacks (21.68%), a 2.17 p.p. increase from the previous year.



The percentage of users on whose computers the anti-phishing system was triggered out of the total number of users of Kaspersky Lab products in the country, 2015

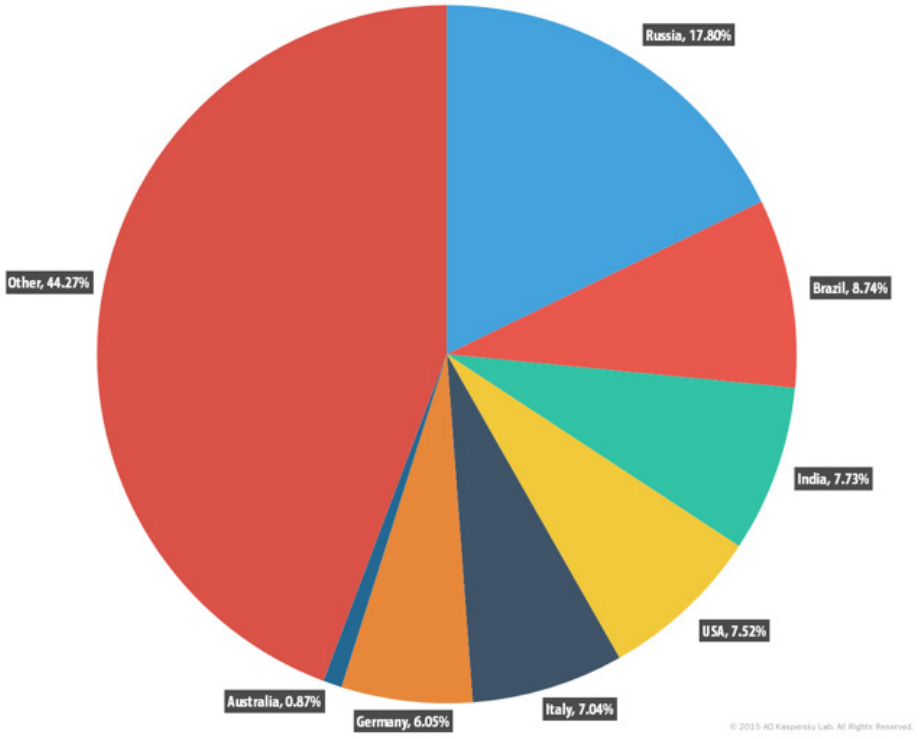
TOP 10 countries by percentage of attacked users

	Country	% attacked users
1	Japan	21.68%
2	Brazil	21.63%
3	Ecuador	20.03%
4	Mozambique	18.30%
5	Russia	17.88%
6	Australia	17.68%
7	Vietnam	17.37%
8	Canada	17.34%
9	France	17.11%

Last year's leader, Brazil (21.63%), fell to second place with a drop of 5.77 percentage points in the number of attacked users. It was followed by India (21.02%, -2.06 p.p.) and Ecuador (20.03%, -2.79 p.p.).

The distribution of attacks by country

Russia accounted for the greatest share of phishing attacks, with 17.8% of the global total, an increase of 0.62 percentage points compared to the previous year.

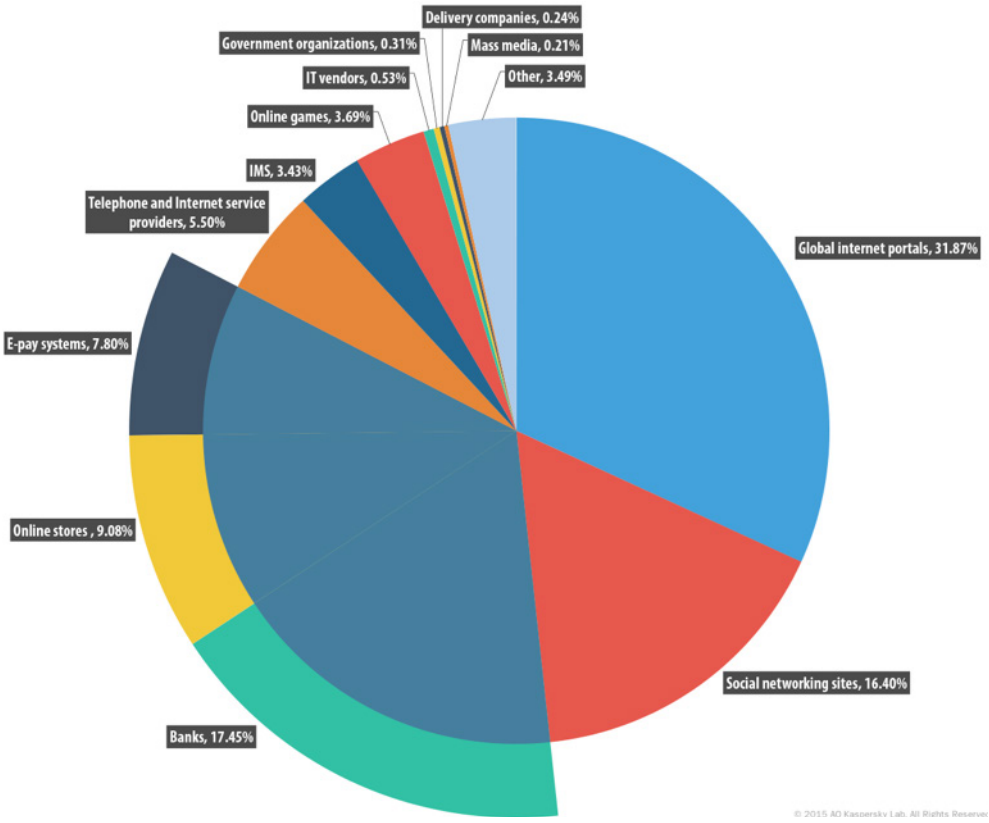


Distribution of phishing attacks by country in 2015

Behind Russia in second place was Brazil (8.74%, +1.71 p.p.), followed by India (7.73%, +0.58 p.p.), the US (7.52%, +0.32 p.p.), with Italy rounding off the Top 5 (7.04%, +1.47 p.p.).

Organizations under attack

The statistics on organizations used in phishing attacks are based on the triggering of the heuristic component in the anti-phishing system. The heuristic component is triggered when a user tries to follow a link to a phishing page and there is no information about the page in Kaspersky Lab's databases.



Distribution of organizations subject to phishing attacks by category, 2015

In 2015, we saw significant growth in the proportion of phishing attacks on organizations belonging to the 'Online finances' category (34.33%, +5.59 pp): they include the 'Banks', 'Payment Systems' and 'Online stores' categories. Of note is the increase in the percentage of targeted organizations in the 'Telephone and Internet service providers' (5.50%, +1.4 p.p.) and 'Social networking sites and blogs' (16.40%, +0.63 p.p.) categories.

Top 3 organizations attacked

	Organization	% of detected phishing links
1	Yahoo!	14.17
2	Facebook	9.51
3	Google	6.8

In 2015, Yahoo! was once again the organization targeted most by phishers, although its share decreased considerably – 14.17% vs 23.3% in 2014. We presume this decrease is a result of the company combating these fake domains. We see that Yahoo!, as well as many other organizations, registers lots of domains that could theoretically be used by the attackers as they are derived from the original domain name.

CONCLUSION AND FORECASTS

In 2015, the proportion of spam in email traffic decreased by 11.48 percentage points and accounted for 55.28%. The largest decline was observed in the first quarter; from April the fluctuations stabilized and were within a few percentage points. This reduction was caused by the migration of advertising for legal goods and services from spam flows to more convenient and legal platforms (social networks, coupon services, etc.), as well as by the expansion of the "gray" zone in mass mailings (mass mailings sent both to voluntary subscribers and to people who have not given their consent). We assume the share of spam will continue to decrease in 2016, though the decline will be insignificant.

The number of malicious and fraudulent messages, however, will increase. It is possible that the attackers will once again make use of their customary tricks as was the case in 2015 (mass mailings of macro viruses and non-standard attachment extensions). The mobile theme may also become yet another weapon in the cybercriminals' arsenal to spread malware and fraudulent spam.

The number of new domains created by spammers especially for distributing mass mailings will continue to grow. We also expect to see an expansion in new domain zones used as spammer resources.

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