KASPERSKY lab

SPAM AND PHISHING IN Q3 2016

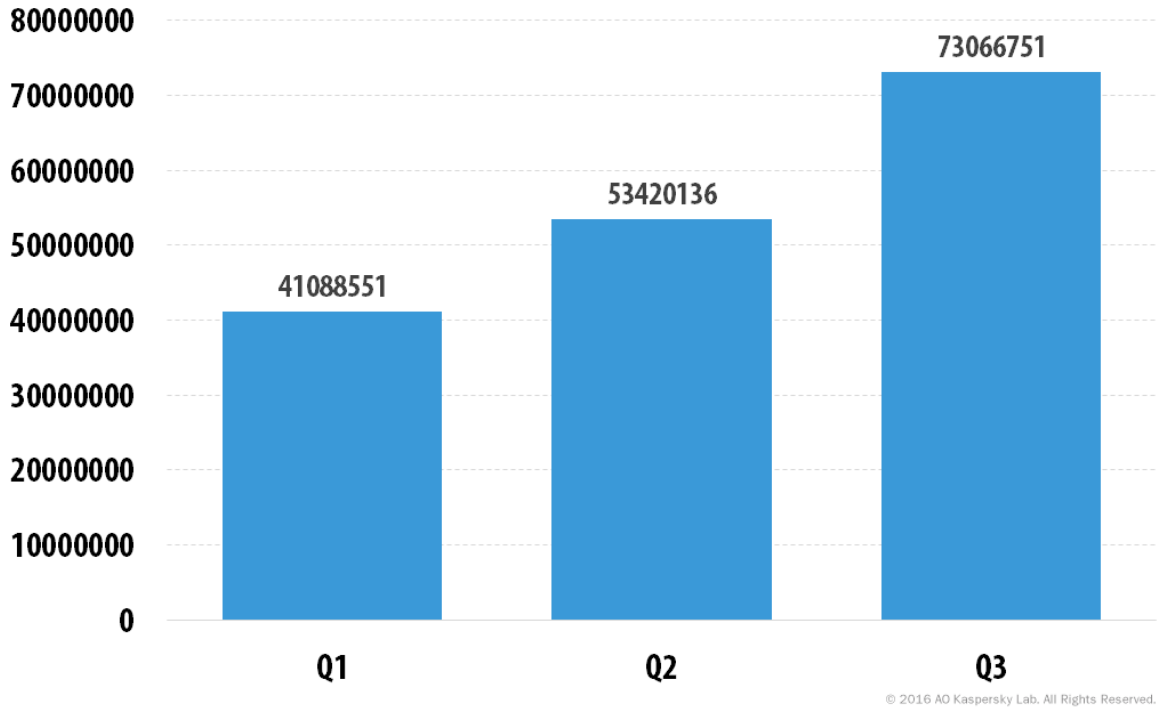
Darya Gudkova, Maria Vergelis, Nadezhda Demidova

Contents

Spam: quarterly highlights

Malicious spam

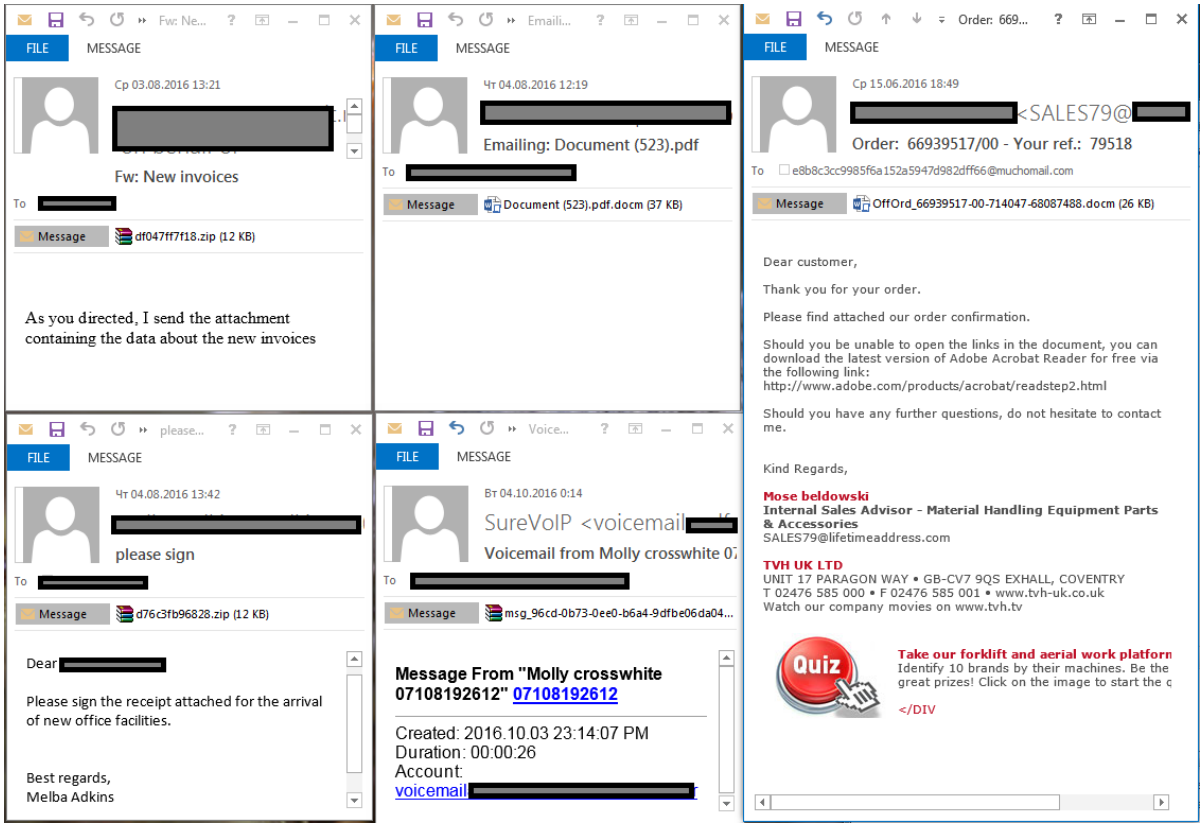
Throughout 2016 we have registered a huge amount of spam with malicious attachments; in the third quarter, this figure once again increased significantly. According to KSN data, in Q3 2016 the number of email antivirus detections totaled 73,066,751. Most malicious attachments contained Trojan downloaders that one way or another loaded ransomware onto the victim's computer.



Number of email antivirus detections, Q1-Q3 2016

The amount of malicious spam reached its peak in September 2016. According to our estimates, the number of mass mailings containing the Necurs botnet alone amounted to **6.5%** of all spam in September. To recap, this kind of malicious spam downloads the Locky malware to computers.

Most emails were neutral in nature. Users were prompted to open malicious attachments imitating bills supposedly sent by a variety of organizations, receipts, tickets, scans of documents, voice messages, notifications from stores, etc. Some messages contained no text at all. All this is consistent with recent trends in spam: fraudsters are now less likely to try and impress or intimidate users to make them click a malicious link or open an attachment. Instead, spammers try to make the email contents look normal, indistinguishable from other personal correspondence. Cybercriminals appear to believe that a significant proportion of users have mastered the basics of Internet security and can spot a fake threat, so malicious attachments are made to look like everyday mail.



Of particular note is the fact that spam coming from the Necurs botnet had a set pattern of technical email headers, while the schemes used by the Locky cryptolocker varied a lot. For example, the five examples above contain the following four patterns:

- JavaScript loader in a ZIP archive loads and runs Locky.
- Locky is loaded using a macro in the .docm file.
- Archived HTML page with a JavaScript script downloads Locky.
- Archived HTML page with a JavaScript script downloads the encrypted object Payload.exe, which runs Locky after decryption.

Methods and tricks: links in focus

IP obfuscation

The third quarter saw spammers continue to experiment with obfuscated links. This well-known method of writing IP addresses in hexadecimal and octal systems was updated by scammers who began to add 'noise'. As a result, an IP address in a link may end up looking like this:

HTTP://@[::ffff:d598:a862]:80/

Spammers also began to insert non-alphanumeric symbols and slashes in domain/IP addresses, for example:

http:`````````/``````````/0122.0142.0xBABD/

<a href=````````````````````````/@/0x40474B17

URL shortening services

Spammers also continued experimenting with URL shortening services, inserting text between slashes. For example:

```
http://GOO.GL/Kv239tLYan3.Kv239tLYan3.Kv239tLYan3.Kv239tLYan3.[zaza[zaza[zaza[zaza[zaza[zaza[zaz
a[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[z
aza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza
[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[za
za[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[
zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza.Kv239tLYan3.Kv239tLYan3.K
v239tLYan3.Kv239tLYan3.W8RPGt4KDYKKh7d.W8RPGt4KDYKKh7d.[zaza[zaza[zaza[zaza[zaza[zaza[zaza[z
aza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza
[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[za
za[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[
zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaz
a[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza[zaza/../01fZuB">
```

Sometimes other links were used to add text noise:

```
<A
HREF="http://goo.gl/....www.Chinadaily.com.cn.......www.Chinadaily.com.cn.......www.Chinadaily.com.c
n.......www.Chinadaily.com.cn.......www.Chinadaily.com.cn.......www.Chinadaily.com.cn.......www.Chinad
aily.com.cn.......www.Chinadaily.com.cn.......www.Chinadaily.com.cn.......www.Chinadaily.com.cn.......ww
w.Chinadaily.com.cn.......www.Chinadaily.com.cn.......www.Chinadaily.com.cn.......www.Chinadaily.com.
cn....... <here there was a page of similar URLs>/../7dNlq9">
```

```
http://qck.pl/0C/pacmmta7848.windstream.net/../../../..google.com./././.T/./././youtube.com/../../winds
tream.net/./../././././././../../../.-----___*-*-*-13149976.7731897.39037-----___*-*-*------___*-*-*-
../././../././/WTv
```

The use of search queries

Some spammers have returned to the old method of hiding the addresses of their sites as search queries. This allows them to solve two problems: it bypasses black lists and makes the links unique for each email. In the third quarter, however, spammers went even further and used the Google option "I'm Feeling Lucky". This option immediately redirects users to the website that's displayed first in the list of search results, and it can be activated simply by adding “&btnI=ec” to the end of the link. Clicking on the link redirects users to the spammer's site rather than to the page displayed in the Google search results. The advertising site itself is obviously optimized to appear first in the search results. There could be lots of similar queries within a single mass mailing.

```
<a href="http://www.google.de/search?q=%22%26%231040%3B%26%231074%3B%26%231
090%3B%26%231086%3B%26%231082%3B%26%231088%3B%26%231077%3B%26%231076%3B%26%2
31080%3B%26%231090%3B%2C+%26%231082%3B%26%231072%3B%26%231083%3B%26%231100%3
B%26%231082%3B%26%231091%3B%26%231083%3B%26%231103%3B%26%231090%3B%26%231086
%3B%26%231088%3B+%26%231088%3B%26%231072%3B%26%231089%3B%26%231095%3B%26%231
077%3B%26%231090%3B%26%231072%3B+%26%231086%3B%26%231085%3B%26%231083%3B%26%
231072%3B%26%231081%3B%26%231085%3B+%26%231091%3B%26%231089%3B%26%231083%3B%
26%231086%3B%26%231074%3B%26%231080%3B%26%231081%3B+%26%231072%3B%26%231074%
3B%26%231090%3B%26%231086%3B%26%231082%3B%26%231088%3B%26%231077%3B%26%23107
6%3B%26%231080%3B%26%231090%3B%26%231072%3B+%26%231074%3B%22+%22%26%231050%3
B%26%231088%3B%26%231077%3B%26%231076%3B%26%231080%3B%26%231090%3B%26%231099
%3B+%26%231072%3B%26%231074%3B%26%231090%3B%26%231086%3B%22&btnI=ec
">
```

The example above involves yet another trick. The search query is written in Cyrillic. The Cyrillic letters are first converted to a decimal format (e.g., "авто" becomes "Авто"), and then the whole query in decimal format, including special symbols, are converted to a hexadecimal URL format.

Imitations of popular sites

The third quarter saw phishers trying to cheat users by making a link look similar to that of a legitimate site. This trick is as old as the hills. In the past, real domain names were distorted very slightly; now, cybercriminals make use of either subdomains imitating real domain names or long domains with hyphens. So, in phishing attacks on PayPal users we came across the following domain names:

http://www.paypal.com.e-service-billing.info/

http://www.paypal.com-authorized-login.net/

http://www.paypal.com.authorization-login.com/

http://paypal.com-secured-your-account.info/

http://paypal-service-virifivation.tk

Phishing attacks targeting Apple users included the following names:

flhob-apple.co.uk

cancel-order-apple.co.uk

Spammers have also found help from new "descriptive" domain zones, where a fake link can seem more topical and trusted, for example:

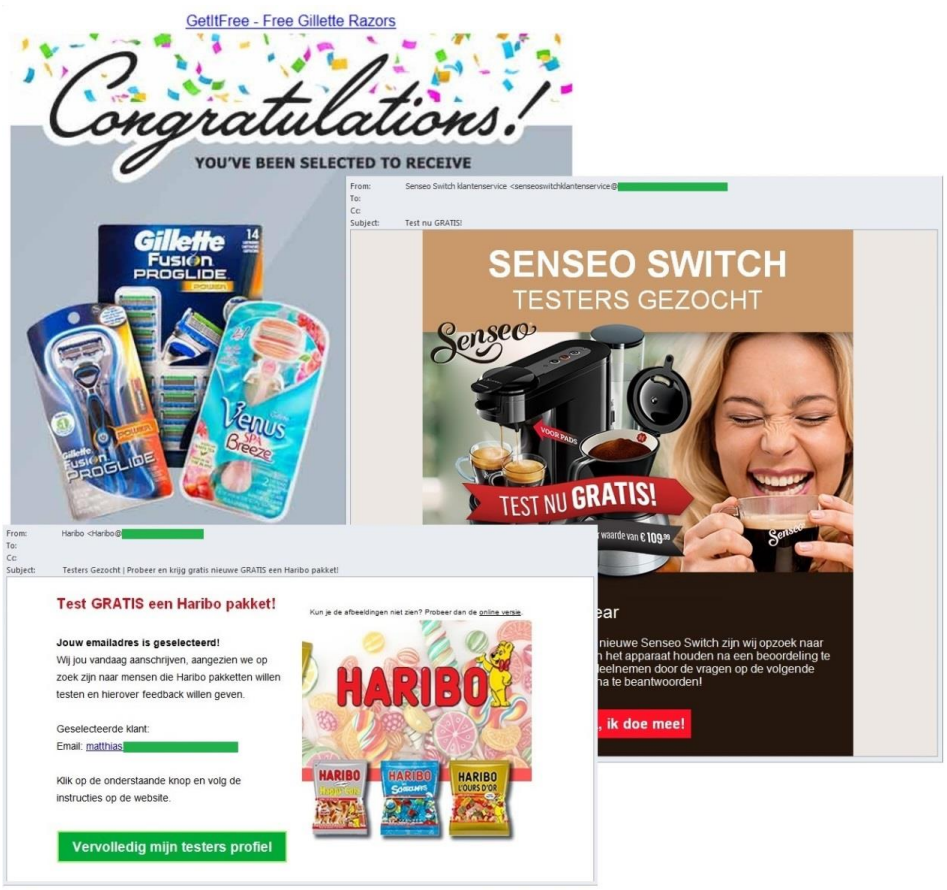
http://uk_applesecurelog_in.sec1.cloud

http://uk_iosApplevalidate.ath1.support

Testers required

Q3 email traffic contained mass mailings asking users to participate in free testing of a product that they could then keep. The authors of the emails we analyzed were offering popular goods such as expensive brand-name home appliances (coffee machines, robot vacuum cleaners), cleaning products, cosmetics and even food. We also came across a lot of emails offering the chance to test the latest models of electronic devices including the new iPhone that was released at the end of the third quarter. The headers used in these mass mailings include: “Register to test & keep a new iPhone 7S! Wanted:! IPhone 7S Testers”. The release of the latest iPhone was met with the usual surge of spam activity dedicated exclusively to Apple products.

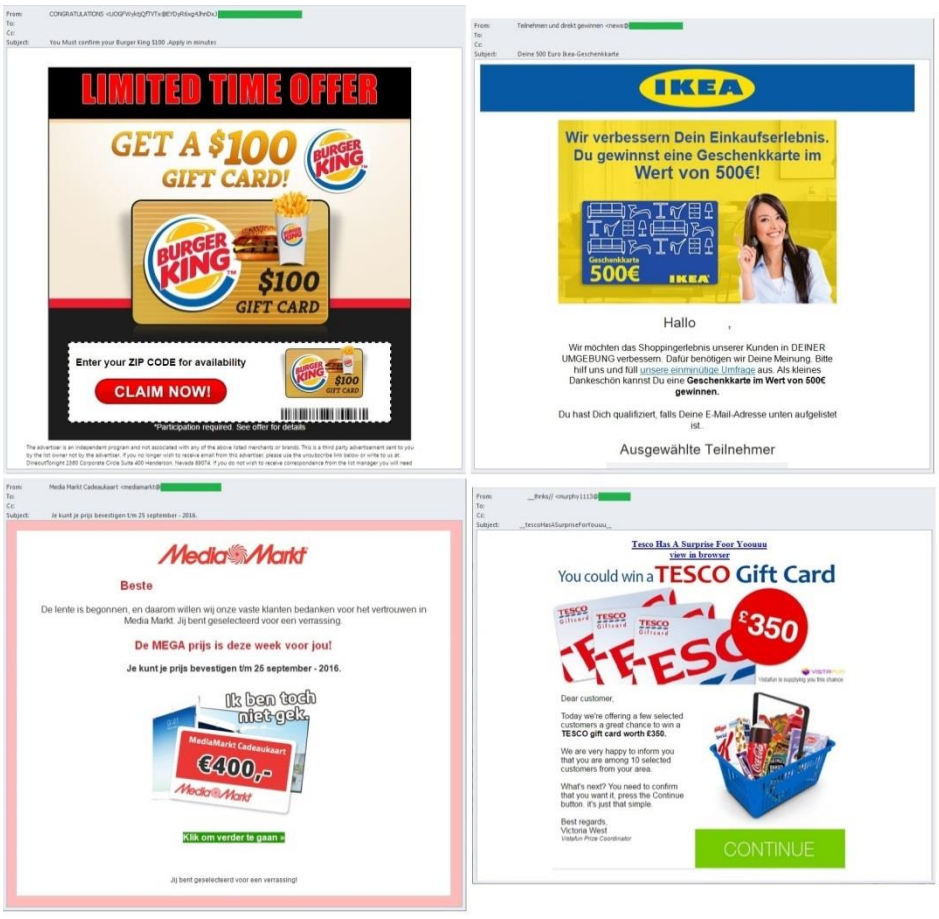
The people sending out these messages are in no way related to the companies whose products they use as bait. Moreover, they send out their mass mailings from fake email addresses or from empty, newly created domains.



The senders promise to deliver the goods for testing by post, and using this pretext they ask for the recipient's postal and email addresses as well as other personal information. A small postal charge in is imposed on the user, but even if the goods are delivered, there is no guarantee they will be good quality. There are lots of posts on the Internet by users saying they never received any goods, even after paying the postage costs. This has an element of old-fashioned non-virtual fraud: the cybercriminals receive money transfers under the pretext of a postal charges and then disappear.

Gift certificates to suit all tastes

Spam traffic in Q3 included some interesting mailings using the common theme of fake gift certificates. Recipients were offered the chance to participate in an online survey in return for a certificate worth anything from ten to hundreds of euros or dollars. They were led to believe that the certificates were valid for large international retail chains, online hypermarkets, grocery stores, popular fast-food chains as well as gas stations.



In some cases, the senders of these fraudulent messages said they were carrying out a survey to improve the customer support services of the organizations that were allegedly behind these generous offers, as well as to improve the quality of their products. In other cases, the message was described as a stroke of luck and that the recipient's email address was randomly selected for a generous gift as a mark of appreciation for using the brand's goods or services. The messages were

indeed randomly sent out to email addresses that had been collected by spammers, and did not necessarily belong to customers of the companies named in emails.

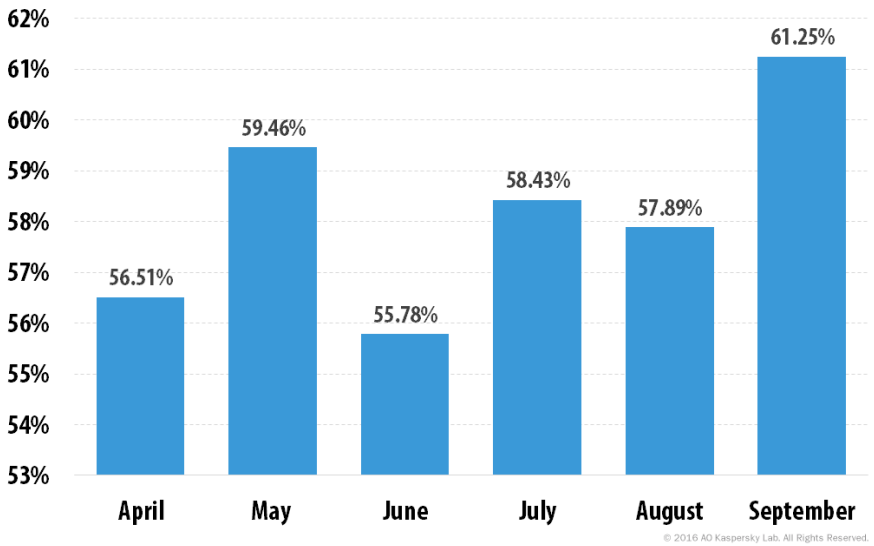
To confirm receipt of the gift certificate, the user is asked to follow a link in the email which in fact leads to an empty domain with a descriptive name (e.g. “winner of the day”). Then, via the redirect, the user ends up at a newly created site with a banner designed in the style of the brand that supposedly sent out the mailing. The user is notified that the number of certificates is limited and that they have only 90 seconds to click on a link, thereby agreeing to receive the gift. After completing a short survey asking things such as "How often do you use our services?" and "How are you planning to use the certificate?" the user is asked to enter their personal data in a form. And finally the "lucky winner" is redirected to a secure payment page where they have to enter their bank card details and pay a minor fee (in the case we analyzed the sum was 1 krone).

According to online reviews, some potential victims of this type of certificate fraud were asked to call a number to participate in a telephone survey rather than an online survey. This type of fraudulent scheme is also quite common: the idea is to keep someone on the paid line for as long as possible until they give up on the promised reward.

Like the offers to participate in the testing of goods, these themed messages were sent out from fake addresses with empty or newly created domains that had nothing to do with the organizations in whose name the cybercriminals were offering the certificates.

Statistics

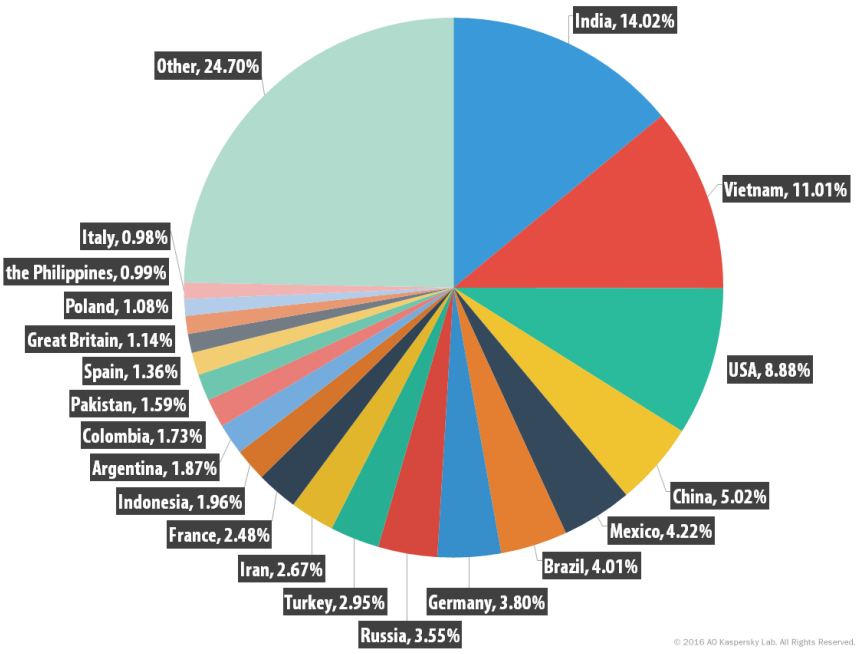
Proportion of spam in email traffic



Percentage of spam in global email traffic, Q2 and Q3 2016

The largest percentage of spam in the third quarter – 61.25% – was registered in September. The average share of spam in global email traffic for Q3 amounted to 59.19%, which was 2 p.p. more than in the previous quarter.

Sources of spam by country

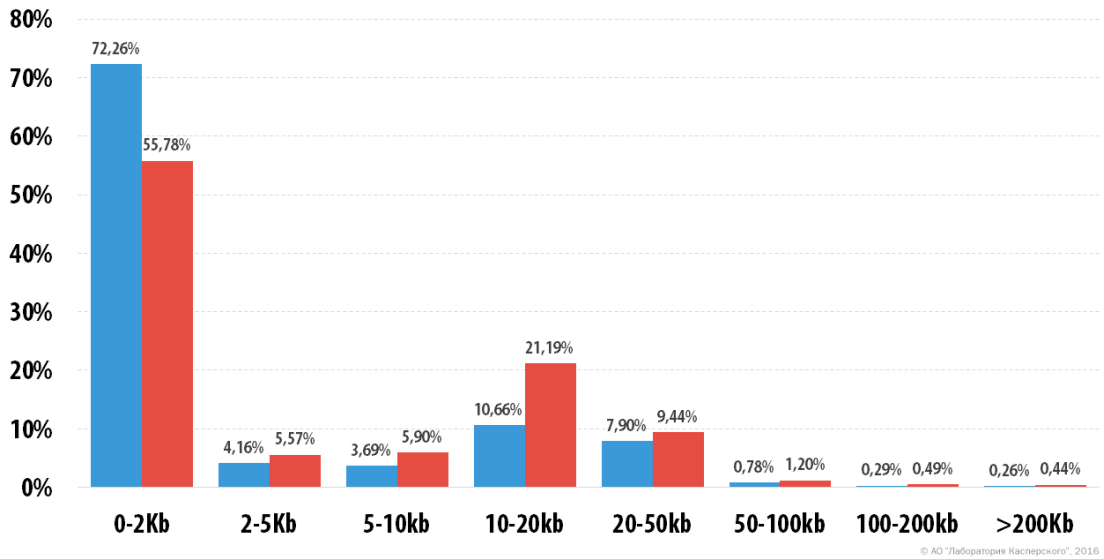


Sources of spam by country, Q3 2016

In Q3 2016, the contribution from India increased considerably – by 4 p.p. – and became the biggest source of spam with a share of 14.02%. Vietnam (11.01%, +1 p.p.) remained in second place. The US fell to third after its share (8.88%) dropped by 1.9 p.p.

As in the previous quarter, fourth and fifth were occupied by China (5.02%) and Mexico (4.22%) respectively, followed by Brazil (4.01%), Germany (3.80%) and Russia (3.55%). Turkey (2.95%) rounded off the TOP 10.

Spam email size



Breakdown of spam emails by size, Q2 and Q3 2016

Traditionally, the most commonly distributed emails are very small – up to 2 KB (55.78%), although the proportion of these emails has been declining throughout the year, and in Q3 dropped by 16 p.p. compared to the previous quarter. Meanwhile, the proportion of emails sized 10-20 KB increased considerably from 10.66% to 21.19%. The other categories saw minimal changes.

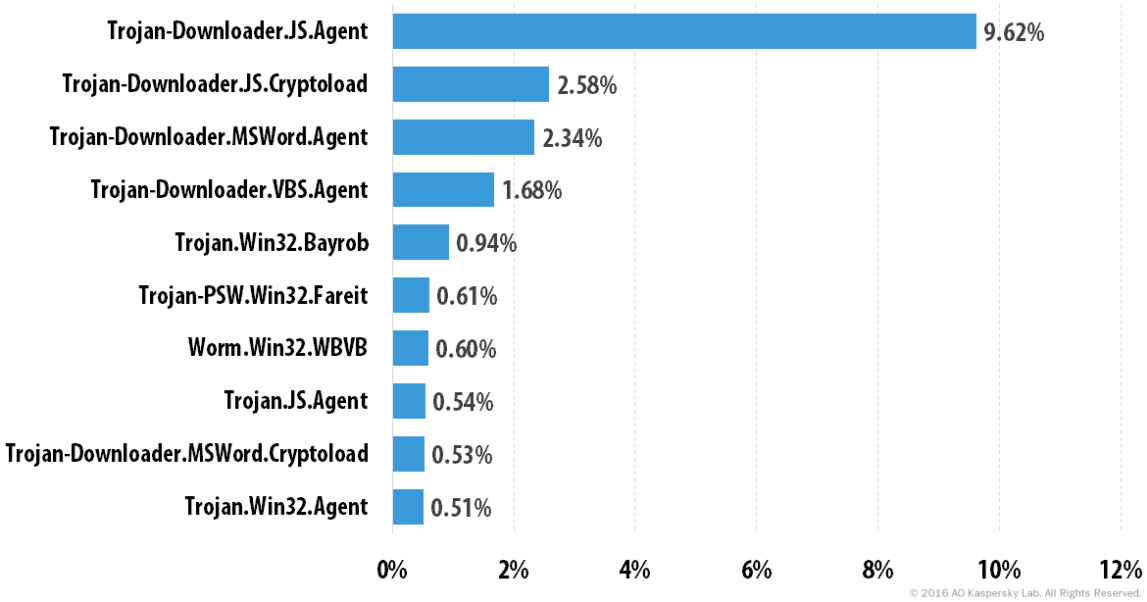
Malicious email attachments

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 to trigger mail antivirus.

TOP 10 malware families

Trojan-Downloader.JS.Agent (9.62%) once again topped the rating of the most popular malware families. Trojan-Downloader.JS.Cryptoload (2.58%) came second. Its share increased by 1.34 p.p. As in the previous quarter, Trojan-Downloader.MSWord.Agent (2.34%) completed the top three.

The popular Trojan-Downloader.VBS.Agent family (1.68%) fell to fourth with a 0.48 p.p. decline. It was followed by Trojan.Win32.Bayrob (0.94%).



TOP 10 malware families in Q3 2016

A number of newcomers made it into the bottom half of this TOP 10. Worm.Win32.WBVB (0.60%) in seventh place includes executable files written in Visual Basic 6 (in both P-code and Native modes) that are not recognized as trusted by KSN. The malware samples of this family are only detected by Mail Anti-Virus. For this type of verdict File Antivirus only detects objects with names that are likely to mislead users, for example, AdobeFlashPlayer, InstallAdobe, etc.

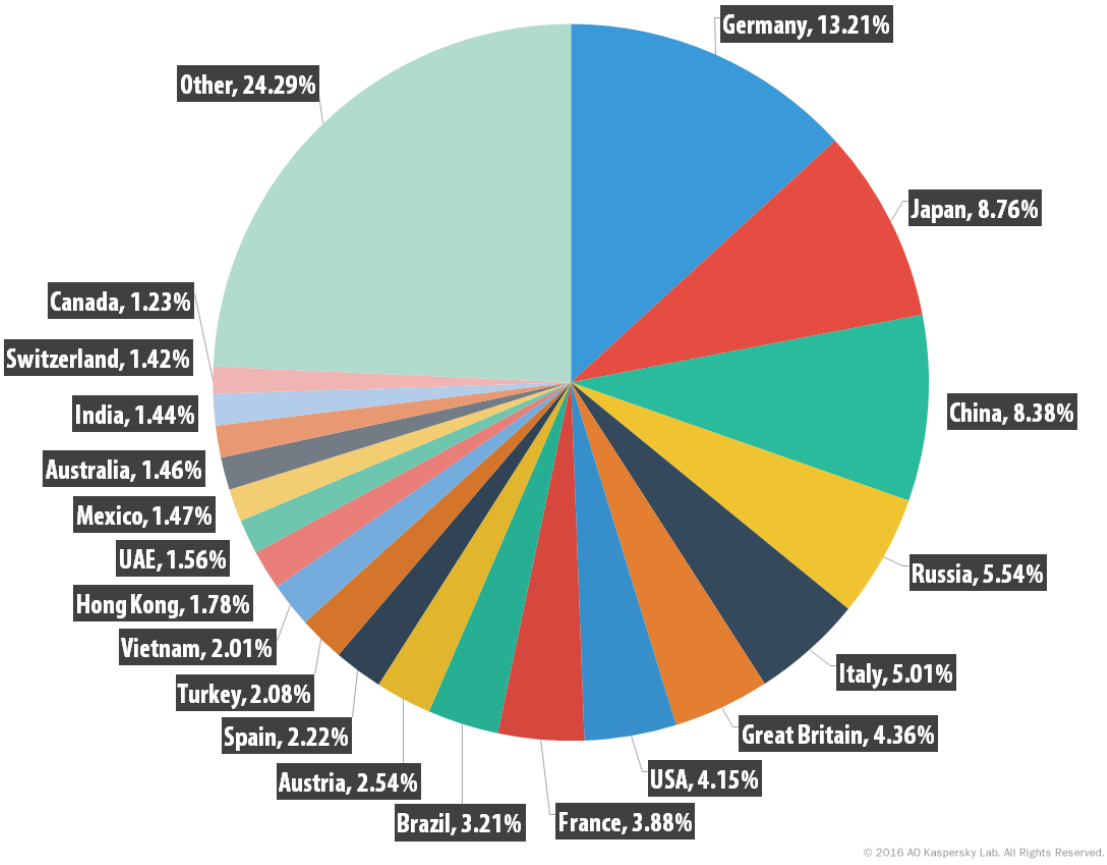
Trojan.JS.Agent (0.54%) came eighth. A typical representative of this family is a file with .wsf, .html, .js and other extensions. The malware is used to collect information about the browser, operating system and software whose vulnerabilities can be used. If the desired vulnerable software is found, the script tries to run a malicious script or an application via a specified link.

Yet another newcomer – Trojan-Downloader.MSWord.Cryptoload (0.52%) – occupied ninth place. It is usually a document with a .doc or .docx extension containing a script that can be executed in MS

Word (Visual Basic for Applications). The script includes procedures for establishing a connection, downloading, saving and running a file – usually a Trojan cryptor.

Trojan.Win32.Agent (0,51%), which was seventh in the previous quarter, rounded off the TOP 10 in the third quarter.

Countries targeted by malicious mailshots



Distribution of email antivirus verdicts by country, Q3 2016

Germany (13.21%) remained the country targeted most by malicious mailshots, although its share continued to decline – by 1.48 p.p. in Q3. Japan (8.76%), whose share increased by 2.36 p.p., moved up to second. China (8.37%) in third saw its share drop by 5.23 p.p.

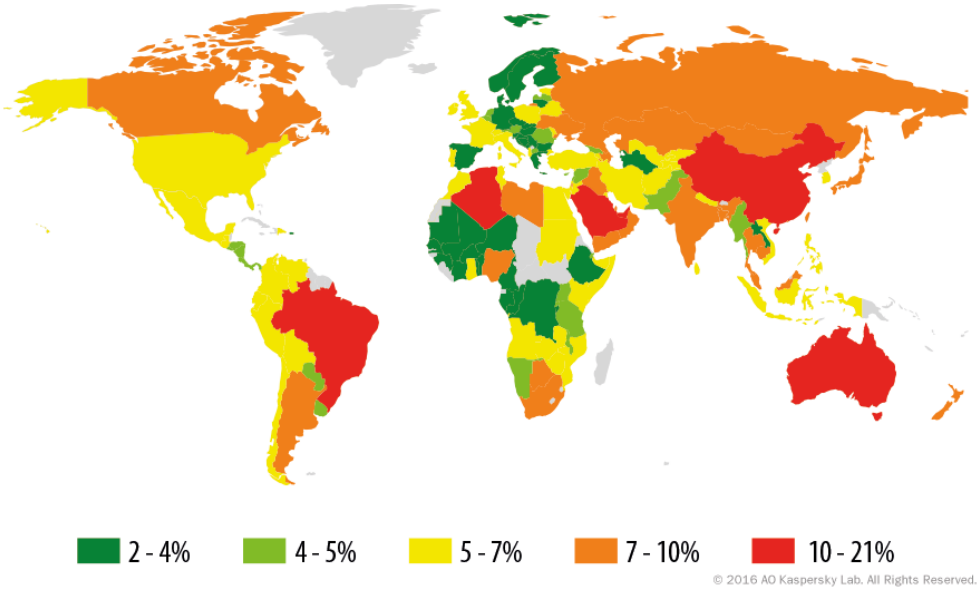
In Q3 2016, fourth place was occupied by Russia (5.54%); its contribution increased by 1.14 p.p. from the previous quarter. Italy came fifth with a share of 5.01%. The US remained in seventh (4.15%). Austria (2.54%) rounded off this TOP 10.

Phishing

In Q3 2016, the Anti-Phishing system was triggered **37,515,531** times on the computers of Kaspersky Lab users, which is **5.2** million more than the previous quarter. Overall, **7.75%** of unique users of Kaspersky Lab products worldwide were attacked by phishers in Q3 2016.

Geography of attacks

China (20.21%) remained the country where the largest percentage of users is affected by phishing attacks. In Q3 2016, the proportion of those attacked increased by 0.01 p.p.



Geography of phishing attacks*, Q3 2016

**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 0.4 p.p. and accounted for 18.23%, placing the country second in this rating. UAE added 0.88 p.p. to the previous quarter's figure and came third with 11.07%. It is followed by Australia (10.48%, -2.29 p.p.) and Saudi Arabia (10.13%, +1.5 p.p.).

TOP 10 countries by percentage of users attacked:

China	20.21%
Brazil	18.23%
United Arab Emirates	11.07%
Australia	10.48%
Saudi Arabia	10.13%

Algeria	10.07%
New Zealand	9.7%
Macau	9.67%
Palestinian Territory	9.59%
South Africa	9.28%

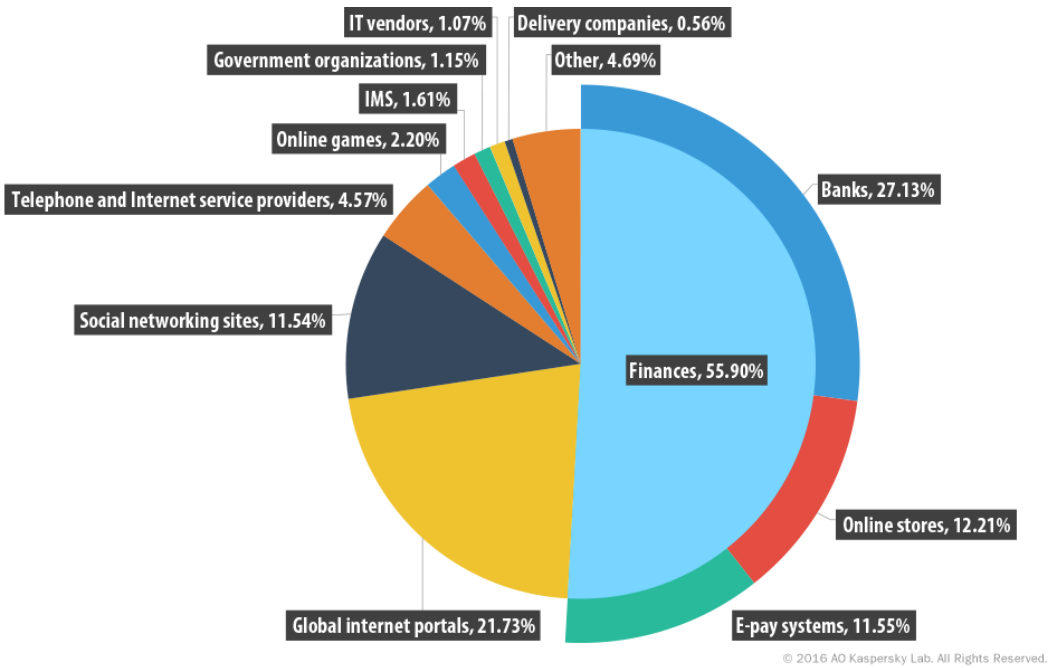
The share of attacked users in Russia amounted to 7.74% in the third quarter. It is followed by Canada (7.16%), the US (6.56%) and the UK (6.42%).

Organizations under attack

Rating the categories of organizations attacked by phishers

The rating of attacks by phishers on different categories of organizations is 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 Q3 of 2016, the share of the 'Financial organizations' category (banks, payment systems, online stores) accounted for more than half of all registered attacks. The percentage of the 'Banks' category increased by 1.7 p.p. and accounted for 27.13%. The proportion of 'Online stores' (12.21%) and 'Payment systems' (11.55%) increased by 2.82 p.p. and 0.31 p.p. respectively.



Distribution of organizations affected by phishing attacks by category, Q3 2016

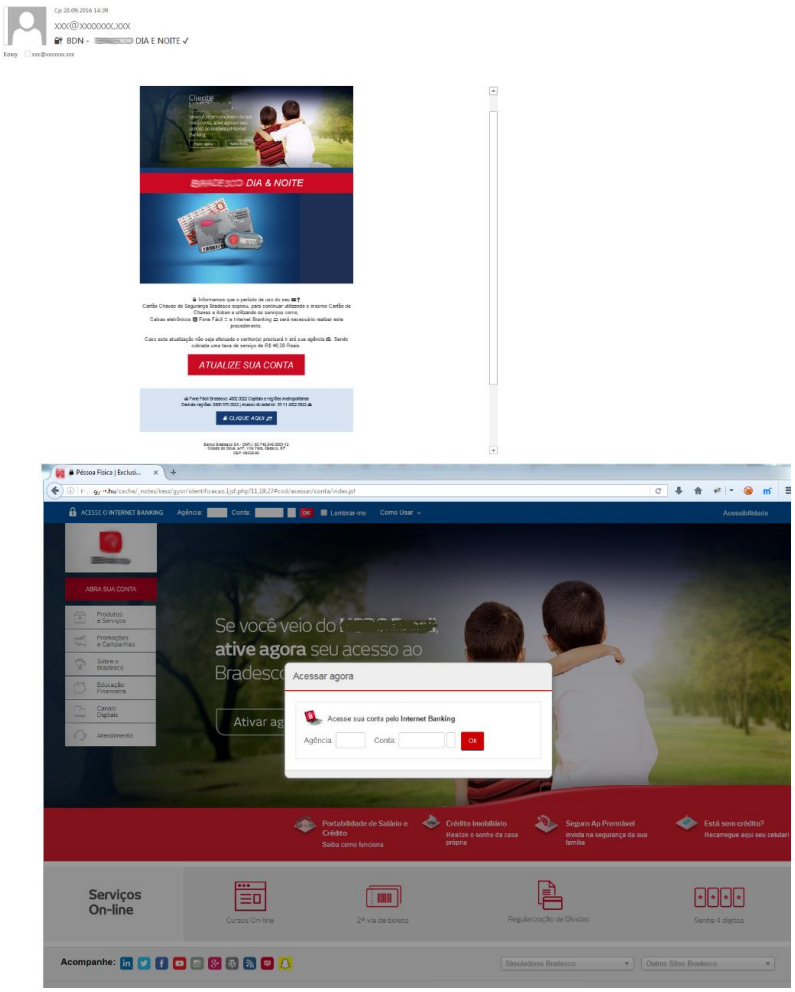
In addition to financial organizations, phishers most often attacked 'Global Internet portals' (21.73%), 'Social networking sites' (11.54%) and 'Telephone and Internet service providers' (4.57%). However, their figures remained almost unchanged from the previous quarter – the change for each category was no more than a single percentage point.

Hot topics this quarter

Attacks on users of online banking

The third quarter saw the proportion of attacked users in the 'Banks' category increase significantly – by 1.7 p.p. The four banks whose clients were attacked most often are all located in Brazil. For several years in a row this country has ranked among the countries with the highest proportion of users attacked by phishers, and occasionally occupies first place. Naturally, online banking users are priority targets for cybercriminals, since the financial benefits of a successful attack are self-evident.

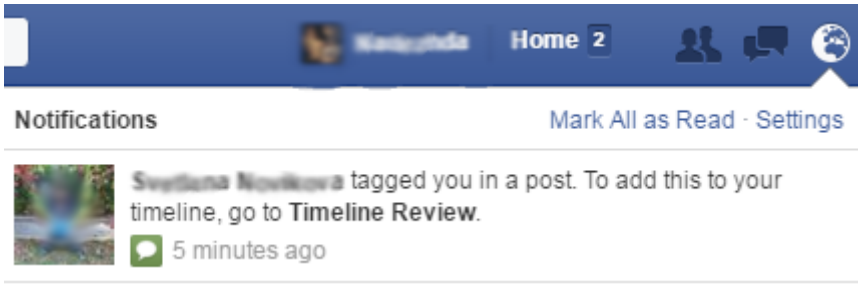
Links to fake banking pages are mostly spread via email.



Example of a phishing email sent on behalf of a Brazilian bank. The link in the email leads to a fake page that imitates the login page to the user's banking account

‘Porn virus’ for Facebook users

At the beginning of the previous quarter, Facebook users were subjected to phishing attacks. Almost half a year later, the same scheme was used by fraudsters to attack users in Europe. During the attack, a provocative adult video was used as bait. To view it, the user was directed to a fake page (a page on the xic.graphics domain was especially popular) imitating the popular YouTube video portal.



Example of a user being tagged in a post with the video

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.

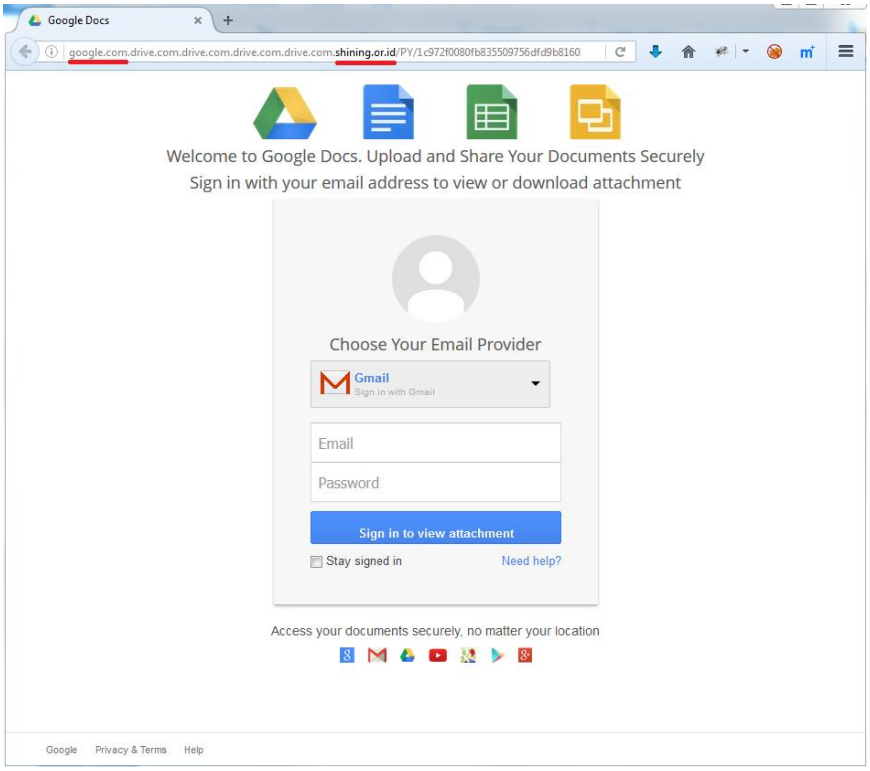
Phisher tricks

Carrying on from the second quarter, we continue to talk about the popular tricks of Internet fraudsters. The objectives are simple – to convince their victims that they are using legitimate resources and to bypass security software filters. It is often the case that the more convincing the page is for the victim, the easier it is to detect with a variety of technologies for combating fraudsters.

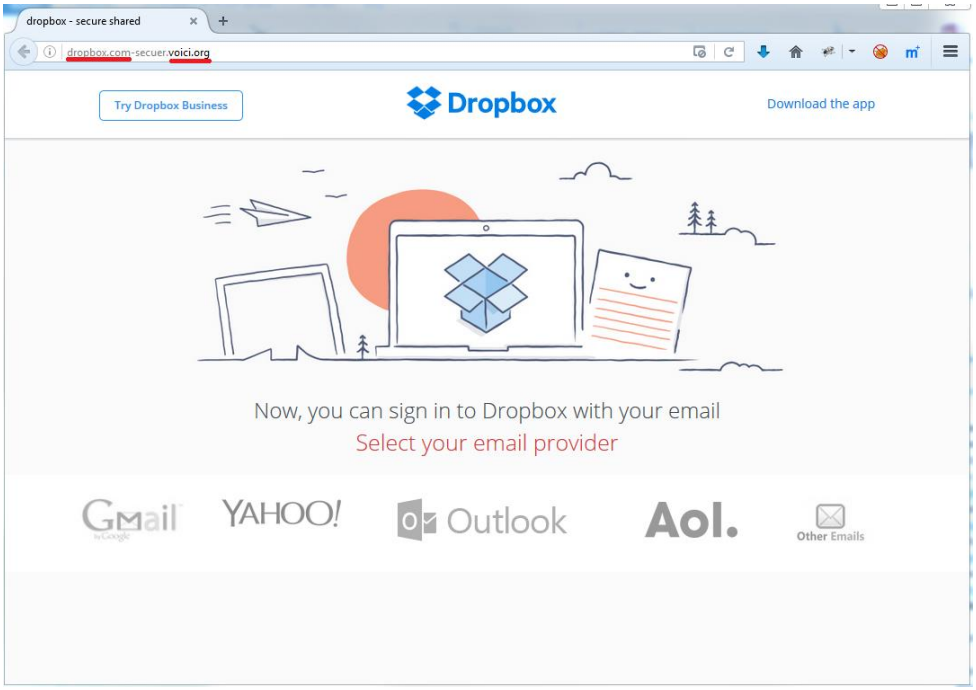
Nice domains

We have already described a trick whereby spammers use genuine-looking links in emails to spread phishing content. Fraudsters often resort to this technique regardless of how the phishing page is distributed. They are trying to mislead users, who do actually pay attention to the address in the address bar, but who are not technically savvy enough to see the catch.

The main domain of the organization that is being attacked might be represented, for example, by a 13th-level domain:



Or might simply be used in combination with another relevant word, e.g., secure:



These tricks help deceive potential victims, though they make it much easier to detect phishing attacks using security solutions.

Different languages for different victims

By using information about the IP address of a potential victim, phishers determine the country in which they are located. In the example below, they do so by using the service http://www.geoplugin.net/json.gp?ip=.

```
$ip_data = @json_decode(file_get_contents("http://www.geoplugin.net/json.gp?ip=".$ip));

if($ip_data && $ip_data->geoplugin_countryCode != null)
{
    $country = $ip_data->geoplugin_countryCode;
}

$ip_data2 = @json_decode(file_get_contents("http://www.geoplugin.net/json.gp?ip=".$ip));

if($ip_data2 && $ip_data2->geoplugin_countryName != null)
{
    $countryname = $ip_data2->geoplugin_countryName;
}
```

Depending on the country that has been identified, the cybercriminals will display pages with vocabulary in the corresponding language.

```
<?php
$aaaaaaaaa1 = "Meine Zusammenfas
$aaaaaaaaa2 = "Geld";
$aaaaaaaaa3 = "Aktivität";
$aaaaaaaaa4 = "Berichte";
$aaaaaaaaa5 = "Tools";
$aaaaaaaaa6 = "Mehr";
$aaaaaaaaa7 = "Abmelden";
$aaaaaaaaa8 = "Aktualisieren Sie
$aaaaaaaaa9 = "Einstellungen und
$aaaaaaaaa10 = "Schritt";
$aaaaaaaaa11 = "Personal";
$aaaaaaaaa12 = "Karten";
$aaaaaaaaa13 = "Bezahlung";
$aaaaaaaaa14 = "Bestätigen";
$aaaaaaaaa15 = "Weiter";
$aaaaaaaaa16 = "Zurück";
$aaaaaaaaa17 = "Schützen Sie Ihr
$aaaaaaaaa18 = "Jede Transaktion
$aaaaaaaaa19 = "Internet-Zahlung
$aaaaaaaaa20 = "&#80;&#97;&#121;
$aaaaaaaaa35 = "Sie müssen die I
$aaaaaaaaa38 = "Schließen Sie Ih
$aaaaaaaaa33 = "Alle Rechte vorb
$aaaaaaaaa34 = "Einige von Ihnen
$aaaaaaaaa22 = "Fehler : Anmeldu
$aaaaaaaaa24 = "Geben Sie eine g
$aaaaaaaaa26 = "Geben Sie ein Pa
$aaaaaaaaa23 = "E-Mail-Adresse";
$aaaaaaaaa28 = "E-Mail-Adresse v
$aaaaaaaaa25 = "Passwort";
$aaaaaaaaa27 = "Einloggen";
$aaaaaaaaa29 = "Neu anmelden";
$aaaaaaaaa30 = "Über &#80;&#97;&
$aaaaaaaaa36 = "Sitemap";
```

```
<?php
$aaaaaaaaa1 = "min Sammanfattning
$aaaaaaaaa2 = "Pengar";
$aaaaaaaaa3 = "Aktivitet";
$aaaaaaaaa4 = "rapporter";
$aaaaaaaaa5 = "Verktyg";
$aaaaaaaaa6 = "Mer";
$aaaaaaaaa7 = "Logga ut";
$aaaaaaaaa8 = "Uppdatera ditt kon
$aaaaaaaaa9 = "Inställningar och
$aaaaaaaaa10 = "Steg";
$aaaaaaaaa11 = "Personal";
$aaaaaaaaa12 = "Card";
$aaaaaaaaa13 = "Betalning";
$aaaaaaaaa14 = "Bekräfta";
$aaaaaaaaa15 = "Nästa";
$aaaaaaaaa16 = "Tillbaka";
$aaaaaaaaa17 = "Skydda dina penga
$aaaaaaaaa18 = "Varje transaktion
$aaaaaaaaa19 = "Internet betalkort
$aaaaaaaaa20 = "&#80;&#97;&#121;&
$aaaaaaaaa35 = "Du måste bekräfta
$aaaaaaaaa38 = "Stäng för att akt
$aaaaaaaaa33 = "Alla rättigheter
$aaaaaaaaa34 = "Viss information
$aaaaaaaaa22 = "Fel: Logga in ";
$aaaaaaaaa24 = "Ange en giltig e-
$aaaaaaaaa26 = "Lösenord krävs";
$aaaaaaaaa23 = "E-postadress";
$aaaaaaaaa28 = "Glömt din e-posta
$aaaaaaaaa25 = "Lösenord";
$aaaaaaaaa27 = "Logga in";
$aaaaaaaaa29 = "Skapa konto";
$aaaaaaaaa30 = "Om &#80;&#97;&#12
$aaaaaaaaa36 = "Utvecklare";
```

```
<?php
$aaaaaaaaa1 = "Benim Özeti";
$aaaaaaaaa2 = "Para";
$aaaaaaaaa3 = "etkinlik";
$aaaaaaaaa4 = "Raporlar";
$aaaaaaaaa5 = "Araçlar";
$aaaaaaaaa6 = "Daha";
$aaaaaaaaa7 = "Çıkış Yap";
$aaaaaaaaa8 = "Hesabınızı güncelleyin";
$aaaaaaaaa9 = "Ayarlar ve ödemeler";
$aaaaaaaaa10 = "Step";
$aaaaaaaaa11 = "Personel";
$aaaaaaaaa12 = "Kartpostal";
$aaaaaaaaa13 = "Ücret";
$aaaaaaaaa14 = "Onaylamak";
$aaaaaaaaa15 = "Bir sonraki";
$aaaaaaaaa16 = "Geri";
$aaaaaaaaa17 = "Paranızı koruma";
$aaaaaaaaa18 = "Her işlem izlenir ve ağır dolandırıcılık
$aaaaaaaaa19 = "İnternet ödeme kartları";
$aaaaaaaaa20 = "&#80;&#97;&#121;&#80;&#97;I online ödeme
$aaaaaaaaa35 = "Hesabınıza bu sorunu ve erişim düzeltmek
$aaaaaaaaa38 = "Hesabınızı etkinleştirmek için Kapat";
$aaaaaaaaa33 = "Her hakkı saklıdır.";
$aaaaaaaaa34 = "Girdiğiniz Bazı bilgiler doğru değil.";
$aaaaaaaaa22 = "Hata: Giriş ";
$aaaaaaaaa24 = "Geçerli bir e-posta adresi gereklidir";
$aaaaaaaaa26 = "Şifre gereklidir";
$aaaaaaaaa23 = "E-posta adresi";
$aaaaaaaaa28 = "E-posta adresinizi unuttunuz mu?";
$aaaaaaaaa25 = "Şifre";
$aaaaaaaaa27 = "Giriş Yapın";
$aaaaaaaaa29 = "Hesap Açın";
$aaaaaaaaa30 = "Yardım";
$aaaaaaaaa36 = "Güvenlik";
```

Examples of files that are used to display a phishing page in a specified language

```
<!-- end /.header-->
<div  for=\"". rand(99999999999, 999999999999999999999999)."\"  class=\"content\">
    <!-- start steps -->
    <div  for=\"". rand(99999999999, 999999999999999999999999)."\"  class=\"kansawb-adawat-spam-omakanspamich
        <div class=\"span4 step\">
            <div  id=\"". rand(99999999999999, 999999999999999999999999)."\"   class=\"steps\">
                <span>". $aaaaaaaal10 ." 1</span>
                <p>". $aaaaaaaal11 ." info</p>
            </div>
        </div>
        <div  for=\"". rand(99999999999, 999999999999999999999999)."\"  class=\"span4 step\">
            <div class=\"steps\">
                <span>". $aaaaaaaal10 ." 2</span>
                <p>". $aaaaaaaal12 ." info</p>
            </div>
        </div>
        <div  id=\"". rand(99999999999999, 999999999999999999999999)."\"   class=\"span4 step\">
            <div  for=\" ".md5(gmdate('r'))." \"  class=\"steps\">
                <span>". $aaaaaaaal10 ." 3</span>
                <p>". $aaaaaaaal13 ." info</p>
            </div>
        </div>
    </div>
    <fieldset  for=\" ".md5(gmdate('r'))." \" >
        <div  for=\"". rand(99999999999, 999999999999999999999999)."\"  class=\"divider gap-bottom-25\"></div
        <!-- start name -->
        <div  for=\" ".md5(gmdate('r'))." \"  class=\"kansawb-adawat-spam-omakanspamich\">
            <div class=\" unit\">
                <div class=\"input\">
                    <input value=\"".$_SESSION['AYCOUNT']."\" type=\"text\" id=\"first_name\" name=\"first_na
                </div>
            </div>
            <div  for=\"". rand(99999999999, 999999999999999999999999)."\"  class=\" unit\">
                <div class=\"input\">
                    <input  for=\"". rand(99999999999, 999999999999999999999999)."\"  type=\"text\" id=\"last
                </div>
```

The example below shows 11 different versions of pages for 32 different locations:

```
if ($country == "FR" || $country == "DZ" || $country == "MA" || $country == "TN" || $country == "CD" || $country == "MG" || $c
    $_SESSION['ANONISMA-AYOUB']="/fr.php";
} elseif ($country == "MX" || $country == "PH" || $country == "ES" || $country == "CO" || $country == "AR" || $country == "PE"
    $_SESSION['ANONISMA-AYOUB']="/es.php";
} elseif ($country == "IT" || $country == "SM") {
   $_SESSION['ANONISMA-AYOUB']="/it.php";
} elseif ($country == "RU" || $country == "BY" || $country == "KZ" || $country == "KG" || $country == "TJ") {
    $_SESSION['ANONISMA-AYOUB']="/ru.php";
}
elseif ($country == "PT" || $country == "BR" || $country == "AO" || $country == "MZ" || $country == "MO") {
    $_SESSION['ANONISMA-AYOUB']="/pt.php";
}
elseif ($country == "TR" || $country == "cy") {
    $_SESSION['ANONISMA-AYOUB']="/tr.php";
}
elseif ($country == "PL") {
    $_SESSION['ANONISMA-AYOUB']="/pl.php";
}
elseif ($country == "NO") {
    $_SESSION['ANONISMA-AYOUB']="/no.php";
}
elseif ($country == "NL" || $country == "AW") {
    $_SESSION['ANONISMA-AYOUB']="/nl.php";
}
elseif ($country == "DE" || $country == "CH") {
    $_SESSION['ANONISMA-AYOUB']="/de.php";
}
else {
   $_SESSION['ANONISMA-AYOUB']="/en.php";
```

Example of a script used by phishers to display the relevant page depending on the location of the victim

TOP 3 attacked organizations

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 are for phishing pages hiding behind the names of fewer than 15 companies.

The TOP 3 organizations attacked most frequently by phishers accounted for 21.96% of all phishing links detected in Q3 2016.

Organization	% of detected phishing links
Facebook	8.040955
Yahoo!	7.446908
Amazon.com	6.469801

In Q3 2016, Facebook (8.1%, +0.07 p.p.) topped the ranking of organizations used by fraudsters to hide their attacks. Microsoft, the leader in the previous quarter, dropped out of the TOP 3. Second place was occupied by Yahoo! (7.45%), whose contribution increased by 0.38 p.p. Third place went to Amazon, a newcomer to the TOP 3 with 6.47%.

Conclusion

In the third quarter of 2016, the proportion of spam in email traffic increased by 2 p.p. compared to the previous quarter and accounted for 59.19%. The largest percentage of spam – 61.25% – was registered in September. India (14.02%), which was only fourth in the previous quarter, became the biggest source of spam. The top three sources also included Vietnam (11.01%) and the US (8.88%).

The top three countries targeted by malicious mailshots remained unchanged from the previous quarter. Germany (13.21%) came first again, followed by Japan (8.76%) and China (8.37%).

In Q3 2016, Kaspersky Lab products prevented over 37.5 million attempts to enter phishing sites, which is 5.2 million more than the previous quarter. Financial organizations were the main target, with banks the worst affected, accounting for 27.13% of all registered attacks. The most attractive phishing targets in Q3 2016 were clients of four banks located in Brazil.