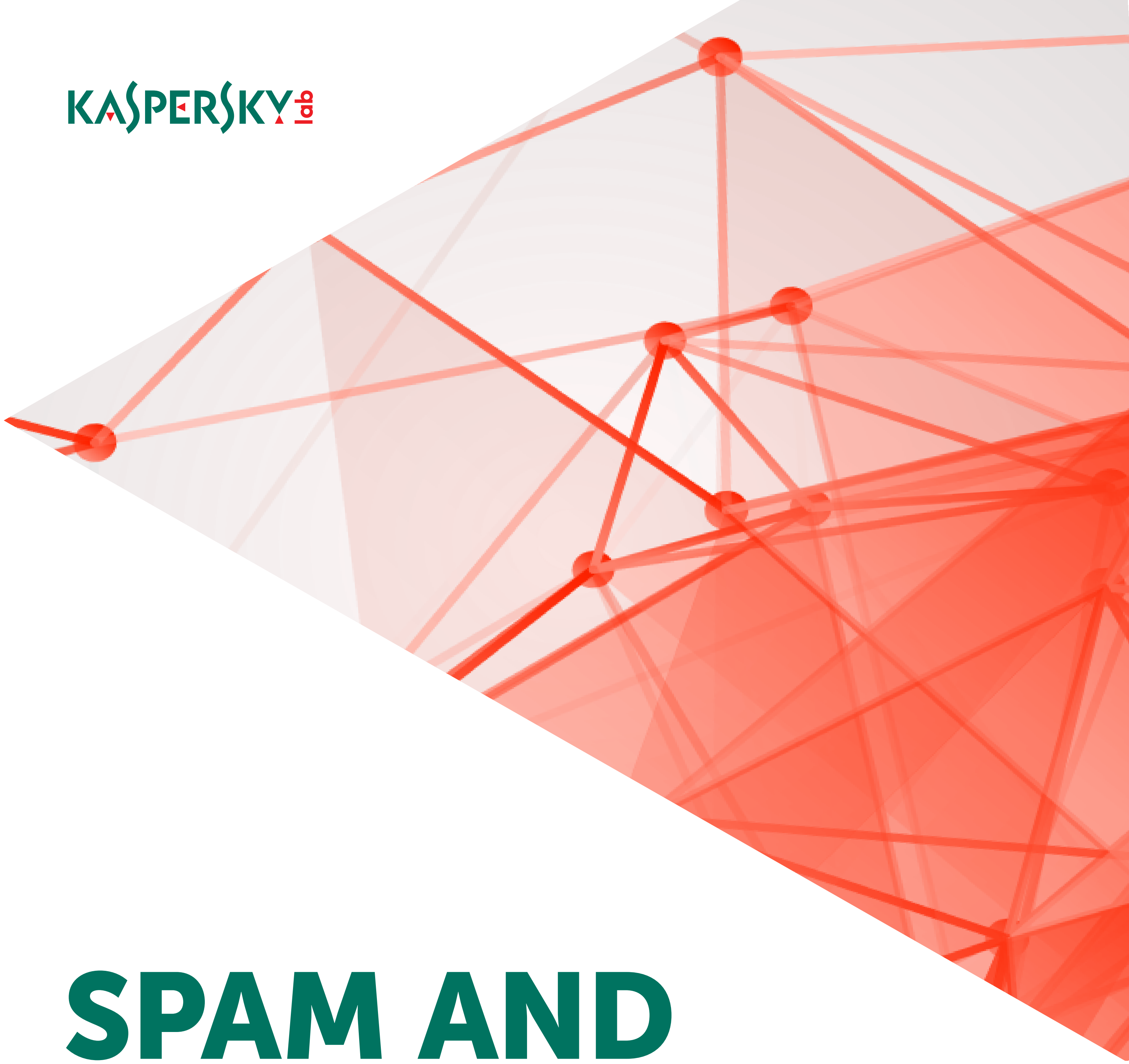


SPAM AND PHISHING IN Q3 2015

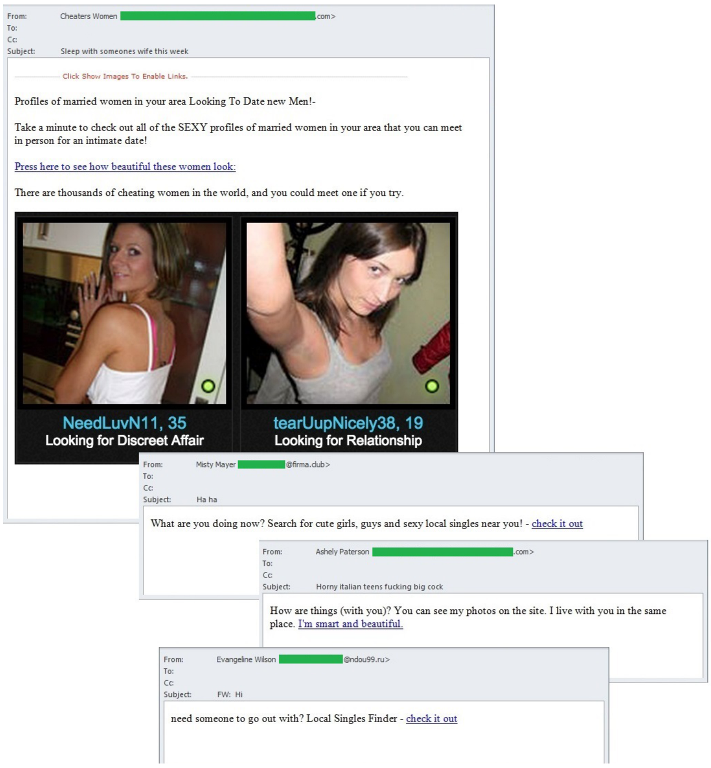
Tatyana Shcherbakova,
Maria Vergelis,
Nadezhda Demidova

CONTENTS

SPAM: FEATURES OF THE QUARTER

Online dating

The dating theme is typical for spam emails, but in the third quarter of 2015 we couldn't help but notice the sheer variety appearing in these types of mailings. We came across some rather interesting attempts to deceive recipients and to bypass filters, as well as new types of spam mailings that were bordering on fraud.



From: Cheaters Women [redacted].com>
To:
Cc:
Subject: Sleep with someones wife this week

Click Show Images To Enable Links.

Profiles of married women in your area Looking To Date new Men!-

Take a minute to check out all of the SEXY profiles of married women in your area that you can meet in person for an intimate date!

Press here to see how beautiful these women look:

There are thousands of cheating women in the world, and you could meet one if you try.

From: Misty Mayer [redacted]@firma.club>
To:
Cc:
Subject: Ha ha

What are you doing now? Search for cute girls, guys and sexy local singles near you! - check it out

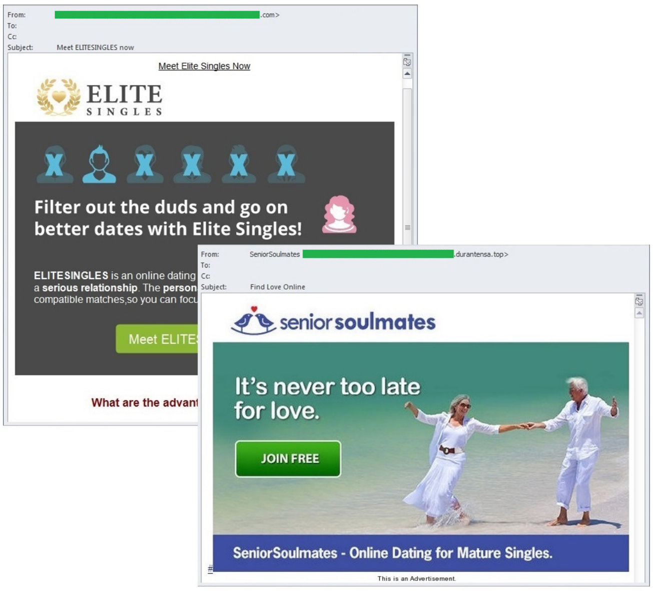
From: Ashely Paterson [redacted].com>
To:
Cc:
Subject: Horny italian teens fucking big cock

How are things (with you)? You can see my photos on the site. I live with you in the same place. I'm smart and beautiful.

From: Evangeline Wilson [redacted]@ndou99.ru>
To:
Cc:
Subject: FW: Hi

need someone to go out with? Local Singles Finder - check it out

The main aim of spammers exploiting the dating theme is usually to advertise recently created dating sites that are still relatively unknown. The owners of these sites resort to spamming to attract the largest possible audience to their resource. The messages often address different categories of recipients, for example, dating sites for older people, married people or the religious.



From: [redacted].com>
To:
Cc:
Subject: Meet ELITESINGLES now

Meet Elite Singles Now

ELITE
SINGLES
Filter out the duds and go on better dates with Elite Singles!

ELITESINGLES is an online dating
a serious relationship. The person
compatible matches,so you can focu

What are the advant

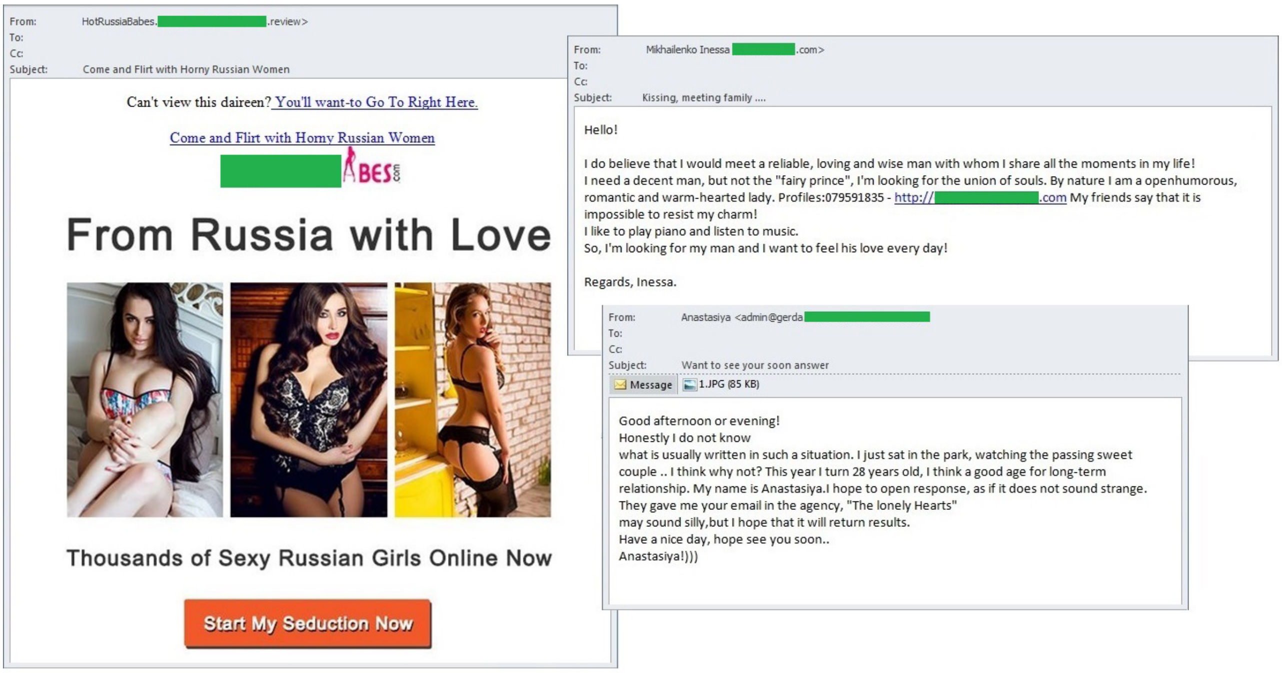
From: SeniorSoulmates [redacted].durantensa.top>
To:
Cc:
Subject: Find Love Online

senior soulmates
It's never too late for love.
JOIN FREE
SeniorSoulmates - Online Dating for Mature Singles.

This is an Advertisement.

Yet another type of advert is for marriage agencies offering a selection of brides (mainly from Russia and Ukraine) to foreign suitors. This type of spam is usually distributed in the English-language segment of the Internet. The messages contain an invitation to register on a site, a short text promising to find the perfect life partner and a link leading to the advertised site.

Similar emails can also be sent from a "bride". This type of spam is closer to the fraudulent tactics used by 'Nigerian letters'. The email is supposedly written by a girl who provides a few details about herself, about how hard her life is in the Russian hinterland, and her dreams of meeting Prince Charming. A photo is often attached, though not necessarily a photo of the "bride" – it could easily be taken from someone's social networking page and attached to make the message look more convincing. That's why emails from different girls may contain the same photos. However, the messages vary: a host of synonyms are used to bypass spam filters. The usual channel for receiving feedback is via email. The address is different for each email – they are obviously created in large quantities on free email services for each mass mailing. After replying, the user will, at best, receive a notification that the address is non-existent. The worst case scenarios will see his address targeted by further spam mailings and he may even get caught up in a scam where the girl asks for money to buy a ticket to come and see him. Once she gets the money, she disappears without a trace.



From: HotRussiaBabes.[redacted].review>
To:
Cc:
Subject: Come and Flirt with Horny Russian Women

Can't view this daireen? You'll want-to Go To Right Here.

Come and Flirt with Horny Russian Women

[redacted] BES.com

From Russia with Love

Thousands of Sexy Russian Girls Online Now

From: Mikhailenko Inessa [redacted].com>
To:
Cc:
Subject: Kissing, meeting family ....

Hello!

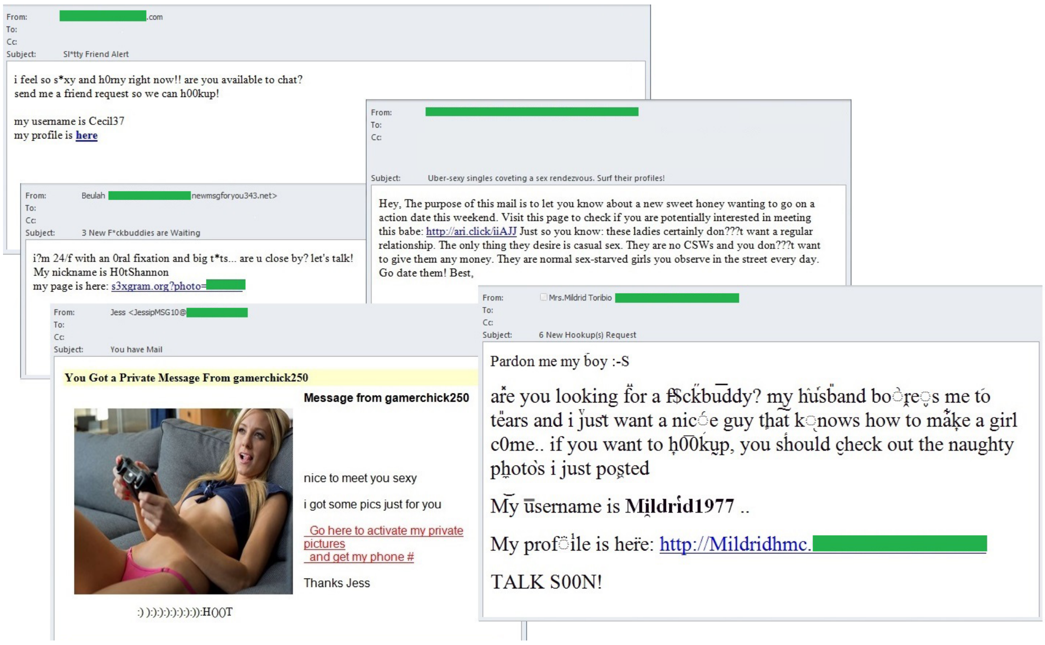
I do believe that I would meet a reliable, loving and wise man with whom I share all the moments in my life!
I need a decent man, but not the "fairy prince", I'm looking for the union of souls. By nature I am a openhumorous, romantic and warm-hearted lady. Profiles:079591835 - http://[redacted].com My friends say that it is impossible to resist my charm!
I like to play piano and listen to music.
So, I'm looking for my man and I want to feel his love every day!

Regards, Inessa.

From: Anastasiya <admin@gerda[redacted]
To:
Cc:
Subject: Want to see your soon answer

Good afternoon or evening!
Honestly I do not know
what is usually written in such a situation. I just sat in the park, watching the passing sweet couple .. I think why not? This year I turn 28 years old, I think a good age for long-term relationship. My name is Anastasiya.I hope to open response, as if it does not sound strange.
They gave me your email in the agency, "The lonely Hearts"
may sound silly,but I hope that it will return results.
Have a nice day, hope see you soon..
Anastasiya!)))

A similar method is used to advertise dating sites "for adults". The emails contain either an invitation to register on the site and a promise of intimate dating, or a message from a girl who is looking for a partner for intimate relations plus a link to the resource with her alleged profile. This type of spam is often disguised as personal notifications on social networking sites, as well as image or audio files sent via instant messengers. As a result, the site is hidden, and the user cannot clearly identify what it is until he follows all the links. Of course, the contents of these messages aim to arouse the recipient's interest and make him click the links, often due to the flirty content or heavy hints and intimate photos.



From: [redacted].com
To:
Cc:
Subject: Sl*tty Friend Alert

i feel so s*xy and h0rny right now!! are you available to chat?
send me a friend request so we can h00kup!

my username is Cecil37
my profile is here

From: [redacted]
To:
Cc:
Subject: Uber-sexy singles coveting a sex rendezvous. Surf their profiles!

Hey, The purpose of this mail is to let you know about a new sweet honey wanting to go on a action date this weekend. Visit this page to check if you are potentially interested in meeting this babe: http://ari.click/iiAJJ Just so you know: these ladies certainly don???t want a regular relationship. The only thing they desire is casual sex. They are no CSWs and you don???t want to give them any money. They are normal sex-starved girls you observe in the street every day. Go date them! Best,

From: Beulah [redacted]newmsgforyou343.net>
To:
Cc:
Subject: 3 New F*ckbuddies are Waiting

i?m 24/f with an 0ral fixation and big t*ts... are u close by? let's talk!
My nickname is H0tShannon
my page is here: s3xgram.org?photo=[redacted]

From: Jess <JessipMSG10@[redacted]
To:
Cc:
Subject: You have Mail

You Got a Private Message From gamerchick250

Message from gamerchick250

nice to meet you sexy

i got some pics just for you

Go here to activate my private pictures
and get my phone #

Thanks Jess

:)):):):):):):)):H()()T

From: ☐ Mrs.Mildrid Toribio [redacted]
To:
Cc:
Subject: 6 New Hookup(s) Request

Pardon me my b̄oy :-S

ar̽e you looking f̈or a f$cǩbūddy? my hu̓sb̈and bo◌̀re◌̧s me to
tëars and i ǰust want a nic◌́e guy th̰at k◌̧nows how to măk̽e a girl
c0me.. if you want to ḥ00ku̧p, you sh̉ould ̧check out the naughty
pho̱tos̀ i just pos̥ted

Mỹ ūsername is **Mi̯ldri̓d1977** ..

My prof◌̉ile is hėre: http://Mildridhmc.[redacted]

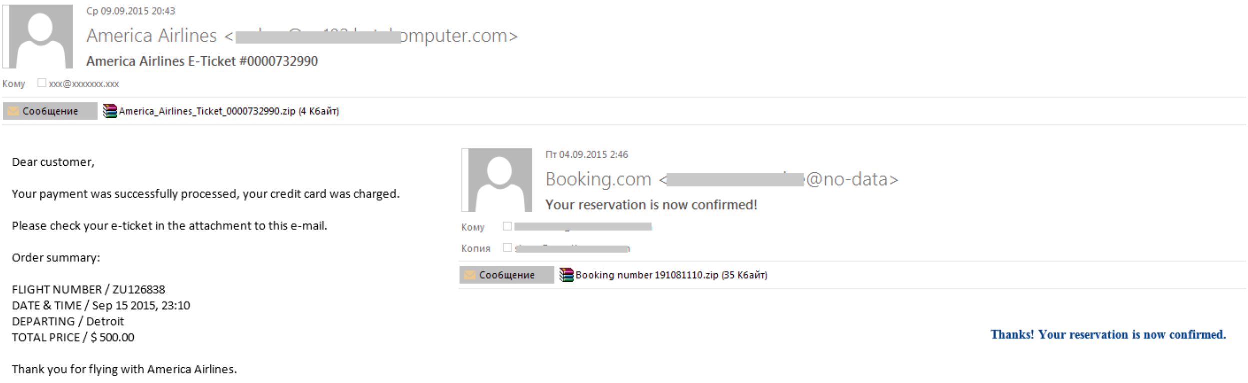
TALK S00N!

And finally, yet another type of spam we detected in Q3 was quite blatantly fraudulent. During the quarter we observed a mass mailing that prompted recipients to send a text message to a specific telephone number; in return a girl promised to send intimate photos of herself. The text of the emails varied, as did the mobile numbers specified in them. We sent messages to some of the numbers and found that they were not premium-rate numbers as might be expected, and users were not charged for sending a text message. We got a reply from a girl, but after a couple of answers it became clear we were dealing with a robot whose task was to make us download an application so we could continue chatting and receive the promised photos. As a result, we received several text messages containing short links that led to an article about useful mobile apps that appeared in a well-known American newspaper. During the redirect to the article an archive with mobile malware was downloaded to the user's phone.

Seasonal malicious spam

The amount of seasonal spam traditionally increases in summer. This is true for both advertising and malicious spam. The holiday season saw spam with a travel theme: fake notifications from booking services, airlines and hotels were used to spread malicious programs.

Fake notifications from major international airlines and booking services were detected by Kaspersky Lab as Trojan-Downloader.JS.Agent.hhy and Trojan-Downloader.Win32.Upatre.



Ср 09.09.2015 20:43
America Airlines <[redacted]mputer.com>
America Airlines E-Ticket #0000732990
Кому ☐ xxx@xxxxxxx.xxx
Сообщение America_Airlines_Ticket_0000732990.zip (4 Кбайт)

Dear customer,

Your payment was successfully processed, your credit card was charged.

Please check your e-ticket in the attachment to this e-mail.

Order summary:

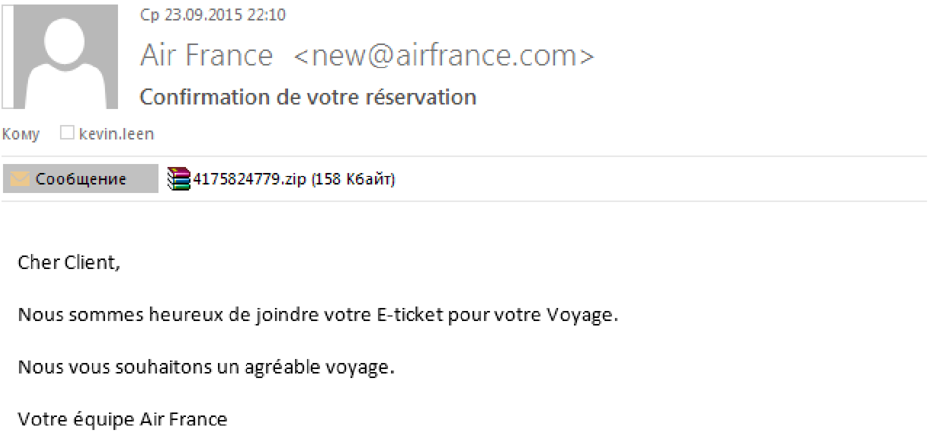
FLIGHT NUMBER / ZU126838
DATE & TIME / Sep 15 2015, 23:10
DEPARTING / Detroit
TOTAL PRICE / $ 500.00

Thank you for flying with America Airlines.

Пт 04.09.2015 2:46
Booking.com <[redacted]@no-data>
Your reservation is now confirmed!
Кому ☐ [redacted]
Копия ☐ [redacted]
Сообщение Booking number 191081110.zip (35 Кбайт)

Thanks! Your reservation is now confirmed.

We came across similar emails supposedly sent by popular airlines that had messages in French. The text informed recipients that the attachment contained an e-ticket. In fact, the ZIP archive contained Trojan.Win32.Xtrat Trojan and the DDoS bot Nitol (the module used to organize DDoS attacks).



Ср 23.09.2015 22:10

Air France <new@airfrance.com>

Confirmation de votre réservation

Кому □ kevin.leen

Сообщение 4175824779.zip (158 Кбайт)

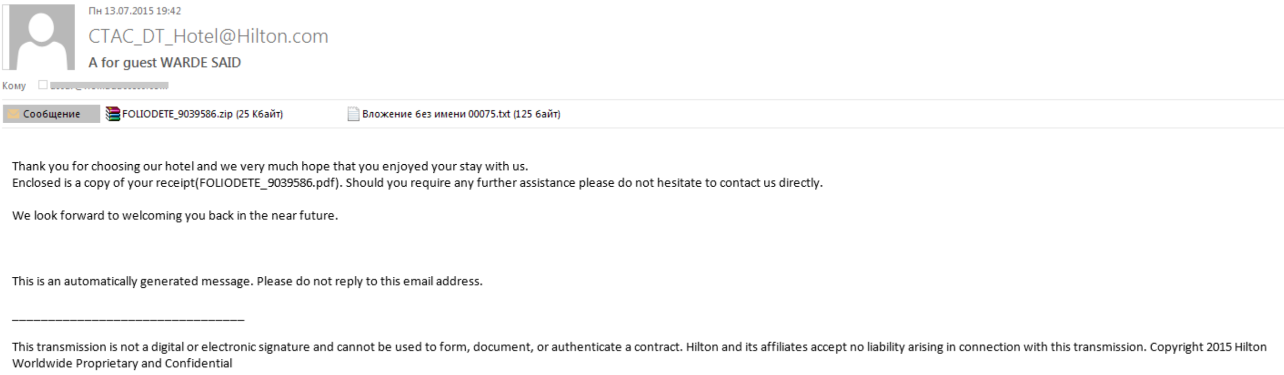
Cher Client,

Nous sommes heureux de joindre votre E-ticket pour votre Voyage.

Nous vous souhaitons un agréable voyage.

Votre équipe Air France

In July, fraudsters tried to trick users by sending fake notifications on behalf of hotels. The message thanked the recipients for staying in their hotel and asked them to view the attached bill. The attached archive actually contained Trojan-Downloader.Win32.Upatre.dhwi, which in turn downloaded and ran Trojan- Banker.Win32.Dyre (viewed as 98. ***. **. 39/cv17.rar) by clicking the links written in the body of the downloader.



Пн 13.07.2015 19:42

CTAC_DT_Hotel@Hilton.com

A for guest WARDE SAID

Кому □ [redacted]

Сообщение FOLIODETE_9039586.zip (25 Кбайт) Вложение без имени 00075.txt (125 байт)

Thank you for choosing our hotel and we very much hope that you enjoyed your stay with us.
Enclosed is a copy of your receipt(FOLIODETE_9039586.pdf). Should you require any further assistance please do not hesitate to contact us directly.

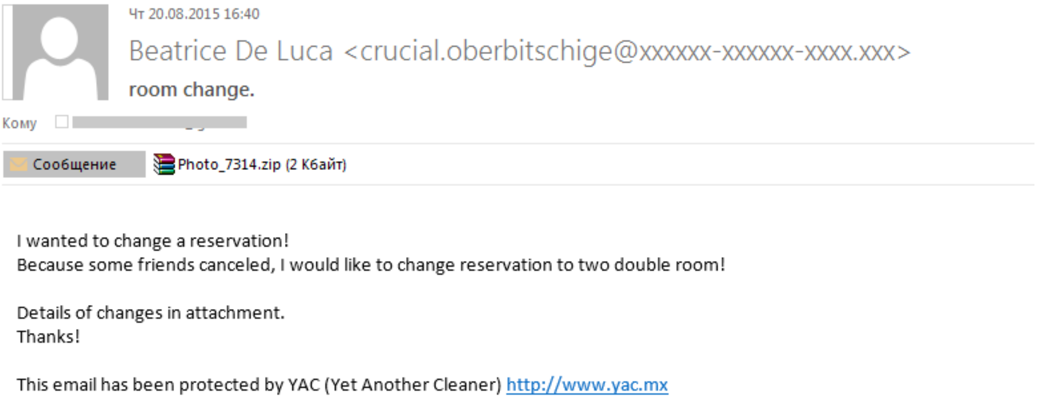
We look forward to welcoming you back in the near future.

This is an automatically generated message. Please do not reply to this email address.

____

This transmission is not a digital or electronic signature and cannot be used to form, document, or authenticate a contract. Hilton and its affiliates accept no liability arising in connection with this transmission. Copyright 2015 Hilton Worldwide Proprietary and Confidential

In addition to fake emails sent on behalf of well-known companies we observed a message in English from an individual. The email contained a request to change a room booking because some friends had cancelled.



Чт 20.08.2015 16:40

Beatrice De Luca <crucial.oberbitschige@xxxxxx-xxxxxx-xxxx.xxx>

room change.

Кому □ [redacted]

Сообщение Photo_7314.zip (2 Кбайт)

I wanted to change a reservation!
Because some friends canceled, I would like to change reservation to two double room!

Details of changes in attachment.
Thanks!

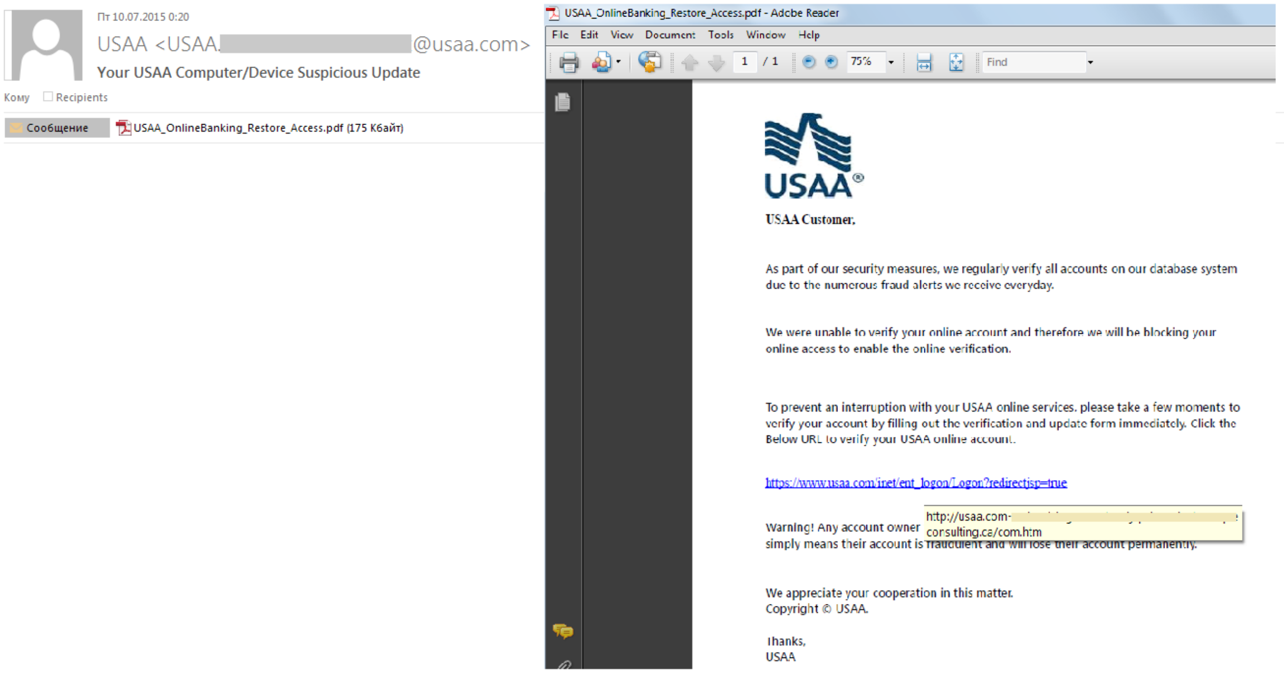
This email has been protected by YAC (Yet Another Cleaner) http://www.yac.mx

The text in the email could easily be seen as a legitimate request from a client; however, the ZIP attachment contained Trojan-Downloader.JS.Agent.hhi that downloaded Backdoor.Win32.Androm.

Spammer tricks

The text in a standard phishing email is usually in the body of the message, while personal information is entered on a web page that opens after clicking a fraudulent link in the text, or in the HTML fields of a page attached to the email, or is sent back in a reply email. The latter is most typical when asking recipients to confirm the address and the password for an email account.

In Q3 2015, cybercriminals came up with a new way of distributing phishing emails and bypassing spam filters. The text of the phishing email and the fake link were included in a PDF document attached to the email. After clicking the link, a standard phishing page opened and the user was asked to enter his personal information. The majority of emails utilizing the new technique imitated bank notifications. The body of these messages usually contained a short text describing the problem; sometimes there was no text at all.


USAA_OnlineBanking_Restore_Access.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 1
75%
Find
USAA®

Пт 10.07.2015 0:20

USAA <USAA.[redacted]@usaa.com>

Your USAA Computer/Device Suspicious Update

Кому □ Recipients

Сообщение USAA_OnlineBanking_Restore_Access.pdf (175 Кбайт)

USAA Customer,

As part of our security measures, we regularly verify all accounts on our database system due to the numerous fraud alerts we receive everyday.

We were unable to verify your online account and therefore we will be blocking your online access to enable the online verification.

To prevent an interruption with your USAA online services. please take a few moments to verify your account by filling out the verification and update form immediately. Click the Below URL to verify your USAA online account.

https://www.usaa.com/inet/ent_logon/Logon?redirectjsp=true

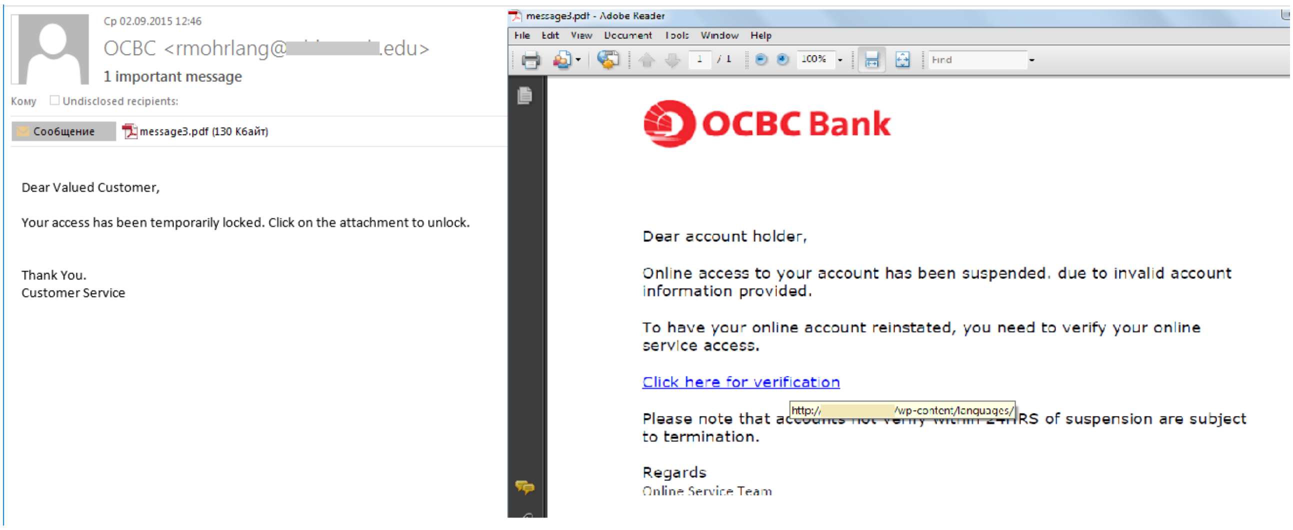
http://usaa.com-[redacted] consulting.ca/com.htm

Warning! Any account owner simply means their account is fraudulent and will lose their account permanently.

We appreciate your cooperation in this matter.
Copyright © USAA.

Thanks,
USAA

It should be noted that the spammers used well-known phrases and tricks in the text of the emails: notifications about an account being blocked, the need to pass a verification procedure, security issues, an investigation into phishing incidents, etc. As usual, the fraudulent links were masked by legitimate links and text fragments.


message3.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 1
100%
Find
OCBC Bank

Ср 02.09.2015 12:46

OCBC <rmohrlang@[redacted].edu>

1 important message

Кому □ Undisclosed recipients:

Сообщение message3.pdf (130 Кбайт)

Dear Valued Customer,

Your access has been temporarily locked. Click on the attachment to unlock.

Thank You.
Customer Service

Dear account holder,

Online access to your account has been suspended. due to invalid account information provided.

To have your online account reinstated, you need to verify your online service access.

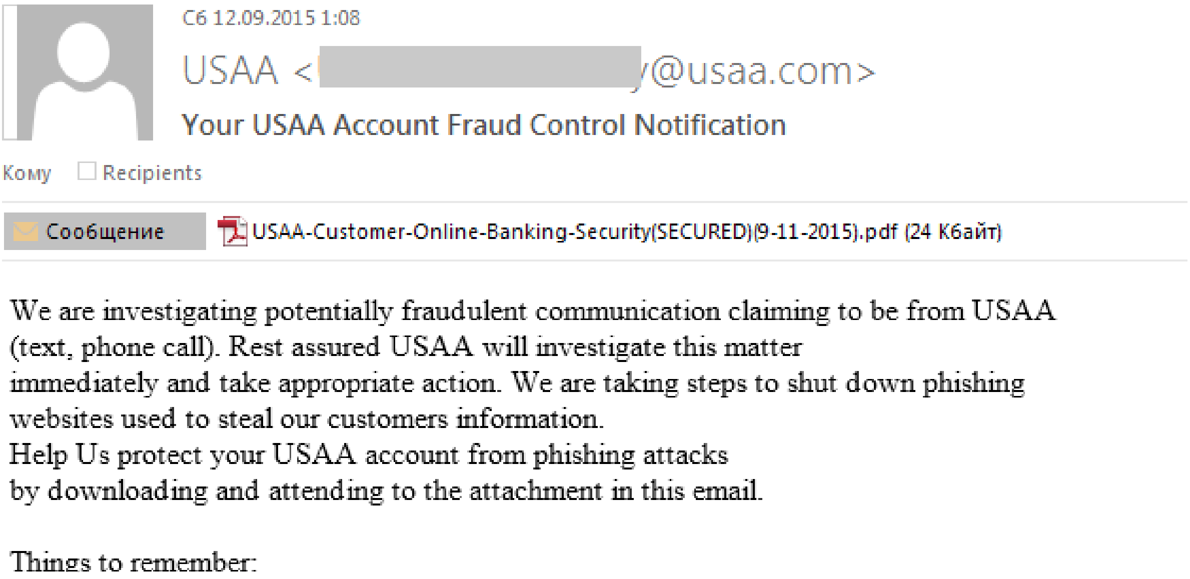
Click here for verification

http://[redacted]/wp-content/languages/

Please note that accounts not verify within 24HRS of suspension are subject to termination.

Regards
Online Service Team

However, there were emails with detailed text in the message body providing genuine links to official bank resources. The phishing notification was included in the PDF attachment.



Сб 12.09.2015 1:08

USAA <[redacted]@usaa.com>

Your USAA Account Fraud Control Notification

Кому □ Recipients

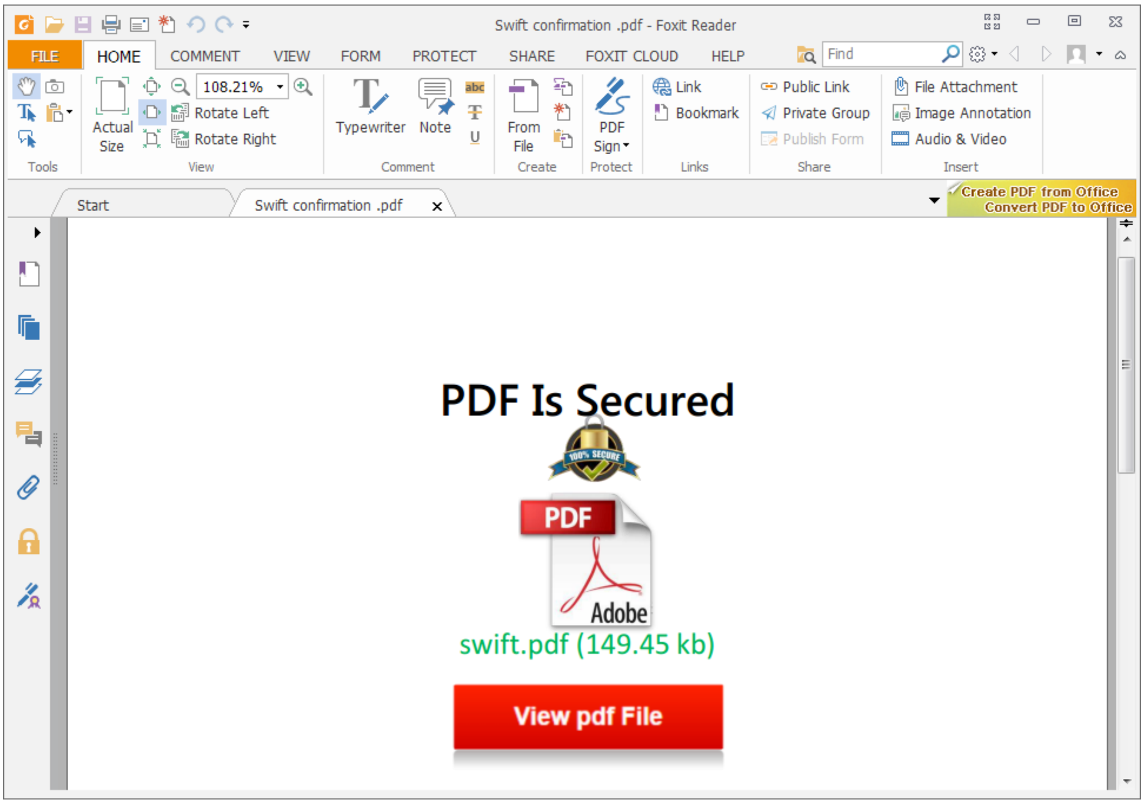
Сообщение | USAA-Customer-Online-Banking-Security(SECURED)(9-11-2015).pdf (24 Кбайт)

We are investigating potentially fraudulent communication claiming to be from USAA
(text, phone call). Rest assured USAA will investigate this matter
immediately and take appropriate action. We are taking steps to shut down phishing
websites used to steal our customers information.
Help Us protect your USAA account from phishing attacks
by downloading and attending to the attachment in this email.

Things to remember:

The main infection modules used by the group are widely used remote access Trojans (RATs): XtremeRAT and PoisonIvy. Their activities are heavily reliant on social engineering. They use filenames related to IT and IR functions and content and domain names that are likely to be of interest to their victims (e.g. '.gov.uae.kim').

Our colleagues also came across a different type of phishing message using Mediabox objects in attached PDF files.



PDF Is Secured

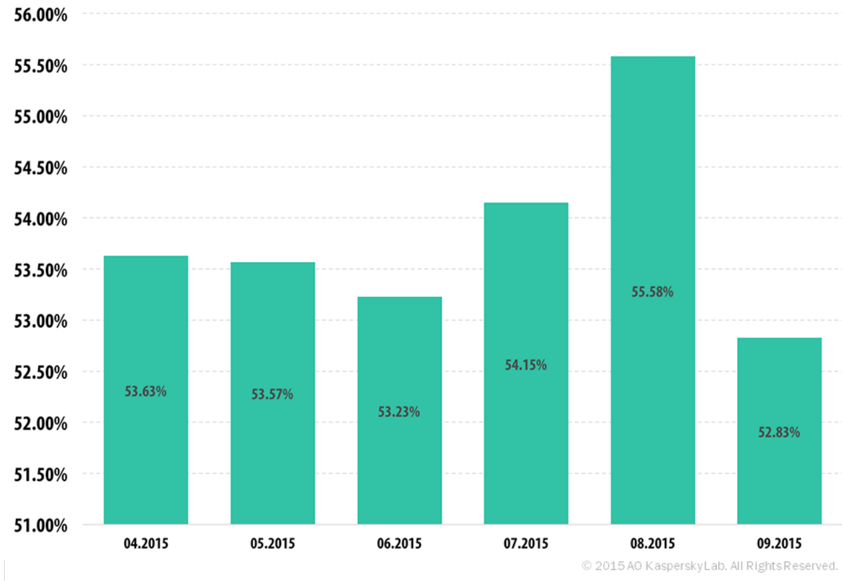
swift.pdf (149.45 kb)

View pdf File

A Mediabox object is a document opened by a mouse click and used to redirect the user to a phishing website.

STATISTICS

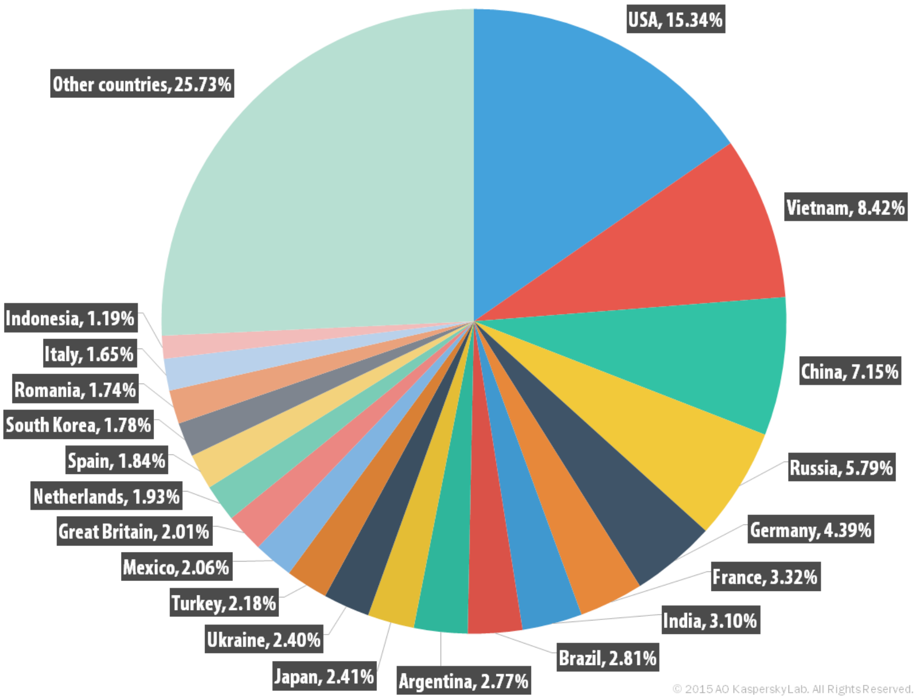
Proportion of spam in email traffic



Percentage of spam in email traffic, April-September 2015

After some relatively stable months in the second quarter the percentage of spam in global email traffic began to change again. A slight growth in July and August of 2015 was followed by a noticeable drop in September. As a result, the average percentage of spam in Q3 amounted to 54.19% – slightly higher than the average for the previous quarter.

Sources of spam by country

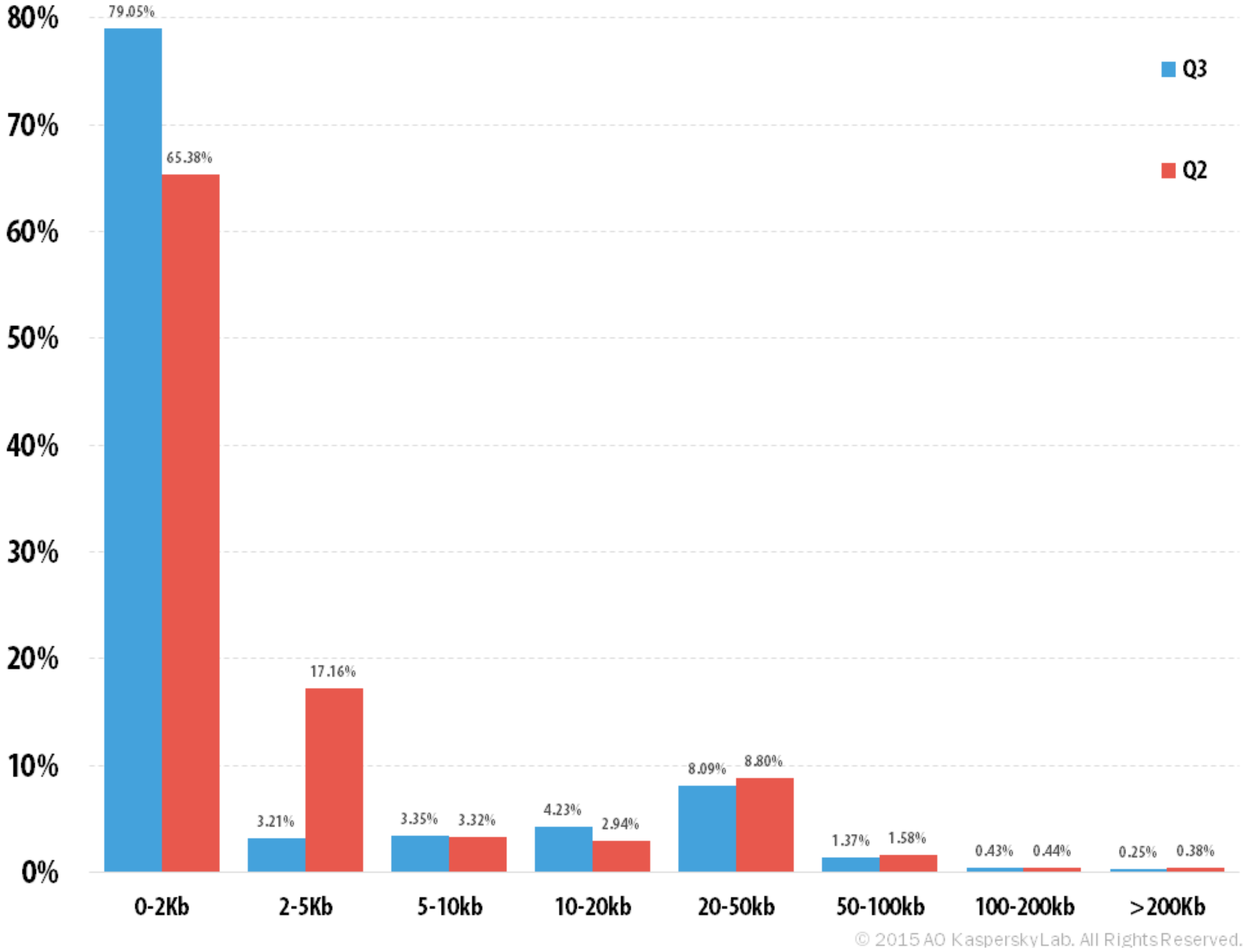


Sources of spam by country, Q3 2015

The US (15.34%) remained the biggest source of spam in Q3. Vietnam was second with 8.42% of global spam, compared to 3.38% in the previous quarter. China rounded off the Top 3 (7.15%) – its share remained unchanged from the previous quarter.

Russia's share (5.79%) dropped by 2.03 p.p., pushing it from second to fourth position. It was followed by Germany (4.39%) and France (3.32%) – their shares changed only slightly compared to Q2.

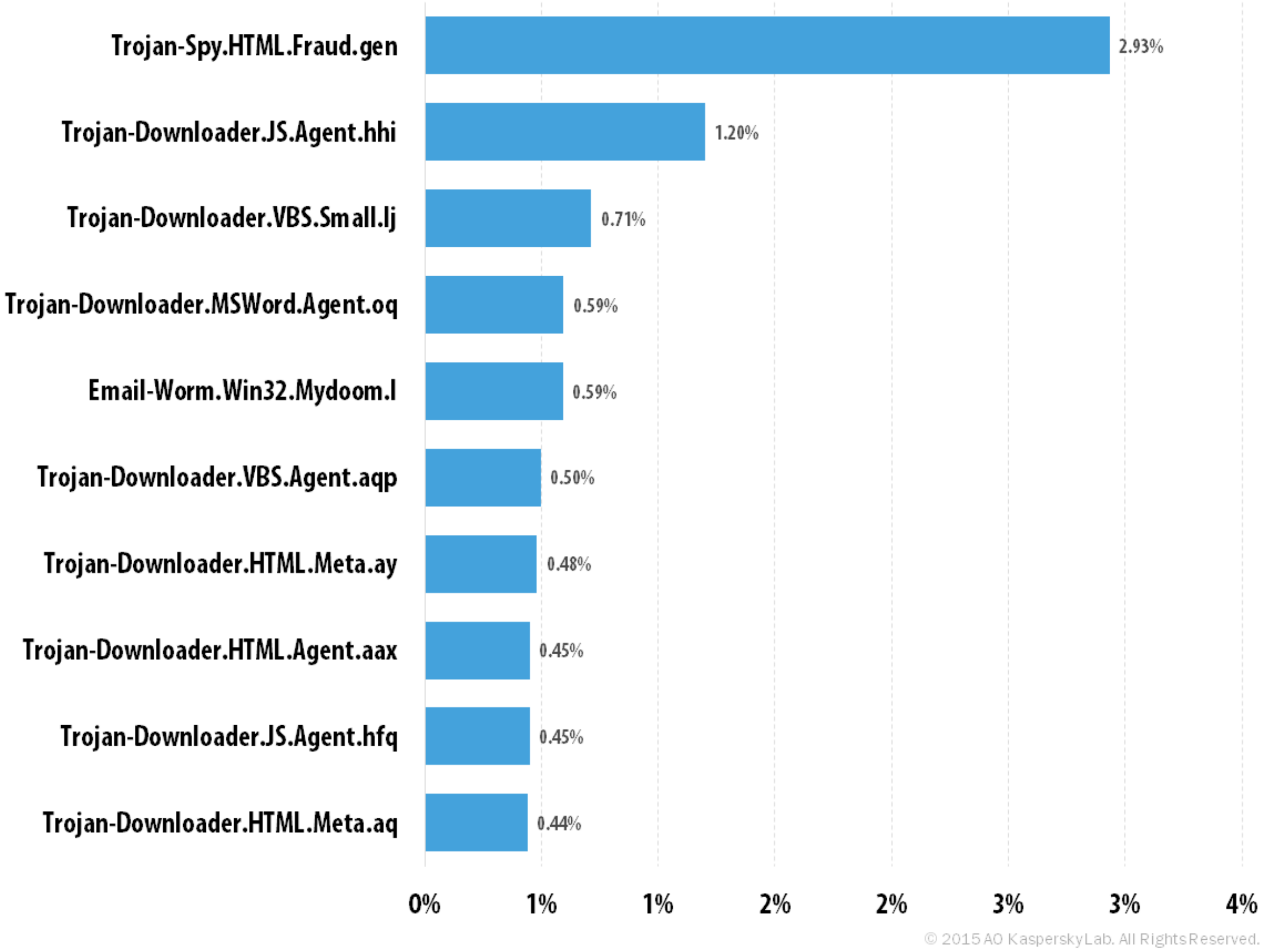
Spam email size



Spam email size distribution, Q2 2015 and Q3 2015

The most commonly distributed emails were very small – up to 2 KB (79.05%). The proportion of these emails grew from the previous quarter (13.67 p.p.), while the share of emails sized 20-50 KB (3.32%) fell by approximately the same number of percentage points. The share of all other emails saw no significant change from Q2 of 2015.

MALICIOUS EMAIL ATTACHMENTS



Top 10 malicious programs sent by email, Q3 2015

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.

Second and ninth places in the Top 10 are occupied by Trojan-Downloader.JS.Agent.hhi and Trojan-Downloader.JS.Agent.hfq, respectively. Both are an obfuscated Java-script. The downloaders use ADODB.Stream technology that allows them to download and run DLL, EXE and PDF files.

Trojan-Downloader.VBS.Small.lj and Trojan-Downloader.VBS.Agent.aqp came third and sixth, respectively. These VBS scripts, which also use the ADODB.Stream technology, download ZIP archives and run malware extracted from them.

Trojan-Downloader.MSWord.Agent.oq came fourth. This malicious program is a DOC file with embedded VBS macros that run when the document is opened. The macros download another malicious VBS script from the cybercriminals' site and run it on the victim's computer.

Email-Worm.Win32.Mydoom.l rounds off the Top 5. This network worm is spread 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. The worm also enables attackers to remotely control the infected computer.

Trojan-Downloader.HTML.Meta.ay, Trojan-Downloader.HTML.Agent.aax and Trojan-Downloader.HTML.Meta.aq were seventh, eighth and tenth in the rating, respectively. They all are HTML pages which, when opened, redirect users to a rigged site. Once there, a victim usually encounters a phishing page or is asked to download a program – Binbot, a binary option trading bot. The three malicious programs spread via email attachments and the only difference between them is the link which redirects users to the rigged sites.

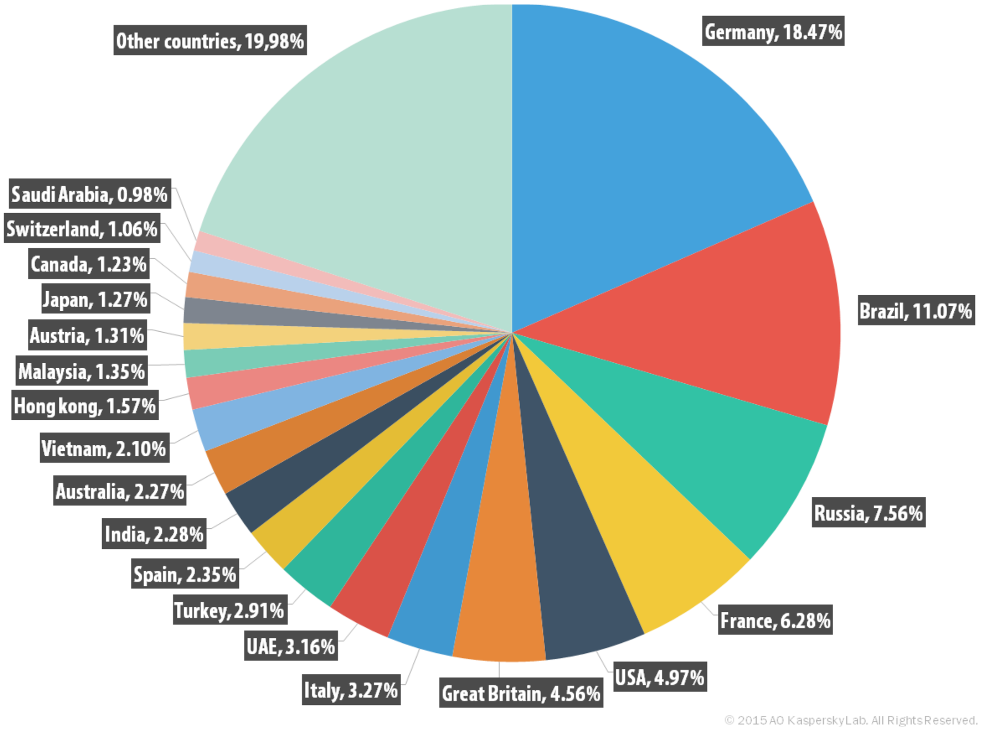
Malware families

As in the previous two quarters, Upatre (9.46%) was the most common malware family. Malware from this family downloads the Trojan banker known as Dyre, Dyreza, Dyzap.

The MSWord.Agent family (5.55%) remained in second position. 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 malicious programs from the Andromeda family.

In third place was the VBS.Agent (5.44%) family. Unlike MSWord.Agent, the malicious programs of this family use the embedded VBS script. To download and run other malware on the user's computer they use the ADODB.Stream technology.

Countries targeted by malicious mailshots



Distribution of email antivirus verdicts by country, Q3 2015

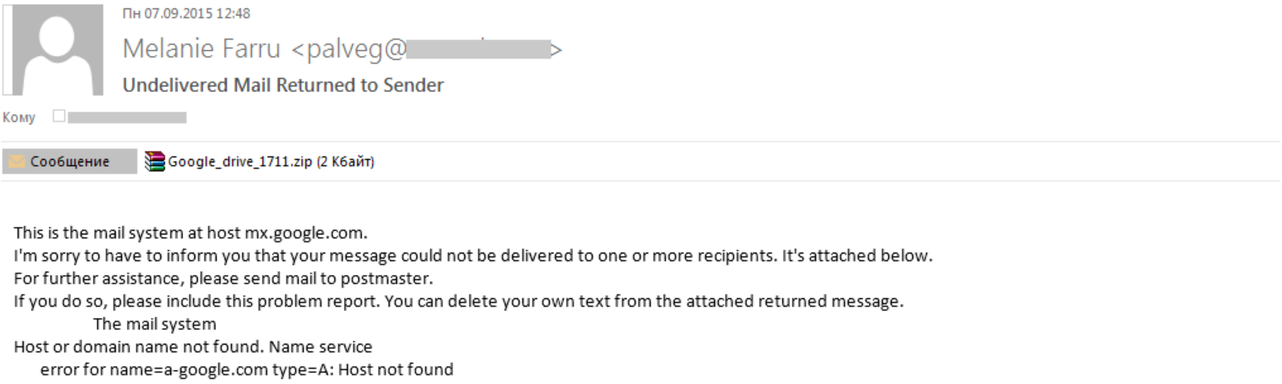
There were some significant changes in the Top 3 countries targeted most often by mailshots in Q3 2015. Russia's appearance in third place (7.56%) was the biggest surprise: its share grew by 2.82 p.p., pushing it up two places from fifth.

Germany (18.47%) remained on top, although its contribution dropped by 1.12 p.p. compared to Q2. Brazil ended the quarter in second place (11.7%) – the amount of malicious spam originating from there almost doubled compared to Q2.

The UK (4.56%), which was second in Q2, ended Q3 in sixth place.

Special features of malicious spam

In spam traffic at the beginning of September we came across a large-scale malicious mass mailing containing emails imitating a non-delivery auto-reply sent by an email server. The text and subject of the message looked very similar to an automatic notification; however, the sender address belonged to an individual, which raised doubts about the legitimacy of the email. The attached ZIP archive named Google_drive_1711 was also suspicious because notifications from email services do not normally contain attachments. Closer inspection revealed that the archive included Trojan Trojan-Downloader.JS.Agent.hhi, which in turn downloaded Backdoor.Win32.Androm.



Пн 07.09.2015 12:48

Melanie Farru <palveg@[redacted]>

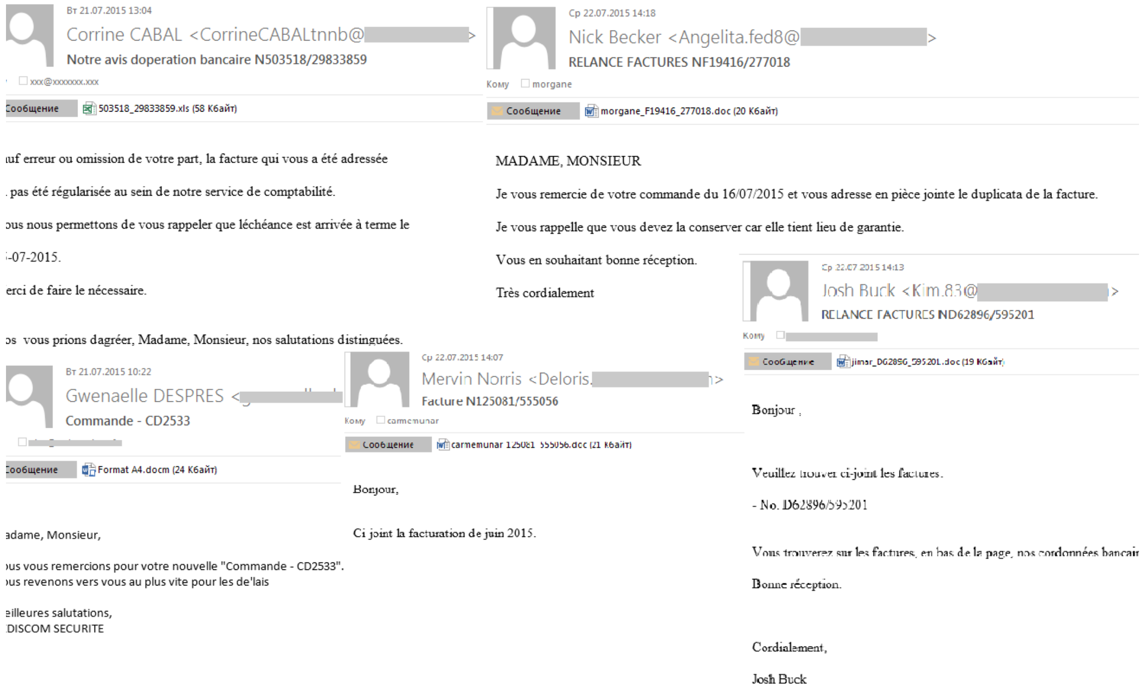
Undelivered Mail Returned to Sender

Кому □ [redacted]

Google_drive_1711.zip (2 Кбайт)

This is the mail system at host mx.google.com.
I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.
For further assistance, please send mail to postmaster.
If you do so, please include this problem report. You can delete your own text from the attached returned message.
The mail system
Host or domain name not found. Name service
error for name=a-google.com type=A: Host not found

At the beginning of the third quarter cybercriminals were actively sending out emails in French containing macro viruses. The macros that we detected belonged to a category of Trojan downloaders and were used to download and install the banking Trojan Dridex on victim computers. To deceive the recipient, the fraudsters imitated a notification about the receipt of an order or an invoice.



Вт 21.07.2015 13:04

Corrine CABAL <CorrineCABALtnnb@[redacted]>

Notre avis doperation bancaire N503518/29833859

□ xxx@xxxxxxx.xxx

503518_29833859.xls (58 Кбайт)

ıuf erreur ou omission de votre part, la facture qui vous a été adressée

. pas été régularisée au sein de notre service de comptabilité.

ɔus nous permettons de vous rappeler que léchéance est arrivée à terme le

-07-2015.

erci de faire le nécessaire.

ɔs vous prions dagréer, Madame, Monsieur, nos salutations distinguées.

Ср 22.07.2015 14:18

Nick Becker <Angelita.fed8@[redacted]>

RELANCE FACTURES NF19416/277018

Кому □ morgane

morgane_F19416_277018.doc (20 Кбайт)

MADAME, MONSIEUR

Je vous remercie de votre commande du 16/07/2015 et vous adresse en pièce jointe le duplicata de la facture.

Je vous rappelle que vous devez la conserver car elle tient lieu de garantie.

Vous en souhaitant bonne réception.

Très cordialement

Вт 21.07.2015 10:22

Gwenaelle DESPRES <[redacted]

Commande - CD2533

□ [redacted]

Format A4.docm (24 Кбайт)

adame, Monsieur,

ɔus vous remercions pour votre nouvelle "Commande - CD2533".
ɔus revenons vers vous au plus vite pour les de'lais

eilleures salutations,
DISCOM SECURITE

Ср 22.07.2015 14:07

Mervin Norris <Deloris.[redacted]n>

Facture N125081/555056

Кому □ carmemunar

carmemunar 125081 555056.dcc (21 Кбайт)

Bonjour,

Ci joint la facturation de juin 2015.

Ср 22.07.2015 14:13

Josh Buck <Kim.83@[redacted]>

RELANCE FACTURES ND62896/595201

Кому □ [redacted]

jimar_D62896_595201.doc (19 Кбайт)

Bonjour ,

Veuillez trouver ci-joint les factures.

- No. D62896/595201

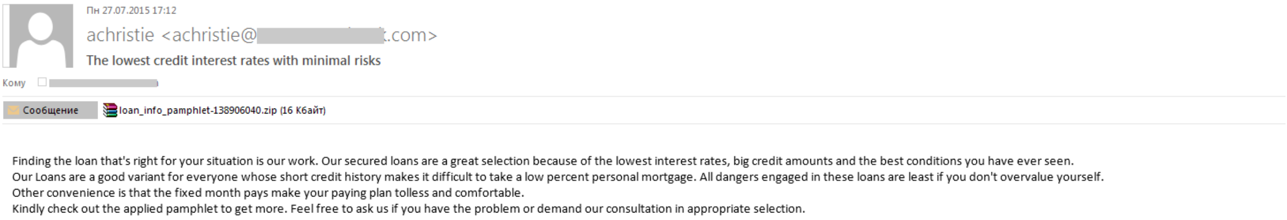
Vous trouverez sur les factures, en bas de la page, nos cordonnées bancair

Bonne réception.

Cordialement,

Josh Buck

In July, spammers exploited the theme of loans to spread malicious files that are now traditional for advertising spam. Some scammer emails offered a loan attracting potential customers with very favorable terms, low interest rates, etc. Other messages notified the recipient that his loan application had been approved. Interestingly, this content can also be seen in ordinary advertising spam, but malicious spam usually contains an attachment masquerading as detailed information about the loan.



Пн 27.07.2015 17:12

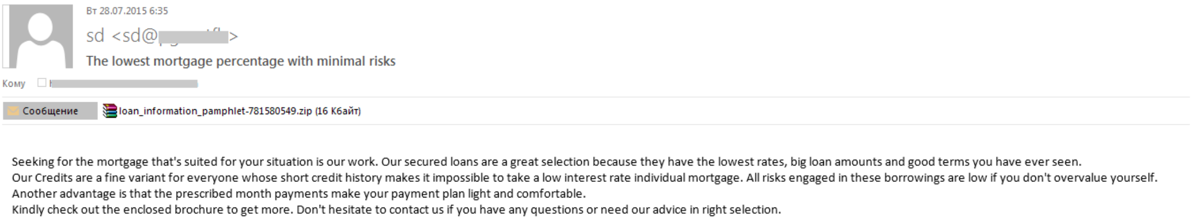
achristie <achristie@[redacted].com>

The lowest credit interest rates with minimal risks

Кому [redacted]

Сообщение loan_info_pamphlet-138906040.zip (16 Кбайт)

Finding the loan that's right for your situation is our work. Our secured loans are a great selection because of the lowest interest rates, big credit amounts and the best conditions you have ever seen.
Our Loans are a good variant for everyone whose short credit history makes it difficult to take a low percent personal mortgage. All dangers engaged in these loans are least if you don't overvalue yourself.
Other convenience is that the fixed month pays make your paying plan tolless and comfortable.
Kindly check out the applied pamphlet to get more. Feel free to ask us if you have the problem or demand our consultation in appropriate selection.



Вт 28.07.2015 6:35

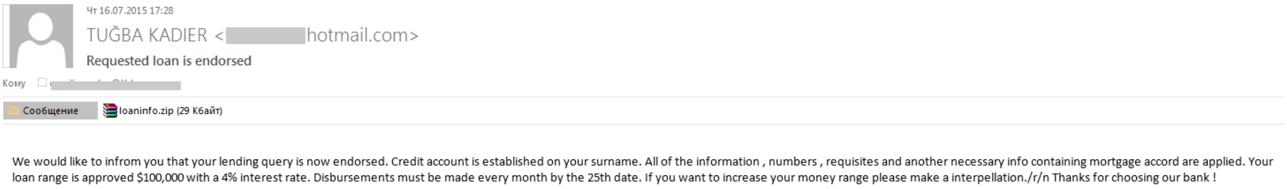
sd <sd@[redacted]>

The lowest mortgage percentage with minimal risks

Кому [redacted]

Сообщение loan_information_pamphlet-781580549.zip (16 Кбайт)

Seeking for the mortgage that's suited for your situation is our work. Our secured loans are a great selection because they have the lowest rates, big loan amounts and good terms you have ever seen.
Our Credits are a fine variant for everyone whose short credit history makes it impossible to take a low interest rate individual mortgage. All risks engaged in these borrowings are low if you don't overvalue yourself.
Another advantage is that the prescribed month payments make your payment plan light and comfortable.
Kindly check out the enclosed brochure to get more. Don't hesitate to contact us if you have any questions or need our advice in right selection.



Чт 16.07.2015 17:28

TUĞBA KADIER <[redacted]hotmail.com>

Requested loan is endorsed

Кому [redacted]

Сообщение loaninfo.zip (29 Кбайт)

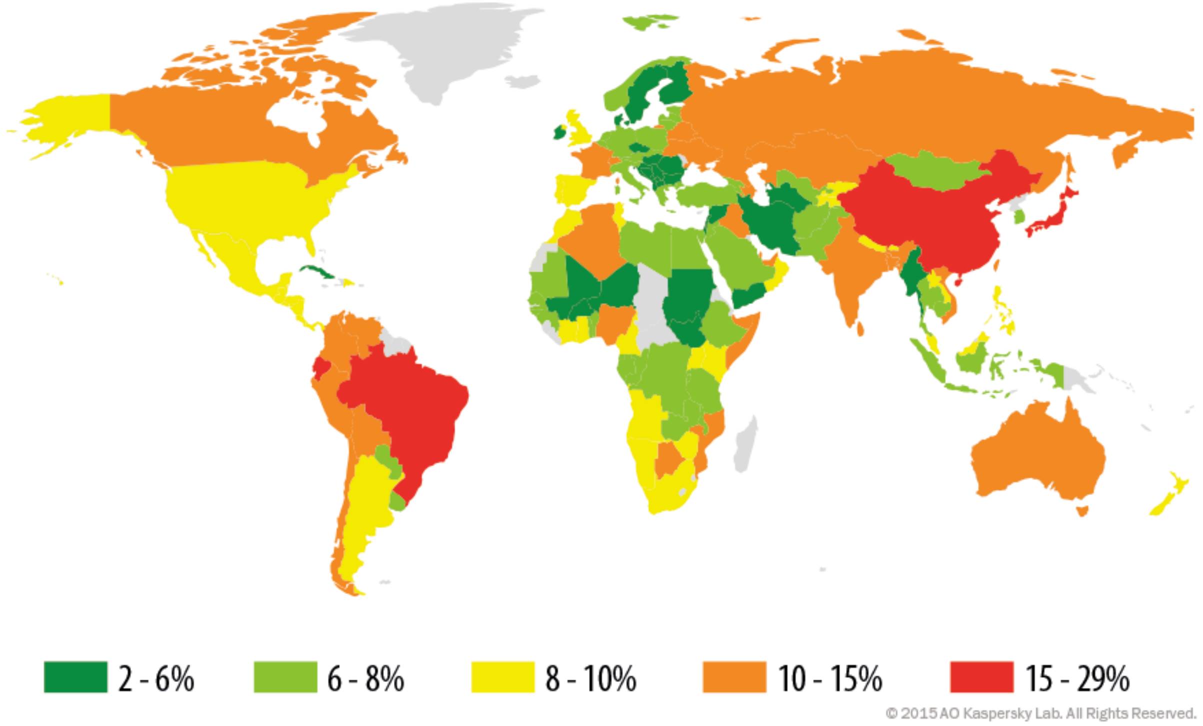
We would like to infrom you that your lending query is now endorsed. Credit account is established on your surname. All of the information , numbers , requisites and another necessary info containing mortgage accord are applied. Your loan range is approved $100,000 with a 4% interest rate. Disbursements must be made every month by the 25th date. If you want to increase your money range please make a interpellation./r/n Thanks for choosing our bank !

Interestingly, malicious emails with Trojan-Downloader.Win32.Upatre in the attachment were sent to employees at different companies.

PHISHING

In Q3 2015, the Anti-Phishing system was triggered 36,300,537 times on computers of Kaspersky Lab users, which is 6 million times more than the previous quarter. Of them, 15,764,588 attempts were blocked by our heuristic detection components and 20,535,949 by signature detection components. 839,672 phishing wildcards were added to the Kaspersky Lab databases.

The country where the largest percentage of users is affected by phishing attacks was once again Brazil (21.7%). In Q3 2015, the share of those attacked increased by 11.33 p.p., meaning Brazil returned to the same sort of figures last seen in Q1.



Geography of phishing attacks, Q3 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 Japan and China also grew considerably (+10.9 p.p. and +7.85 p.p., respectively), which saw these countries ranked second and third in the rating.

Top 10 countries by percentage of users attacked:

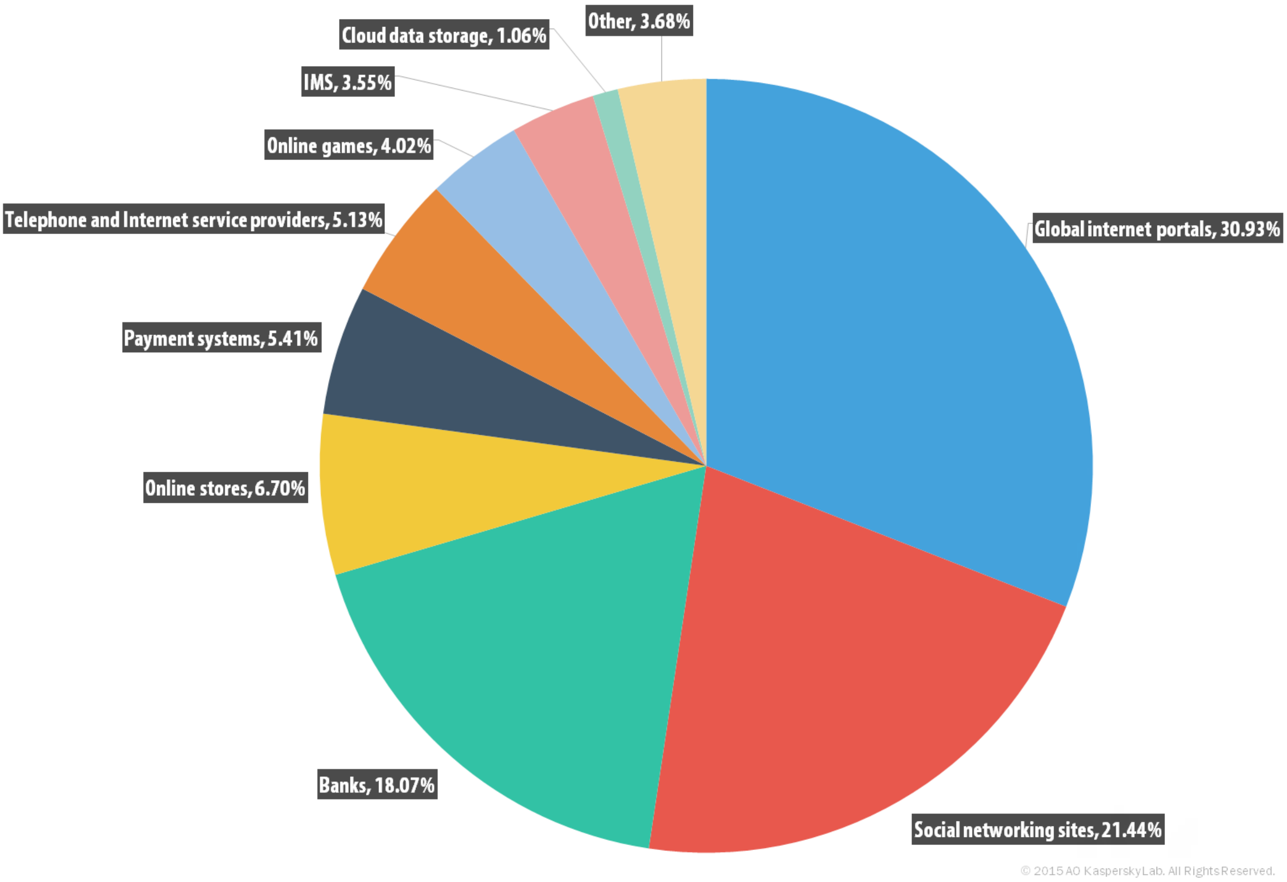
	Country	% of users
1	Brazil	21.07
2	Japan	16.86
3	China	15.08
4	Vietnam	14.50
5	Bangladesh	13.32

6	Nigeria	13.05
7	Russia	12.91
8	Kazakhstan	12,85
9	India	12.44
10	Columbia	12.25

Organizations under attack

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

In the third quarter of 2015, the 'Global Internet portals' category (30.93%) topped the rating of organizations attacked by phishers although its share decreased by 11.42 p.p. from the previous quarter. The share of 'Social networking sites' (21.44%) increased by 6.69 p.p. In third place came 'Banks' with 18.07% (+4.65 p.p.). The 'Online games' category also increased by half and accounted for 4.02%.



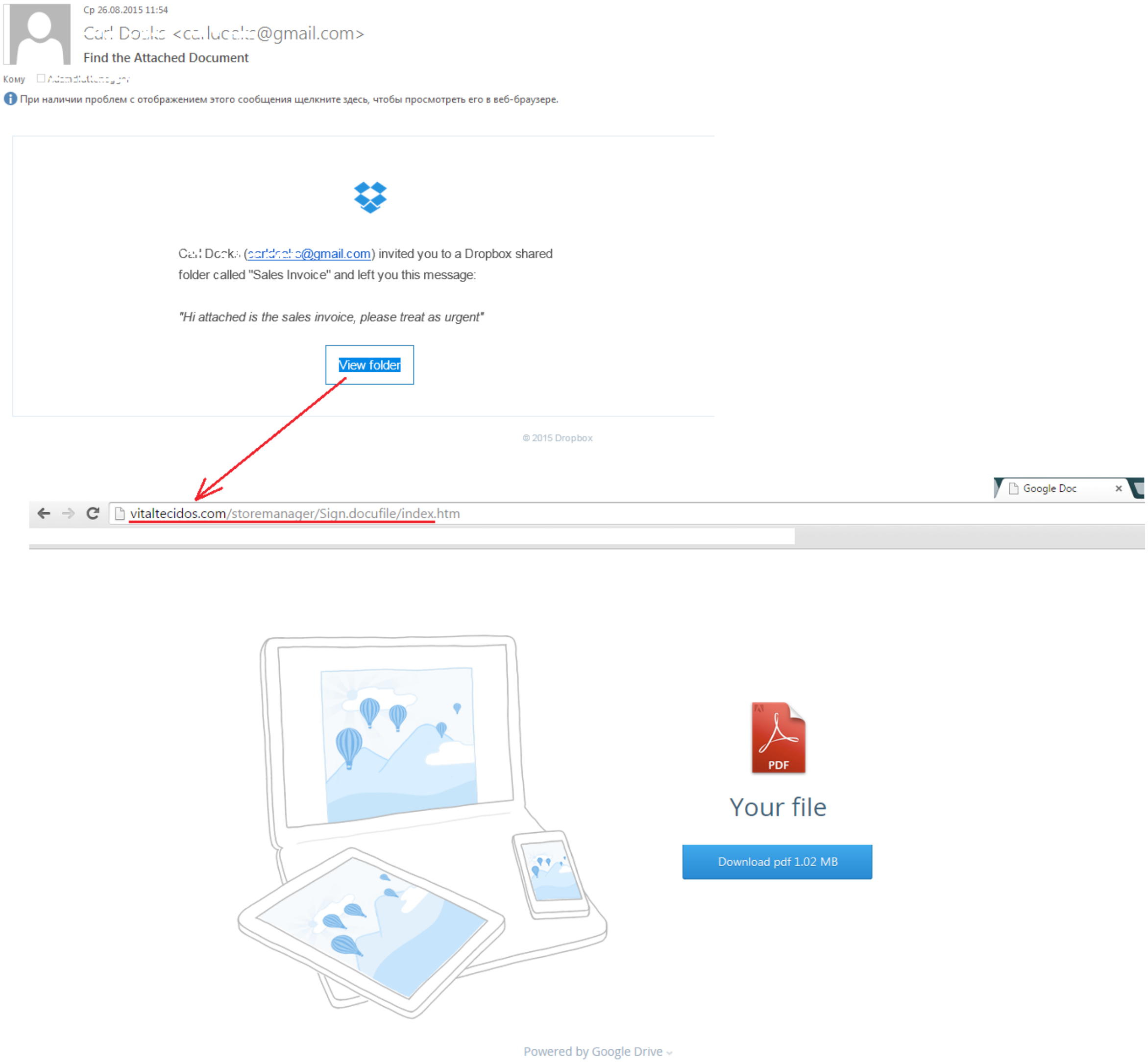
Distribution of organizations affected by phishing attacks, by category, Q3 2015

The proportion of phishing attacks on organizations in the ‘Cloud data storage’ category increased by 0.26 p.p. and amounted to 1.06%. Users are increasingly using cloud storage technology, thus attracting the attention of cybercriminals. The stolen information is used for blackmail, sold to third parties or used in targeted attacks.

This type of phishing is often distributed via email or social networks in the form of a message inviting users to download a document allegedly uploaded to a popular cloud service. Messages can arrive from a compromised account from a user’s friend list or, in the case of email, on behalf of a cloud service administrator.

Phishing pages imitating well-known cloud storage sites are used to distribute various malicious programs. In such cases, a user automatically downloads a malicious program to his computer by clicking the link on the page.

Below is an example of an attack where the user is asked to download an important PDF document. The link in the email leads to a phishing page imitating the site of the popular cloud service Dropbox.



Ср 26.08.2015 11:54

[redacted] <[redacted]@gmail.com>

Find the Attached Document

Кому □ [redacted]

При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.

[redacted] ([redacted]@gmail.com) invited you to a Dropbox shared folder called "Sales Invoice" and left you this message:

"Hi attached is the sales invoice, please treat as urgent"

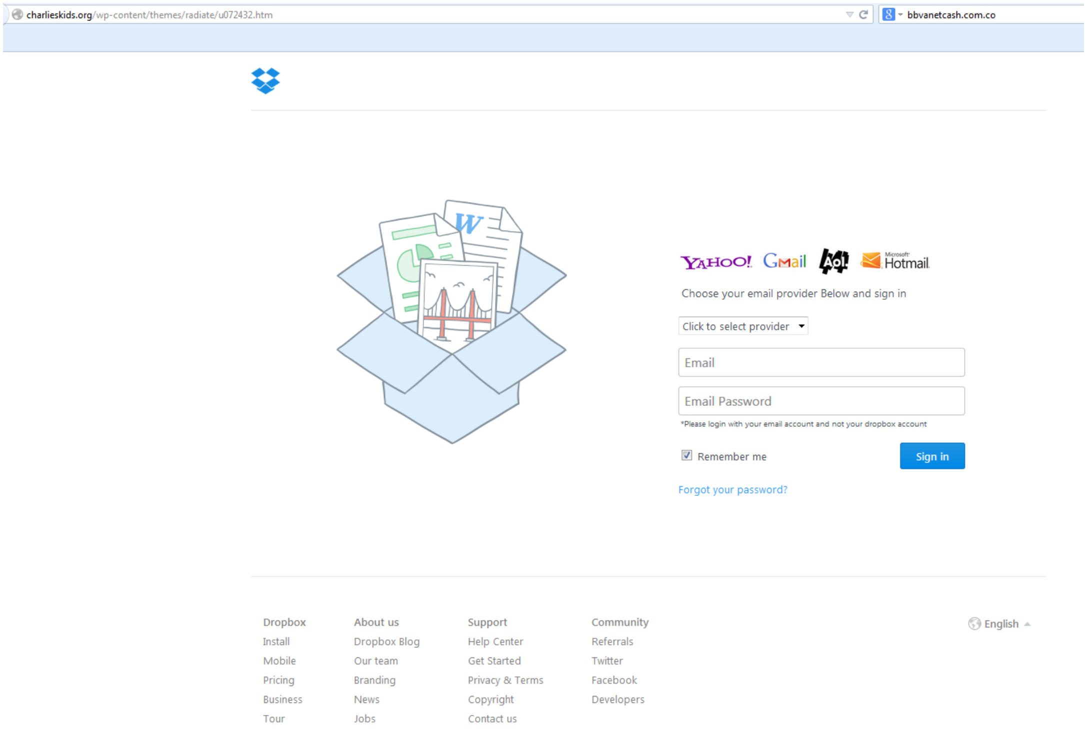
View folder

© 2015 Dropbox

vitaltecidos.com/storemanager/Sign.docufile/index.htm

Example of a phishing attack targeting users of Dropbox

In addition to stealing data stored in the cloud and spreading malware, cybercriminals often use the Dropbox name to steal the victim’s email account data.



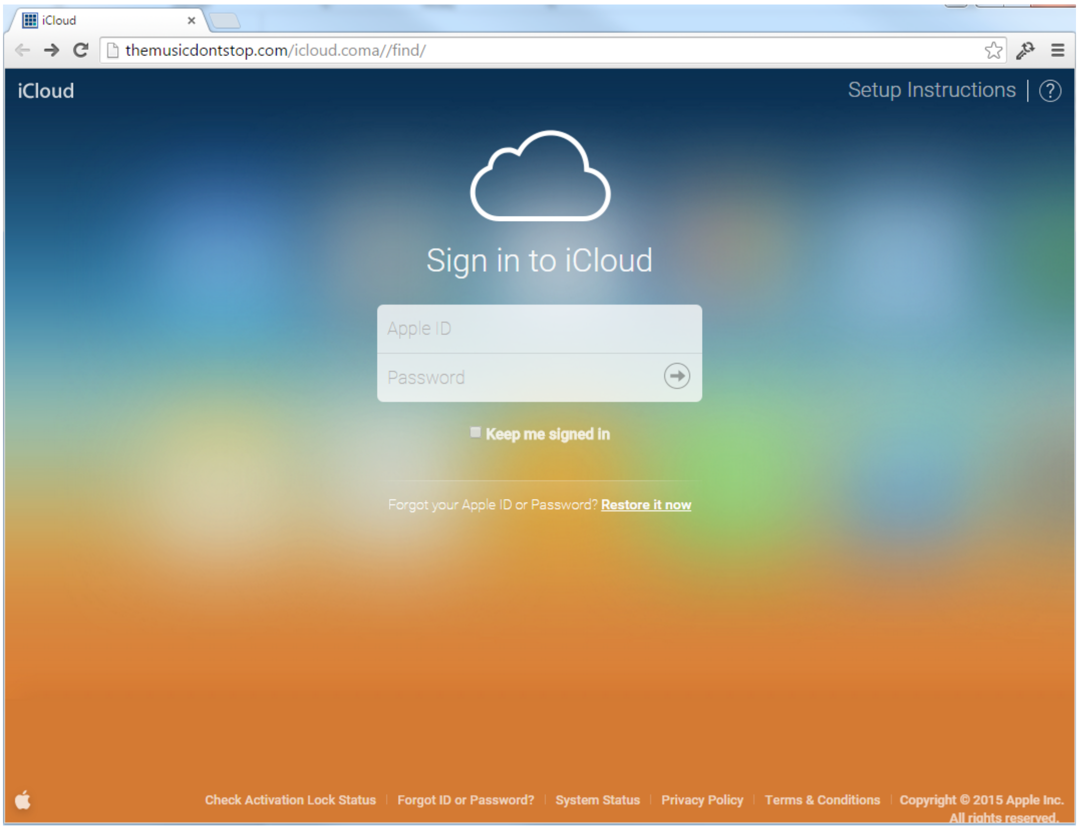
charlieskids.org/wp-content/themes/radiate/u072432.htm

Choose your email provider Below and sign in

*Please login with your email account and not your dropbox account

Example of a phishing page using the Dropbox brand

Here is yet another example of phishing, with the scammers trying to steal the user's AppleID and password for iCloud.



themusicdontstop.com/icloud.coma//find/

Forgot your Apple ID or Password? Restore it now

iCloud
Setup Instructions | ?
Sign in to iCloud
Apple ID
Password
Keep me signed in
Check Activation Lock Status | Forgot ID or Password? | System Status | Privacy Policy | Terms & Conditions | Copyright © 2015 Apple Inc. All rights reserved.

Example of a phishing attack on iCloud users

Among other things, if successful, the attackers gain access to any content purchased by the user as well as his email account.

Top 3 organizations attacked

Fraudsters continue to focus the greatest part of their non-spear phishing attacks on the most popular brands. In this way they are trying to increase the chances of success for their latest phishing attack. In more than half of cases the heuristic component of Anti-Phishing is triggered when a user follows a link to phishing pages hiding behind the names of more than 30 well-known companies.

The Top 3 organizations most often attacked by phishers account for 26.39% of all phishing links detected in Q3 2015.

	Organization	% of all detected phishing links
1	Yahoo!	15.38
2	VKontakte	9.44
3	Facebook	8.95

In Q3 2015, the leading three organizations targeted by phishers saw a few changes. Yahoo! remained top with 15.38%, although its share almost halved (-13.65 p.p.). The Russian social networking site VKontakte (9.44%) came second. Facebook (8.95%) fell by 1.49 p.p. and moved from second to third place.

CONCLUSION

In Q3 of 2015, the percentage of spam in email traffic accounted for 54.2%, a 0.8 p.p. drop from the previous quarter. The Top 3 biggest sources of spam distributed worldwide were: the US (15.3%), Vietnam (8.4%) and China (7.2%).

The holiday season saw an increase in tourism-related malicious spam. Cybercriminals sent out fake notifications from well-known booking services, airlines and hotels, as well as emails from individuals. They typically included attached archives with different Trojan downloaders.

Trojan-Spy.HTML.Fraud.gen remained the most popular malicious program sent by email. As in the previous two quarters, the rating of the most popular malware families was topped by Upatre. Germany topped the ranking of countries whose users were most often targeted by mailshots – 18.5% of antivirus detections were registered there.

A particular feature of Q3 was a new trick used in phishing emails – in order to bypass spam filters they placed the text of the email and fraudulent link in an attached PDF document rather than in the message body.

In Q3, Kaspersky Lab solutions blocked more than 36 million attempts to follow links to phishing pages, which is 6 million more than in the previous quarter. The country where the largest percentage of users is affected by phishing attacks was once again Brazil (21.7%).

About Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997 Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

Learn more at www.kaspersky.com.

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

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

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