KASPERSKY SECURITY BULLETIN. SPAM EVOLUTION 2013

Darya Gudkova

Contents

THE YEAR IN FIGURES 3

ADVERTS FOR LEGITIMATE GOODS AND SERVICES MIGRATE FROM SPAM 4

> Criminalization of commercial spam 4

> 'Gray' mailings 7

TREND OF 2013: FAKE MESSAGES FROM ANTIVIRUS VENDORS 8

WORLD EVENTS IN SPAM 10

STATISTICS 11

> The percentage of spam in email traffic 11

> Sources of spam by country 12

> Sources of spam by region 14

> The size of spam emails 15

MALICIOUS ATTACHMENTS IN EMAIL 16

PHISHING 20

CONCLUSION AND FORECASTS 22

Spam evolution 2013

1 The year in figures

- The proportion of spam in email flows was 69.6% in 2013, which is 2.5 percentage points lower than in 2012
- The percentage of emails with malicious attachments was 3.2%, which is 0.2 percentage points lower than in 2012
- 32.1% of phishing attacks targeted social networks
- The greatest amount of spam – 23% – was sent from China
- 74.5% of spam emails sent in 2013 were no more than 1 KB in size

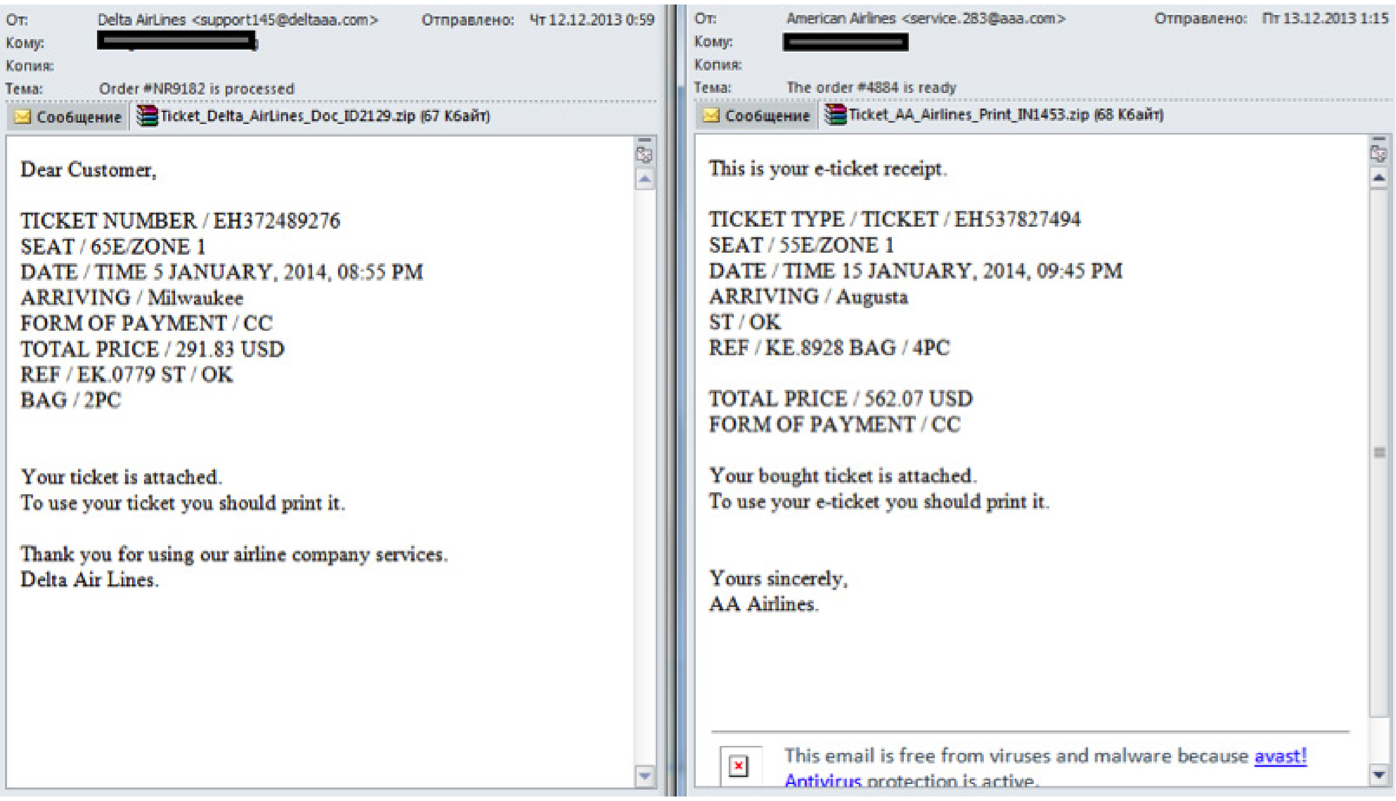
2 Adverts for legitimate goods and services migrate from spam

Criminalization of commercial spam

As we wrote last year, the amount of spam advertising legitimate goods and services is gradually decreasing. Advertisers increasingly prefer legitimate advertising to spam: more varied types of online advertising are becoming available, and these generate higher response rates at lower costs than spam can offer.

At the same time, in some spam categories commercial advertising is being gradually displaced by criminal mailings. A typical example is the Travel and Tourism category. This category used to account for 5 to 10 percent of all spam traffic and was made up entirely of various offers for trips, tours and tickets. These days, commercial advertising in spam is rare, but we see numerous malicious emails exploiting the subject of travel and leisure.

Fake confirmations of hotel or airplane ticket reservations have become a common part of spam; we saw such messages in spam traffic throughout the year. Instead of booking confirmations, files attached to such messages include malware (e.g., Trojan-PSW.Win32.Tepfer or Backdoor.Win32.Androm.qt).



От: Delta AirLines <support145@deltaaa.com> Отправлено: Чт 12.12.2013 0:59
Кому: [redacted]
Копия:
Тема: Order #NR9182 is processed

Ticket_Delta_AirLines_Doc_ID2129.zip (67 Кбайт)

Dear Customer,

TICKET NUMBER / EH372489276
SEAT / 65E/ZONE 1
DATE / TIME 5 JANUARY, 2014, 08:55 PM
ARRIVING / Milwaukee
FORM OF PAYMENT / CC
TOTAL PRICE / 291.83 USD
REF / EK.0779 ST / OK
BAG / 2PC

Your ticket is attached.
To use your ticket you should print it.

Thank you for using our airline company services.
Delta Air Lines.

От: American Airlines <service.283@aaa.com> Отправлено: Пт 13.12.2013 1:15
Кому: [redacted]
Копия:
Тема: The order #4884 is ready

Ticket_AA_Airlines_Print_IN1453.zip (68 Кбайт)

This is your e-ticket receipt.

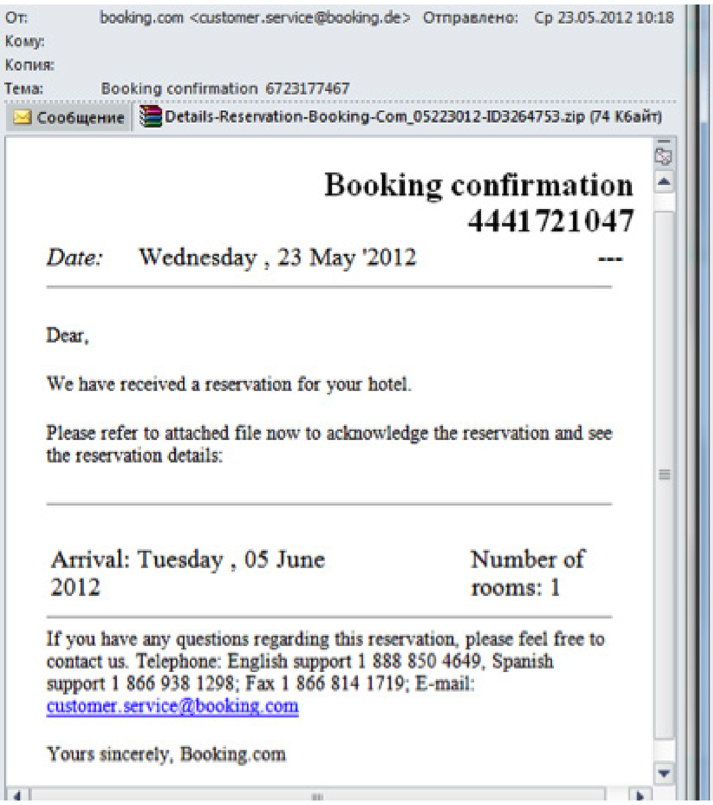
TICKET TYPE / TICKET / EH537827494
SEAT / 55E/ZONE 1
DATE / TIME 15 JANUARY, 2014, 09:45 PM
ARRIVING / Augusta
ST / OK
REF / KE.8928 BAG / 4PC

TOTAL PRICE / 562.07 USD
FORM OF PAYMENT / CC

Your bought ticket is attached.
To use your e-ticket you should print it.

Yours sincerely,
AA Airlines.

This email is free from viruses and malware because avast! Antivirus protection is active.



От: booking.com <customer.service@booking.de> Отправлено: Ср 23.05.2012 10:18
Кому:
Копия:
Тема: Booking confirmation 6723177467

Сообщение | Details-Reservation-Booking-Com_05223012-ID3264753.zip (74 Кбайт)

Booking confirmation
4441721047

Date: Wednesday , 23 May '2012 ---

Dear,

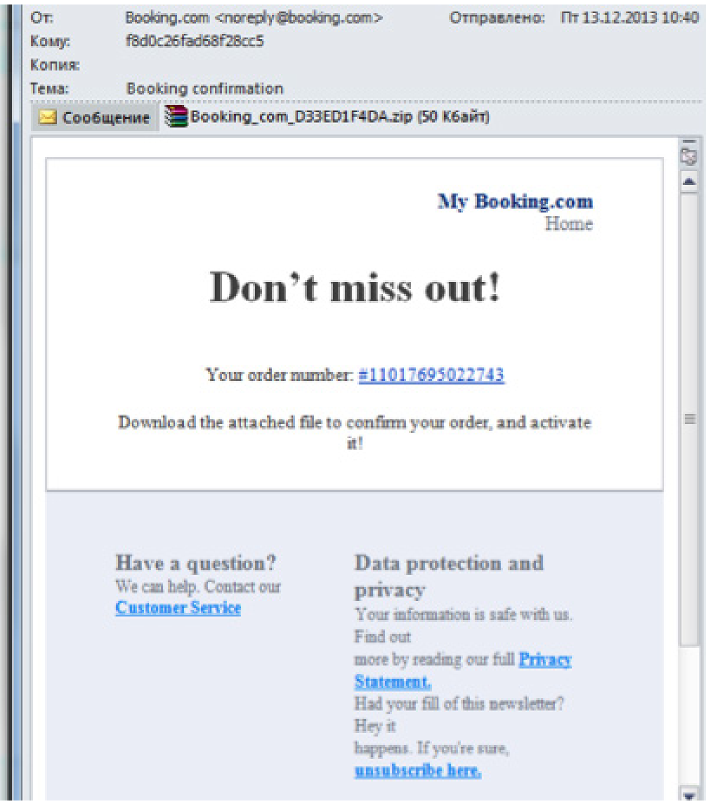
We have received a reservation for your hotel.

Please refer to attached file now to acknowledge the reservation and see the reservation details:

Arrival: Tuesday , 05 June 2012 | Number of rooms: 1

If you have any questions regarding this reservation, please feel free to contact us. Telephone: English support 1 888 850 4649, Spanish support 1 866 938 1298; Fax 1 866 814 1719; E-mail: customer.service@booking.com

Yours sincerely, Booking.com



От: Booking.com <noreply@booking.com> Отправлено: Пт 13.12.2013 10:40
Кому: f8d0c26fad68f28cc5
Копия:
Тема: Booking confirmation

Сообщение | Booking_com_D33ED1F4DA.zip (50 Кбайт)

My Booking.com
Home

Don't miss out!

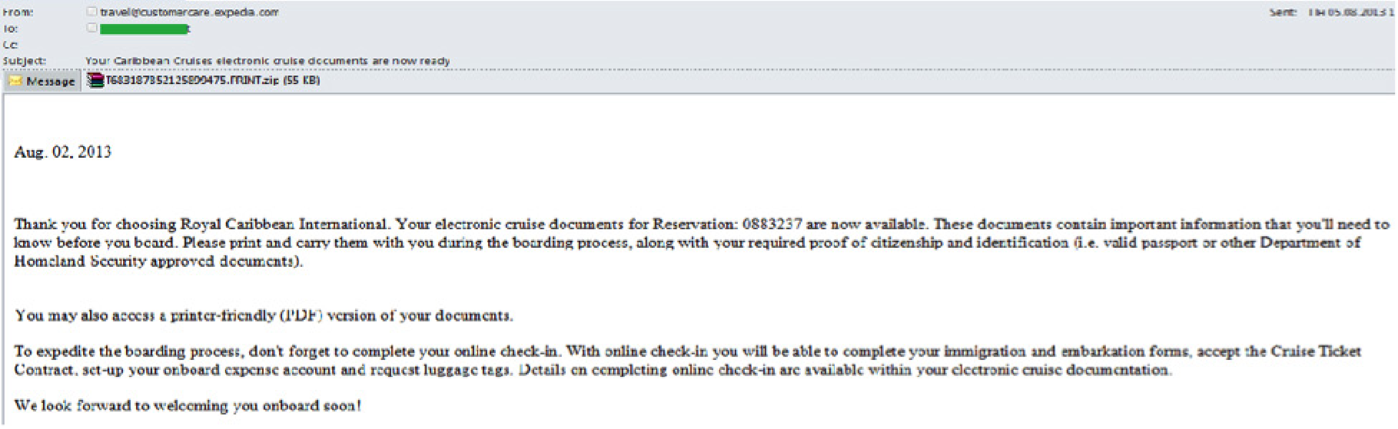
Your order number: #11017695022743

Download the attached file to confirm your order, and activate it!

Have a question?
We can help. Contact our Customer Service

Data protection and privacy
Your information is safe with us. Find out more by reading our full Privacy Statement.
Had your fill of this newsletter? Hey it happens. If you're sure, unsubscribe here.

In 2013, spammers sent false cruise booking confirmations in addition to the usual emails imitating ticket or hotel booking confirmations.



From: travel@customercare.expedia.com Sent: Thu 05.08.2013 1
To: [redacted]
Cc:
Subject: Your Caribbean Cruises electronic cruise documents are now ready

Message | T683187352125809475.PRINT.zip (55 KB)

Aug. 02, 2013

Thank you for choosing Royal Caribbean International. Your electronic cruise documents for Reservation: 0883237 are now available. These documents contain important information that you'll need to know before you board. Please print and carry them with you during the boarding process, along with your required proof of citizenship and identification (i.e. valid passport or other Department of Homeland Security approved documents).

You may also access a printer-friendly (PDF) version of your documents.

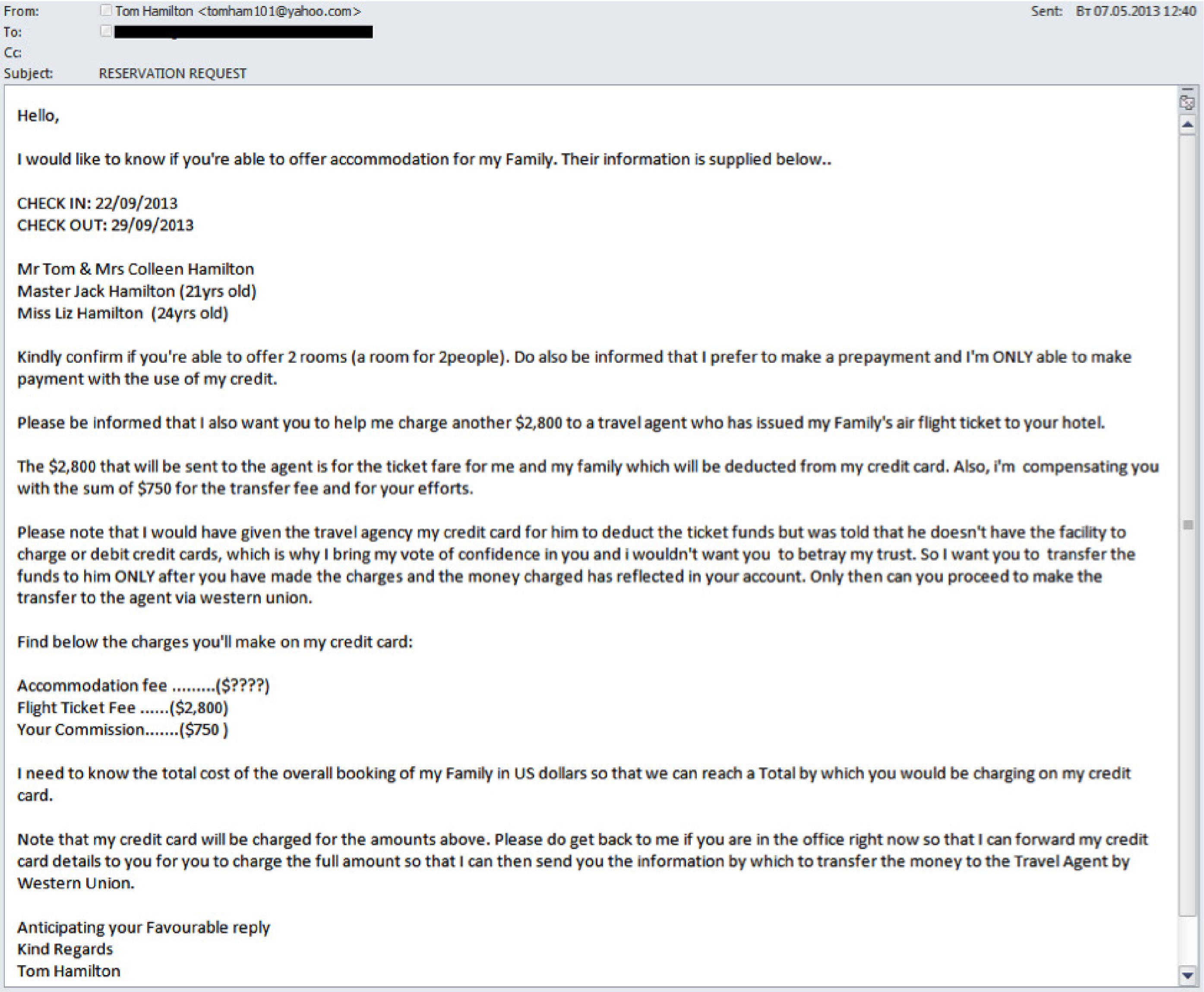
To expedite the boarding process, don't forget to complete your online check-in. With online check-in you will be able to complete your immigration and embarkation forms, accept the Cruise Ticket Contract, set-up your onboard expense account and request luggage tags. Details on completing online check-in are available within your electronic cruise documentation.

We look forward to welcoming you onboard soon!

These emails are similar to fake ticket and hotel booking confirmations: they are impersonal, they include a message about reservations that people have supposedly made and attachments containing malware.

In other words, while a couple of years ago spam might help people to book a tour package, ticket or hotel room, today's spam email will more likely than not offer the recipient malware rather than an ad for a tour company.
The subject of traveling is now attracting fraudsters as well as malware distributors. In 2013,

we detected several mailings in which this spam category is used to launder money from stolen credit cards. Spam messages, which were sent in the hope that some of them would be received by hotels, contained room booking requests.



From: Tom Hamilton <tomham101@yahoo.com>
Sent: Вт 07.05.2013 12:40
To: [redacted]
Cc:
Subject: RESERVATION REQUEST

Hello,

I would like to know if you're able to offer accommodation for my Family. Their information is supplied below..

CHECK IN: 22/09/2013
CHECK OUT: 29/09/2013

Mr Tom & Mrs Colleen Hamilton
Master Jack Hamilton (21yrs old)
Miss Liz Hamilton (24yrs old)

Kindly confirm if you're able to offer 2 rooms (a room for 2people). Do also be informed that I prefer to make a prepayment and I'm ONLY able to make payment with the use of my credit.

Please be informed that I also want you to help me charge another $2,800 to a travel agent who has issued my Family's air flight ticket to your hotel.

The $2,800 that will be sent to the agent is for the ticket fare for me and my family which will be deducted from my credit card. Also, i'm compensating you with the sum of $750 for the transfer fee and for your efforts.

Please note that I would have given the travel agency my credit card for him to deduct the ticket funds but was told that he doesn't have the facility to charge or debit credit cards, which is why I bring my vote of confidence in you and i wouldn't want you to betray my trust. So I want you to transfer the funds to him ONLY after you have made the charges and the money charged has reflected in your account. Only then can you proceed to make the transfer to the agent via western union.

Find below the charges you'll make on my credit card:

Accommodation fee ....($????)
Flight Ticket Fee ......($2,800)
Your Commission.......($750)

I need to know the total cost of the overall booking of my Family in US dollars so that we can reach a Total by which you would be charging on my credit card.

Note that my credit card will be charged for the amounts above. Please do get back to me if you are in the office right now so that I can forward my credit card details to you for you to charge the full amount so that I can then send you the information by which to transfer the money to the Travel Agent by Western Union.

Anticipating your Favourable reply
Kind Regards
Tom Hamilton

If a hotel employee responded to the message, spammers requested that the hotel withdraw an amount significantly exceeding the reservation fees (sometimes the request was made in the original message). The fraudsters requested that this amount be sent to them via Western Union, explaining that this sum was owed to the travel agent organizing their trip. The authors came up with a variety of reasons why the travel agent could not just charge their credit card for the necessary amount and why they themselves could not send the money by bank transfer. After a certain delay, the cybercriminals cancelled the hotel booking and received the second part of the money, which had been laundered in this way.

‘Gray’ mailings

Another issue is that on the one hand, advertisers want to advertise via well-designed official mailings (without any kind of spammer tricks and ‘noise’ making advertisements hard to read), which will reach users. On the other hand, they want to use huge databases that include millions of addresses rather than sending their messages to the few subscribers they already have.

The result is an increasing number of ‘gray’ mailings. These are official mailings that are sent from senders’ own servers rather that via botnets, they can be subscribed to and unsubscribed from. But in addition to official subscribers these messages are often sent to addresses taken from huge databases these companies have purchased – to people who never gave their consent to receive such messages. (It is worth noting that under many countries’ laws mailings without the prior consent of the recipients are illegal.)

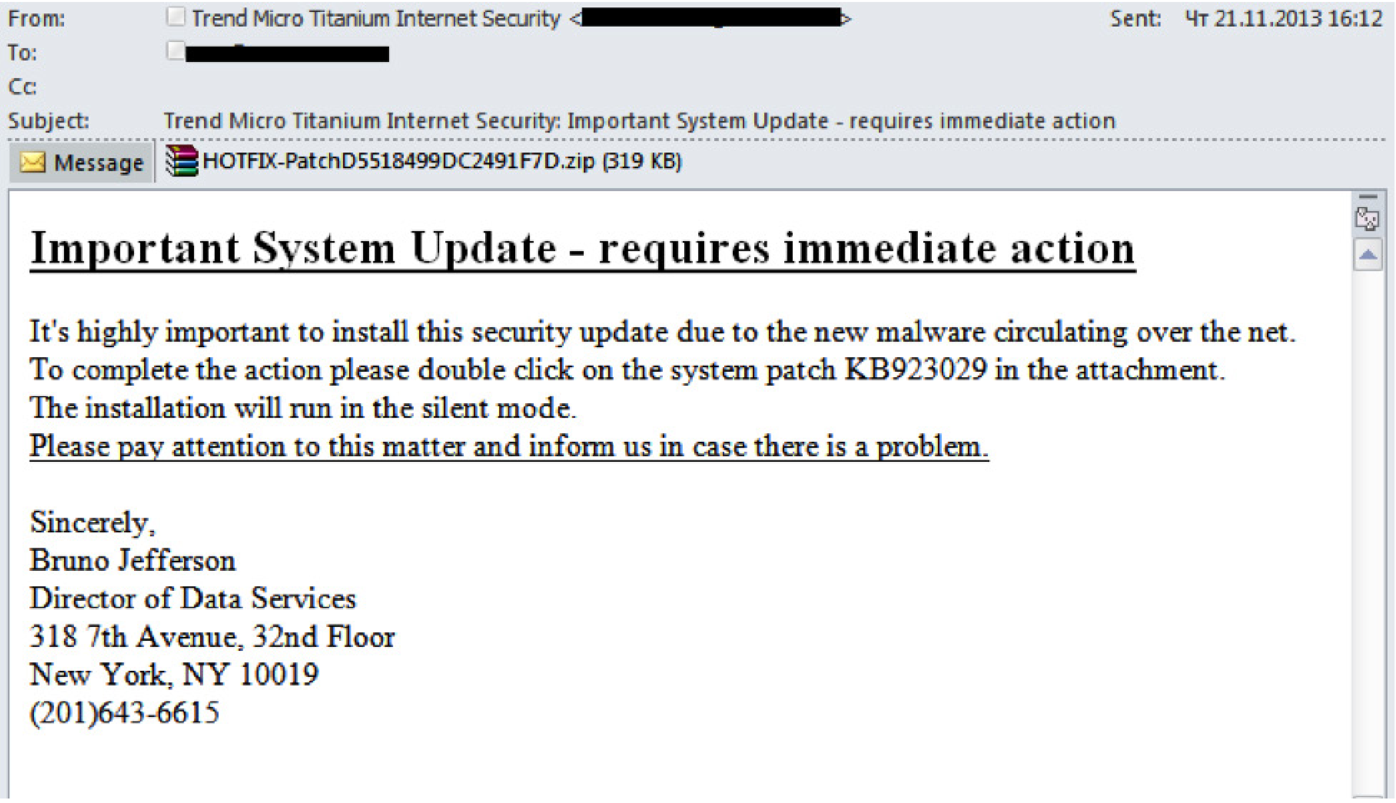
This leads to situations in which part of a mailing is legal and legitimate and part of it is spam. This poses a new challenge for the anti-spam industry and leads to the development of new technologies based on sender reputations.

3 Trend of 2013: fake messages from antivirus vendors

Typically, malicious and fraudulent emails target credulous people or those who know very little about online security rules. A sensible person can hardly be expected to believe in the authenticity of an email saying he or she has won millions of dollars by pure chance, and someone who knows the basic rules of IT security would never follow a link in a message ‘from the bank’ and enter credentials to an online banking account.

In 2013, we detected several mailings which looked like messages from antivirus vendors, i.e., were designed for people who understand the basics of security.

Note that IT security experts strongly advise users to update their antivirus solutions regularly, because this is essential to deliver reliable protection for their computers. Cybercriminals are trying to take advantage of that. In an email sent on behalf of an antivirus vendor, they urged users to update their systems immediately using the file attached. The message itself did not change from one email to the next, but spammers used the names of virtually all major antivirus vendors in the sender field, including Kaspersky Lab, McAfee, ESET, Symantec and others.



From: Trend Micro Titanium Internet Security <[redacted]> Sent: Чт 21.11.2013 16:12
To: [redacted]
Cc:
Subject: Trend Micro Titanium Internet Security: Important System Update - requires immediate action

HOTFIX-PatchD5518499DC2491F7D.zip (319 KB)

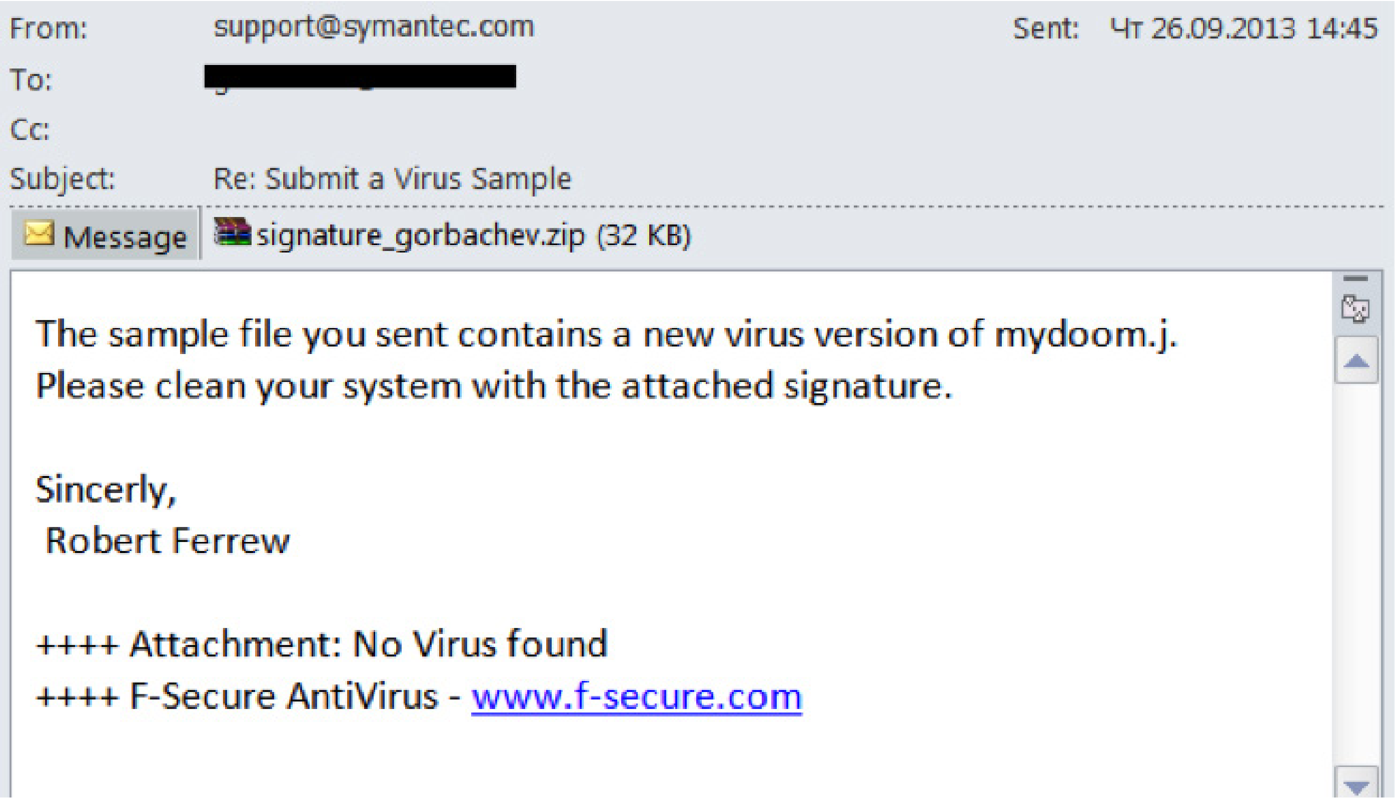
Important System Update - requires immediate action

It's highly important to install this security update due to the new malware circulating over the net.
To complete the action please double click on the system patch KB923029 in the attachment.
The installation will run in the silent mode.
Please pay attention to this matter and inform us in case there is a problem.

Sincerely,
Bruno Jefferson
Director of Data Services
318 7th Avenue, 32nd Floor
New York, NY 10019
(201)643-6615

In reality, the attachment was a malicious program detected by Kaspersky Lab as Trojan-Spy.Win32.Zbot.qsjm. The Trojan belongs to the infamous ZeuS/Zbot family and is designed to steal sensitive user data, particularly financial info. The malware is capable of modifying the contents of bank websites loaded on the browser by embedding malicious scripts in order to obtain authentication data (logins, passwords and security codes). The Trojan also steals personal data by taking screenshots, recording a video of the screen, logging keystrokes, etc. Unusually, Trojan-Spy.Win32.Zbot.qsjm uses a P2P protocol and receives commands and the configuration file from other infected machines instead of connecting to a command-and-control server.

This same trick was also used in another mailing: a user received a fake email imitating a message from an antivirus vendor's support service with the results of a file scan in the attachment.



From: support@symantec.com Sent: Чт 26.09.2013 14:45
To: [redacted]
Cc:
Subject: Re: Submit a Virus Sample

The sample file you sent contains a new virus version of mydoom.j.
Please clean your system with the attached signature.

Sincerly,
Robert Ferrew

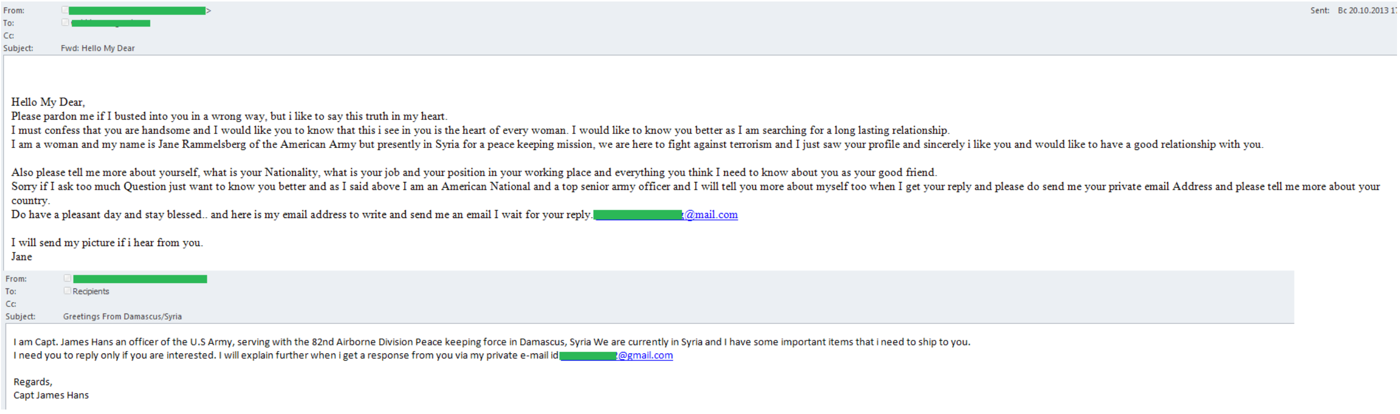
++++ Attachment: No Virus found
++++ F-Secure AntiVirus - www.f-secure.com

The attachment was supposedly a file that could be used to purge a malicious program from the system. In fact, it was an email worm detected by Kaspersky Lab as Email-Worm.Win32.NetSky.q. The worm is designed to collect email addresses from user contact lists.

4 World events in spam

In 2013, spammers actively exploited high-profile world events in their mass mailings. The overwhelming majority of these were fraudulent or malicious. For example, the news of the death of Venezuelan President Hugo Chavez was used both in fraudulent and malicious emails. However, as a rule, different categories of spammers focus on different types of news. For instance, "Nigerian letters" most often exploit events from Asia and the Middle East while European and American news is mainly utilized in emails containing malicious links. Fraudulent emails are distributed in different languages (however, they are often translated with the help of a machine-translation service) while malicious spam is almost always written in English.

In 2013 "Nigerian" spam actively exploited the theme of the overthrow of Egyptian President Mohammed Morsi as well as the issues related to the complicated political situation in Syria. Applying traditional "Nigerian" methods, the scammers tried to con money from users. Similar mass mailings appeared in response to the death of the Libyan leader Muammar Gaddafi and the imprisonment of the Egyptian President Hosni Mubarak. All these emails are very similar although spammers keep trying to come up with new stories. For example, among the Syria-related spam there were messages sent allegedly on behalf of U.S. Army soldiers:



From: [redacted]>
To: [redacted]
Cc:
Subject: Fwd: Hello My Dear
Sent: Вс 20.10.2013 1

Hello My Dear,
Please pardon me if I busted into you in a wrong way, but i like to say this truth in my heart.
I must confess that you are handsome and I would like you to know that this i see in you is the heart of every woman. I would like to know you better as I am searching for a long lasting relationship.
I am a woman and my name is Jane Rammelsberg of the American Army but presently in Syria for a peace keeping mission, we are here to fight against terrorism and I just saw your profile and sincerely i like you and would like to have a good relationship with you.

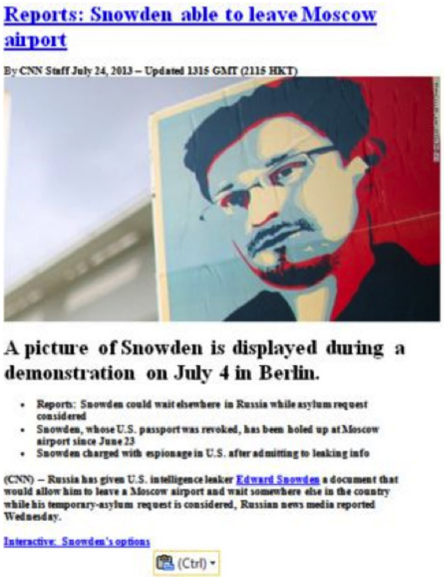
Also please tell me more about yourself, what is your Nationality, what is your job and your position in your working place and everything you think I need to know about you as your good friend.
Sorry if I ask too much Question just want to know you better and as I said above I am an American National and a top senior army officer and I will tell you more about myself too when I get your reply and please do send me your private email Address and please tell me more about your country.
Do have a pleasant day and stay blessed.. and here is my email address to write and send me an email I wait for your reply.[redacted]@mail.com

I will send my picture if i hear from you.
Jane

From: [redacted]
To: Recipients
Cc:
Subject: Greetings From Damascus/Syria

I am Capt. James Hans an officer of the U.S Army, serving with the 82nd Airborne Division Peace keeping force in Damascus, Syria We are currently in Syria and I have some important items that i need to ship to you.
I need you to reply only if you are interested. I will explain further when i get a response from you via my private e-mail id[redacted]@gmail.com

Regards,
Capt James Hans



Reports: Snowden able to leave Moscow airport

By CNN Staff July 24, 2013 – Updated 1315 GMT (2115 HKT)

A picture of Snowden is displayed during a demonstration on July 4 in Berlin.

- Reports: Snowden could wait elsewhere in Russia while asylum request considered
- Snowden, whose U.S. passport was revoked, has been holed up at Moscow airport since June 23
- Snowden charged with espionage in U.S. after admitting to leaking info

(CNN) -- Russia has given U.S. intelligence leaker Edward Snowden a document that would allow him to leave a Moscow airport and wait somewhere else in the country while his temporary-asylum request is considered, Russian news media reported Wednesday.

Interactive: Snowden's options

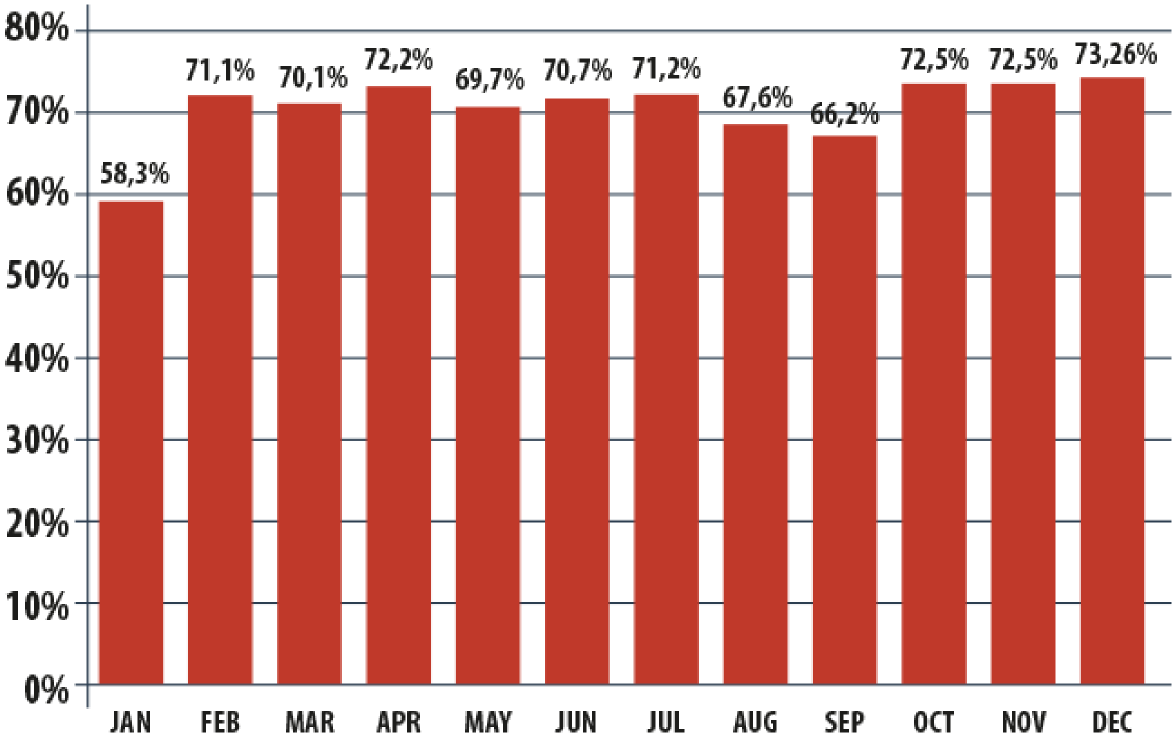
Other malicious spam referenced such events as the election of the new Pope, the birth of the royal baby in the UK, Edward Snowden's exposures, etc. Malicious emails usually imitate newsletters and contain a link to supposedly interesting material. In fact, the link redirects the user to a site with malicious programs.

Many malicious mailings exploiting breaking news contained links to sites using the Blackhole exploit kit. However, since the arrest of the alleged author of the Blackhole exploits in October typical news patterns have no longer been used by spammers. This is likely to be a temporary phenomenon and soon we will come across "newsletters" containing links to other malicious programs.

5 Statistics

The percentage of spam in email traffic

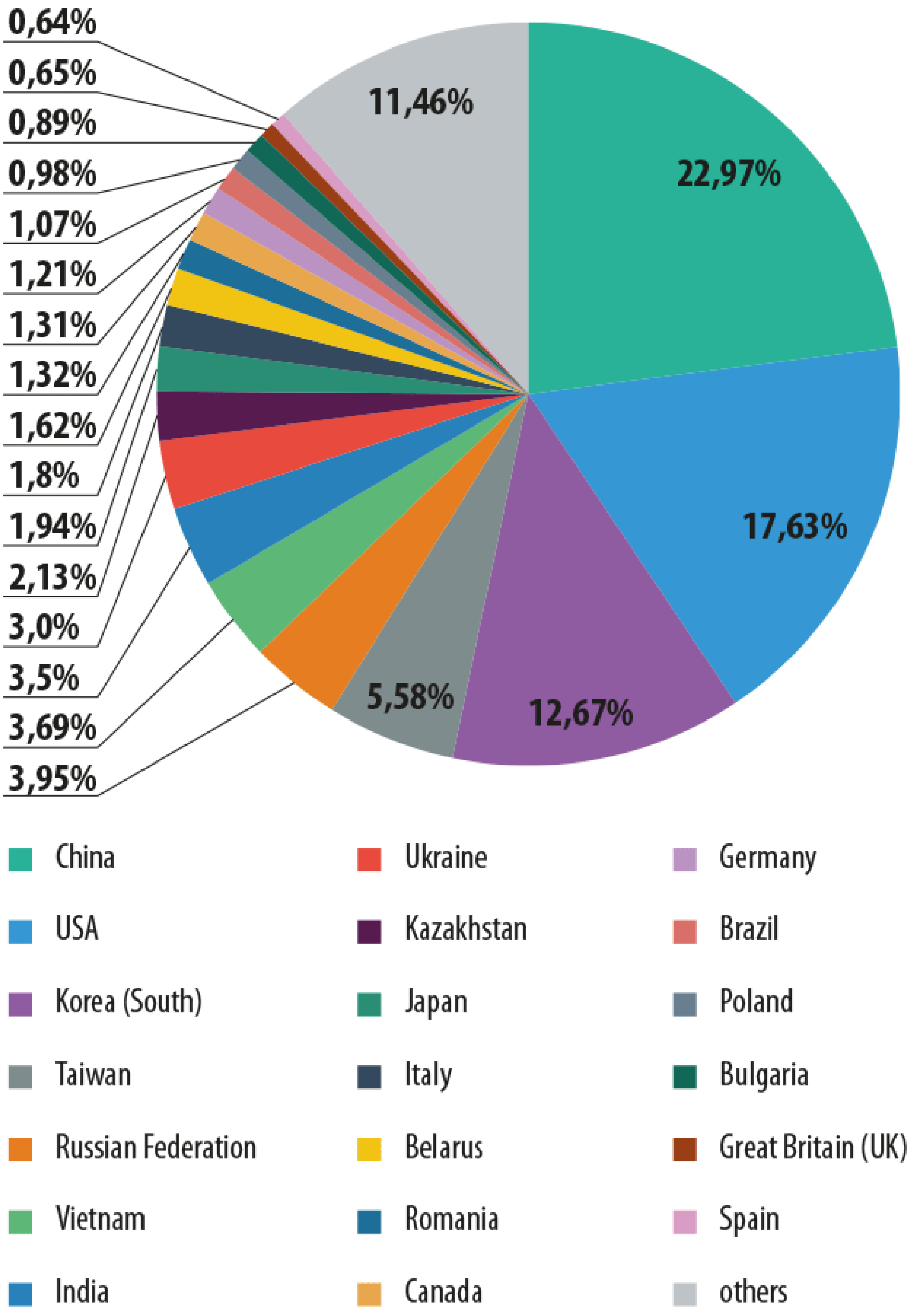
The percentage of spam in total email traffic decreased by 2.5 percentage points in comparison with the previous year and came to 69.6%. For the first time in many years the average annual spam percentage is less than 70%.



The percentage of spam in email traffic, 2013

Over the course of the year the percentage of spam remained fairly constant from month to month (with the exception of the abnormally low figure for January). This suggests stability and we can be confident that there will be little different in the coming year.

Sources of spam by country

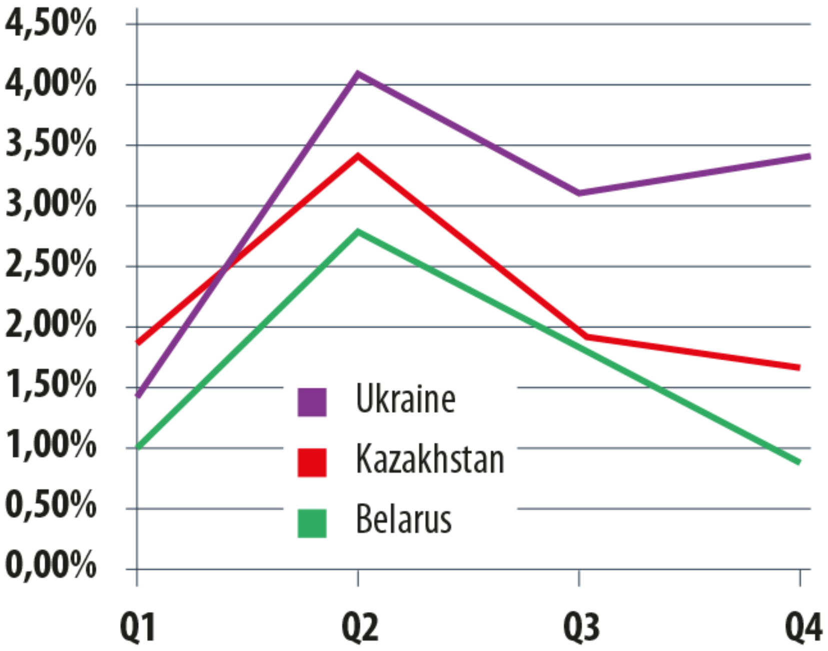


Distribution of spam sources by country in 2013

The countries that are the top sources of spam remain the same: China (+3.5 percentage points) and the US (+2 points) were the source of 40.6% of all the world's spam. These countries came first and second in the spam distribution rating, matching their positions in lists of countries ranked by number of Internet users.

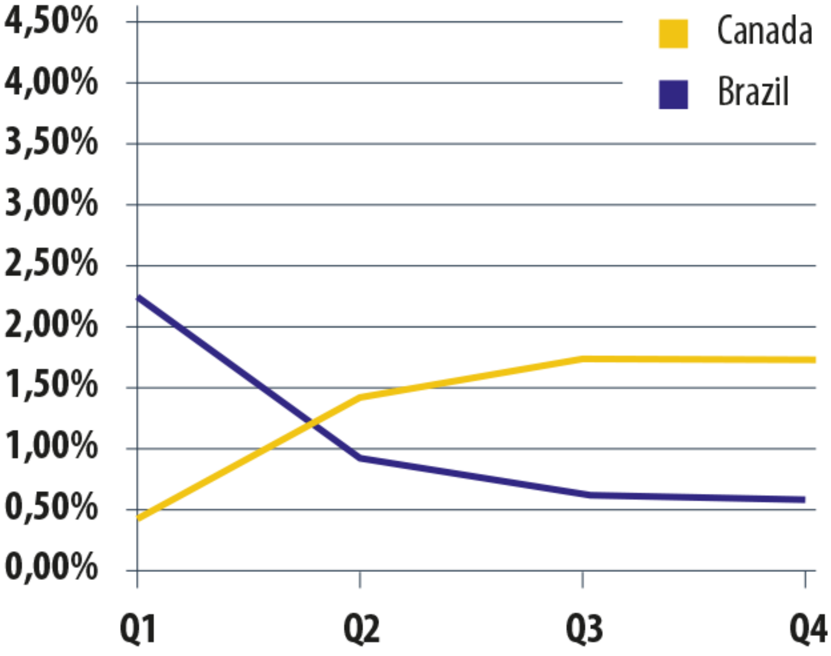
South Korea moved up to third, seeing its percentage share increase 3.5 times compared with the previous year. Taiwan also saw a significant increase (+3.7 percentage points) as it climbed to 4th place.

The volume of spam from Kazakhstan, Ukraine and Belarus also grew, largely due to a spike in Q2, 2013:



The percentage of spam originating in Ukraine, Kazakhstan and Belarus in 2013

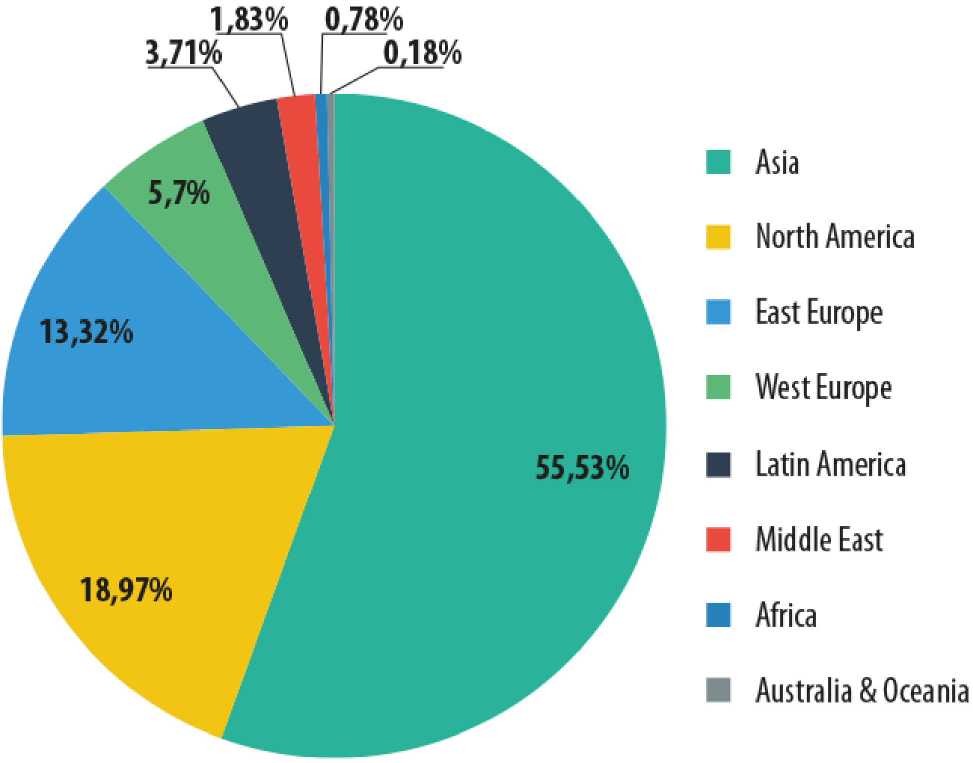
The level of spam coming from Brazil decreased fourfold, which pushed it down from 5th to 16th. At the same time, the percentage of spam from Canada surged significantly, bringing it into the Top 20 spam sources for the first time. On average for 2013 Canada was ranked 14th.



The percentage of outgoing spam from Canada and Brazil in 2013

We hasten to point out Canada has still adopted no legislation against spam. An anti-spam law was first mooted in Canada back in 2005, but it is only due to come into effect on July 1, 2014, according to Industry Minister James Moore. As well as spam, the law will also regulate some related fields, such as botnet organization, phishing and malware distribution.

Sources of spam by region

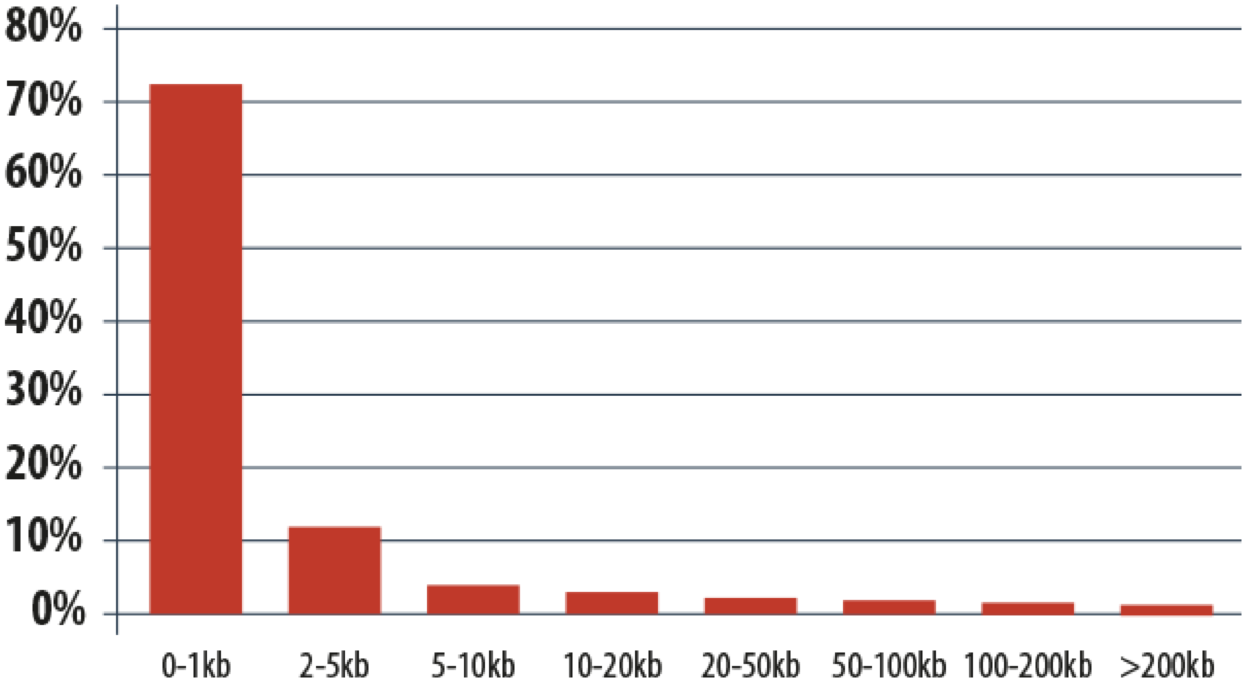


The distribution of spam sources by region in 2013

As for the top sources of spam by region, Asia (+5.3 percentage points) and North America (+3.2 percentage points) are still out in front. Eastern Europe moved up to third place after its share almost doubled compared with the previous year.

Western Europe's share decreased by 2.4 percentage points, though it remains in 4th place. Latin America came 5th in 2013 with a threefold drop in its share.

The size of spam emails



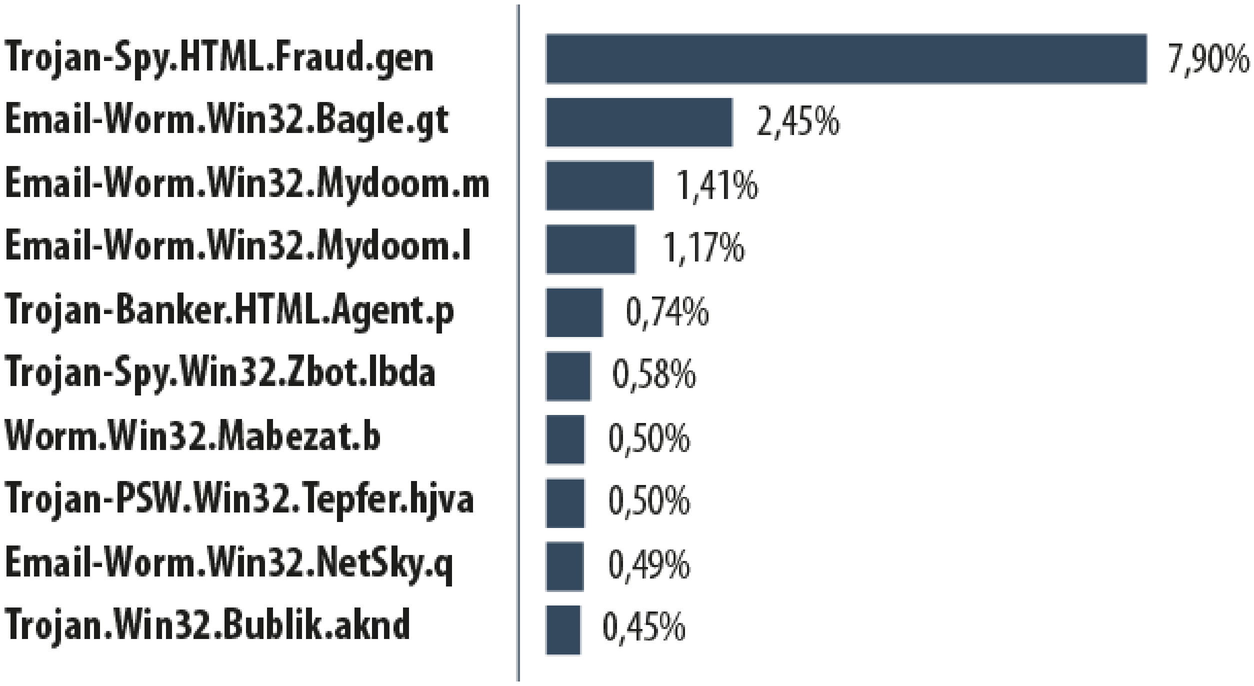
The size of spam emails in 2013

2013 could be called the year of the super-short email. The percentage of spam emails weighing in at under 1 KB came to 74.5%. Using compact messages spammers are able to send out more letters and reduce traffic costs. It is really easy to use machine-written short phrases, which change from message to message, by using a handful of key words and some random distortion. In the end you get unique messages, making the task of spam filters more difficult. These emails usually contain links to advertising websites. A typical example of super short spam is the advertising of medication like Viagra or Cialis.

6 Malicious attachments in email

In 2013 malicious attachments were found in 3.2% of all mail traffic, which is 0.2 percentage points lower than previously.

For the third year in a row the most prevalent malware spread by email were programs that attempted to steal confidential data, usually logins and passwords for Internet banking systems.



The Top 10 malicious programs spread by email in 2013

Trojan-Spy.HTML.Fraud.gen took first place. It is generally distributed using phishing emails and is designed to look like an html page used as the registration form of an online banking service. That page is then used by phishers to steal user account data.

The email worms Bagle and Mydoom dominate the Top 10, occupying positions 2, 3, 4, 7 and 9. The main function of these worms is to collect electronic addresses from infected computers. Bagle email worms can also receive remote commands to integrate with other malicious applications.

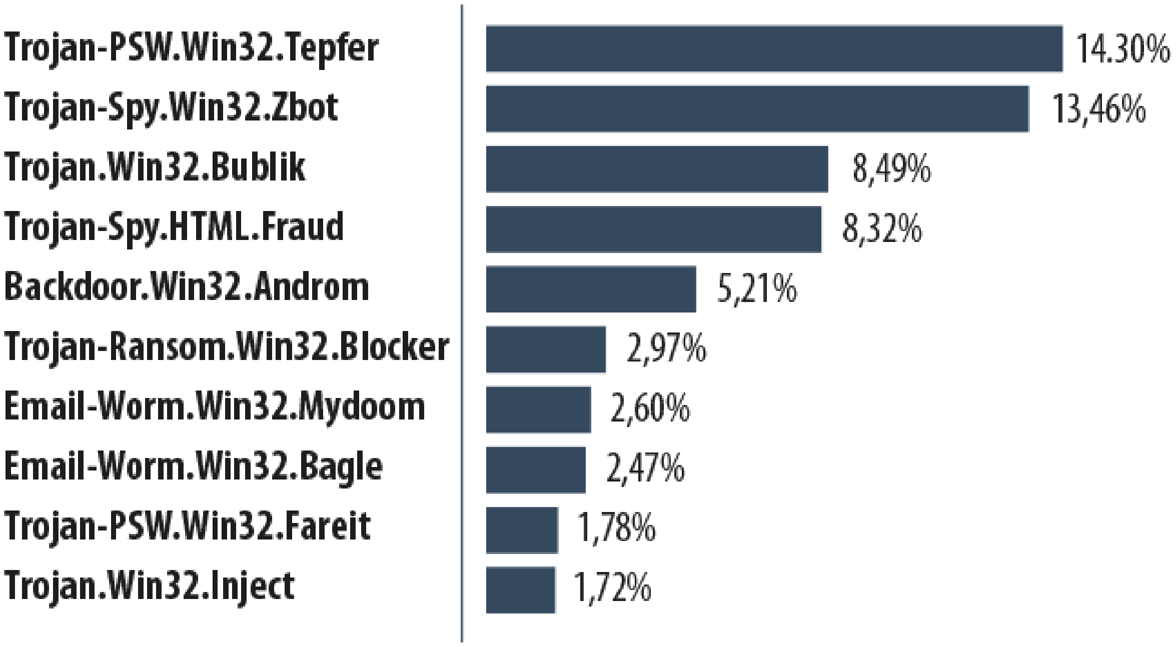
Trojan-Banker.HTML.Agent.p ended 2013 in 5th place. Like Fraud.gen, this malware is designed as an html-page that copies registration forms for online banking and other Internet services. It aims to steal user account details.

In 6th place we find a Trojan spy from the Zbot family. The Zeus/Zbot families also target confidential data, including credit card details. Last year this malware did not make the Top 10 but we knew better than to assume it had gone away. The Zbot malware family has existed for years and is constantly changing.

Trojan-PSW.Win32.Tepfer.hjva came 8th. Malware of this type is created to steal passwords to user accounts.

10th place is occupied by Trojan.Win32.Bublik.aknd, which collects FTP passwords, authorization data for email services and certificates from infected computers. The Trojan can also search for logins and passwords saved in Mozilla Firefox and Google Chrome browsers. All passwords are sent directly to the criminals.

Some malware families have many different modifications, and others only a few types, so our rating of malware families is different from the rating of malicious programs.

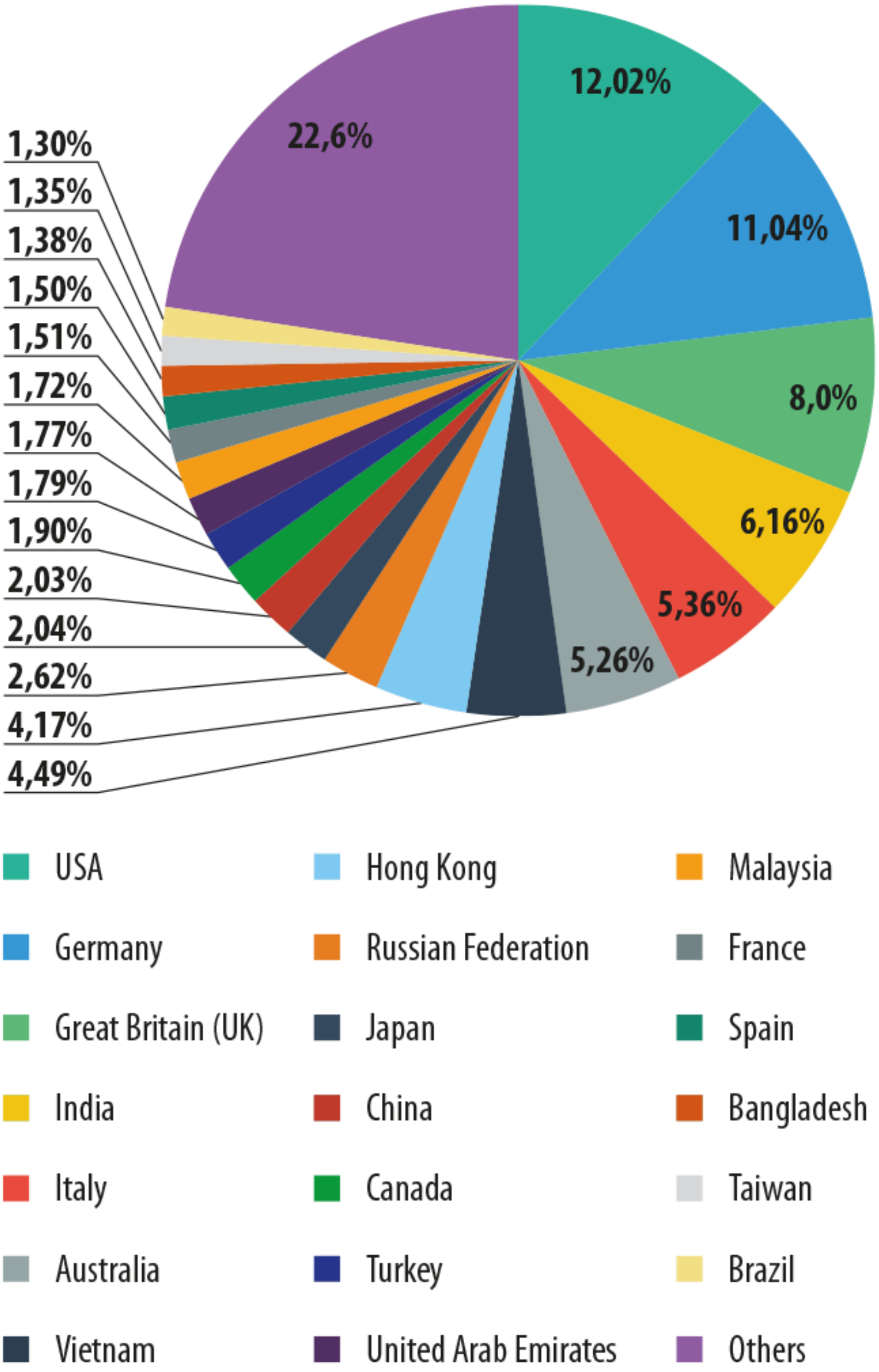


The Top 10 malware families distributed via mail traffic in 2013

Along with the families described above – Tepfer, Zbot, Bublik, Fraud, Mydoom and Bagle – the following species are included in this rating:

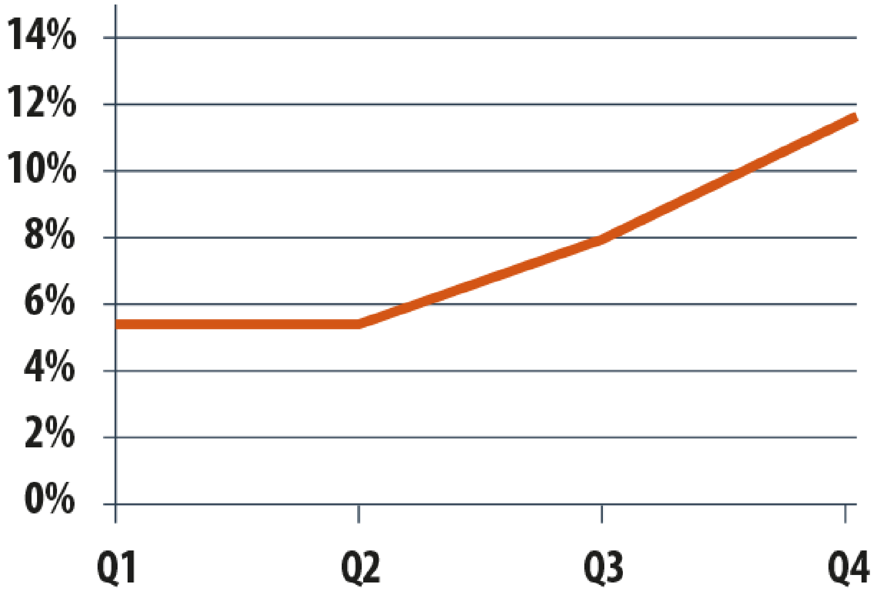
- Backdoor.Win32.Androm allows a criminal to control an infected computer secretly, for example, to download other malicious files and run them, send information from the victim's computer, etc. Moreover, computers infected with this malware are often included in a botnet.
- Trojan-Ransom.Win32.Blocker is designed for blackmail. It blocks the OS activity and displays a banner detailing the conditions needed to regain control of the system. Typically it demands a text message be sent to a premium rate number where the criminals can hoover up the proceeds.
- Trojan-PSW.Win32.Fareit.amdp searches through the registry and system files that store confidential data to find and transmit passwords, logins and other information to the criminals.

- Trojan.Win32.Inject is a loader program that downloads other malware onto an infected computer.



The distribution of email antivirus detections by country in 2013

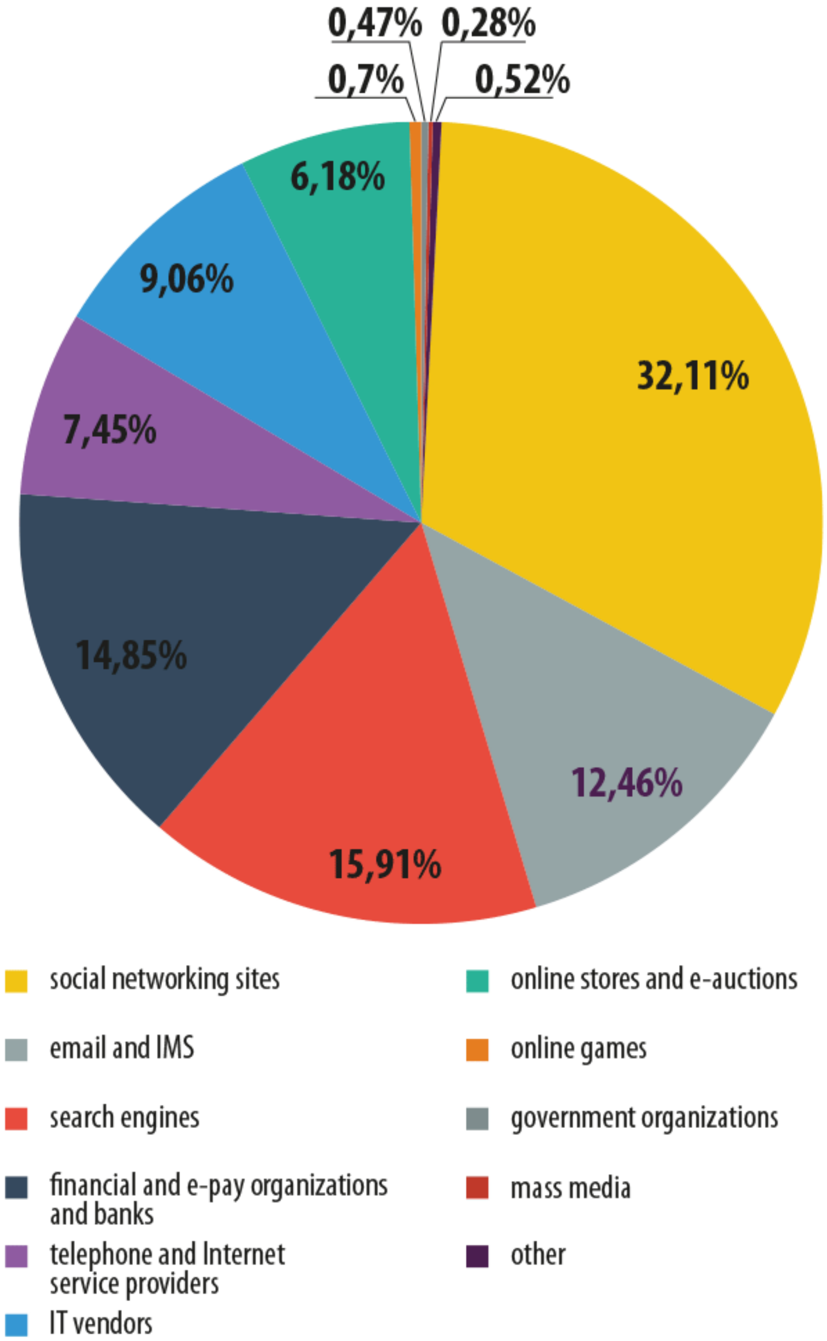
As for the countries which receive most malware, the Top 3 remains the same as before – the US, the UK and Germany. While the share going to Germany and the United States hardly varied, the UK's share rose from 5.4% in Q1 to 11.9% in Q4.



Email antivirus detections changes in the UK in 2013

Other countries showed broadly similar results, except for Italy, which surged from 10th to 5th position (+2.1 percentage points). This may be explained by the events of February when Italy was exposed to a widespread distribution containing Trojan-Banker.HTML.Agent.p. That lifted Italy to first place in the Top 10 for that month.

7 Phishing



Distribution of the Top 100 organizations most frequently targeted by phishers, by category, 2013*

** This rating is based on Kaspersky Lab's anti-phishing component detections, which are activated every time a user attempts to click on a phishing link, regardless of whether the link is in a spam email or on a web page.*

In 2013 we saw phishers targeting more organizations that have no direct link to any financial data or service. There was a 7.6 percentage points increase in attacks using social networks, and search engines saw a 1.8 percentage points rise. The percentage of attacks on email services increased fourfold. At the same time the numbers for financial institutions and online stores dropped by 6 percentage points and 12.2 percentage points respectively.

These significant changes show that phishing is monetized mostly by the sale of stolen accounts. These accounts are later used for spam or malicious distribution across their contact lists. Today's trend to unify services in a single place means that a single account could open up access to email, social networks, file storage and more. It's also quite possible a victim account will be linked to banking data. Thus, every account becomes an attractive target for a cybercriminal.

8 Conclusion and forecasts

Across the whole of 2013 the percentage of spam decreased by 2.5 percentage points in comparison with the previous year, although apart from a sudden dip in January levels remained fairly consistent. In 2014 the percentage of spam in traffic is also likely to remain almost the same. At the same time, the field of "grey" distribution, material sent out both to subscribers and a wide range of uninterested users, is likely to grow.

As we see fewer legal commercial offers in spam, the more we see fraudulent and malicious messages appearing. Previously cybercriminals could rely on exploiting the trust of unwary users, but now they face a new generation of IT-savvy targets. That has prompted them to adopt new tactics, such as sending out malicious attachments in the guises of antivirus updates. Among malicious attachments there is more and more malware which aims to steal confidential data, especially passwords and logins to banking systems. We expect this trend to continue next year.

At the same time, however, phishing attacks are shifting from bank accounts to social networking and email. This can be partly explained by the fact that today's email accounts often give access to a lot of content, including email, social networking, instant messaging, cloud storages and sometimes even a credit card.

Spam is changing and as traditional advertising declines we see far more fraud, malware and phishing. As a result, even experienced Internet users have to be more alert than ever to avoid stumbling into a cybercriminal's trap.