Spam in Q1 2013

Darya Gudkova

Content

The quarter in figures

- The percentage of spam in total mail traffic was up by 0.5 percentage points in the first quarter, averaging 66.5%.
- The proportion of phishing emails decreased 4.25 times and amounted to 0.004%.
- Malicious attachments were found in 3.3% of all emails, an increase of 0.1 percentage points.

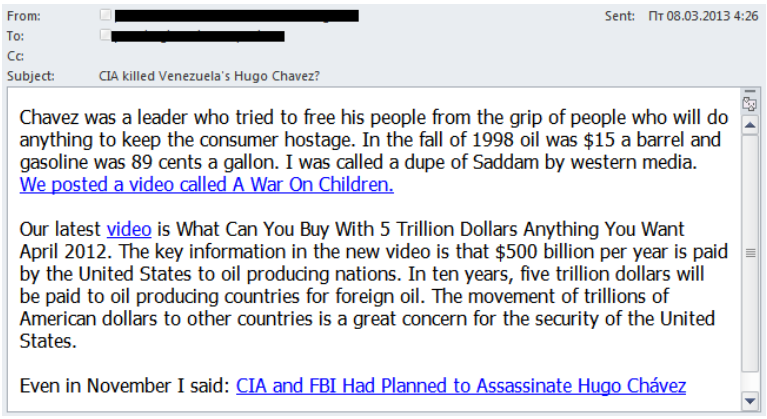
The quarter in the spotlight

In the first quarter of 2013, several high-profile events occurred: the Venezuelan President Hugo Chavez died, Pope Benedict XVI resigned and the new Pope Francis was officially inaugurated. As usual, such events did not go unnoticed by spammers. Public interest in these important world events was widely utilized by the distributors of malicious links and fraudulent emails. However, cybercriminals did not forget about other methods of social engineering.

Hot news with malicious links

After the demise of the President of Venezuela, spam traffic saw the appearance of emails provocatively titled "CIA "DELETED" Venezuela's Hugo Chavez?" Their authors alluded to the involvement of the US

government and the CIA in the death of Hugo Chavez and suggested the recipient click the link to see a related video.


From: [redacted] Sent: Пт 08.03.2013 4:26
To: [redacted]
Cc:
Subject: CIA killed Venezuela's Hugo Chavez?

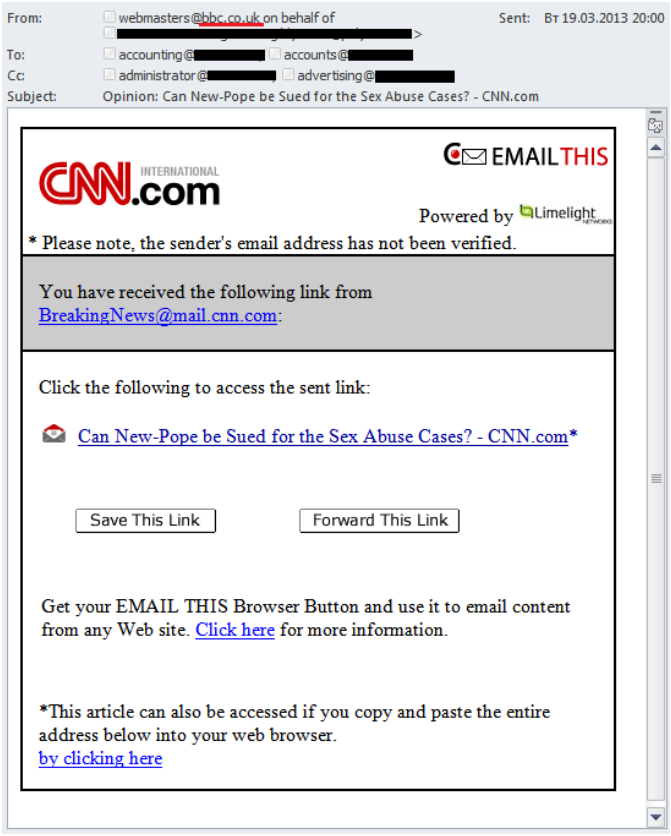
Chavez was a leader who tried to free his people from the grip of people who will do anything to keep the consumer hostage. In the fall of 1998 oil was $15 a barrel and gasoline was 89 cents a gallon. I was called a dupe of Saddam by western media. We posted a video called A War On Children.

Our latest video is What Can You Buy With 5 Trillion Dollars Anything You Want April 2012. The key information in the new video is that $500 billion per year is paid by the United States to oil producing nations. In ten years, five trillion dollars will be paid to oil producing countries for foreign oil. The movement of trillions of American dollars to other countries is a great concern for the security of the United States.

Even in November I said: CIA and FBI Had Planned to Assassinate Hugo Chávez

The link led careless users to a hacked legitimate site that then directed them to a malicious resource which contained obfuscated java script. If a potential victim's operating system complied with certain parameters, a malicious program was installed on the user's computer with the help of the exploit proactively detected by Kaspersky Lab as HEUR:Exploit.Java.CVE-2012-0507.gen.

However, Hugo Chavez was not the sole focus of the fraudsters' attention in Q1 2013. Another mass mailing containing sensational "news" and a malicious link invoked the name of the new Pope to attract users. The mass mailing imitated BBC or CNN news reports, and invited recipients to read about the pontiff. Specifically, one of the headings invited users to join a discussion about His Holiness supposedly facing accusations of sexual abuse.



This spam attack was similar to the Hugo Chavez version: on clicking the link, the user was redirected to a hacked site from which an exploit (most often it was from the Blackhole exploit kit) was downloaded to their computer and used to infect it with a malicious program.

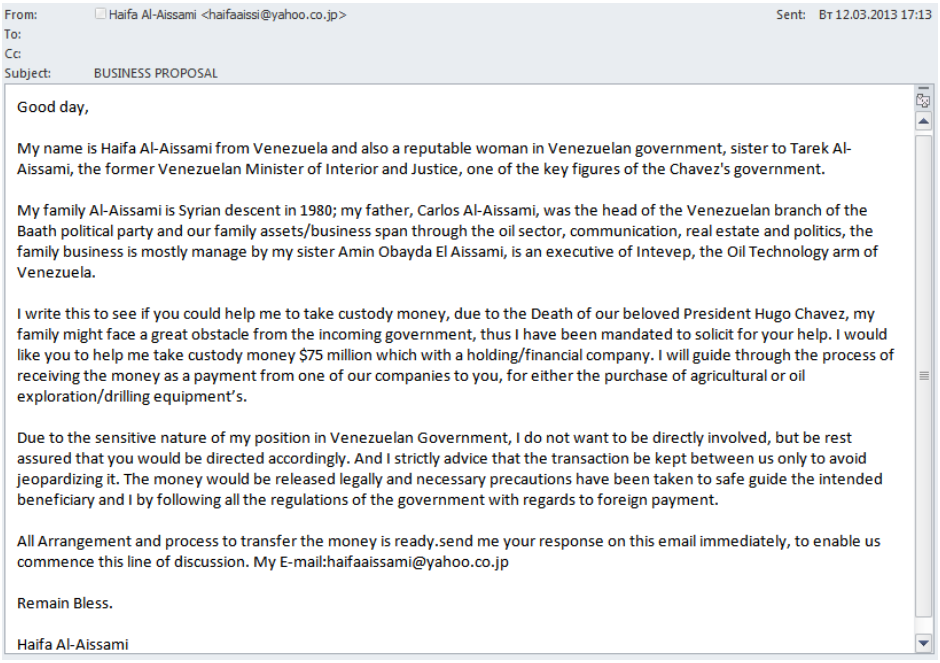
Interestingly, despite the apparent thoroughness of designing fake news notifications, the fraudsters confused the headings at times: for example, they left the word “BBC” in the “From” field of emails when sending messages that purported to be from CNN.

The use of hot news in combination with links to supposedly sensational photos and videos is one of the spammers’ favorite tricks for spreading malware. We have already seen similar mailings offering to show us Osama bin Laden’s photos, compromising material on Barack Obama, etc. Despite the variety of themes used by spammers, the result of clicking the links contained in such messages is the same - the user's computer is subjected to attempted malware downloads.

‘Nigerian’ spam and events in Venezuela

“Nigerian” scammers have always tried to cash in on instability in a country, so certainly weren’t going to overlook events in Venezuela. In Q1 2013, we registered several mass mailings in different languages exploiting global interest in this topic.

The tactics of the English-language email are standard for Nigerian fraud: the message was allegedly written by a person close to the ruling elite who asks for help to get cash out of the country before it is expropriated by the new government.



From: Haifa Al-Aissami <haifaaissi@yahoo.co.jp> Sent: Вт 12.03.2013 17:13
To:
Cc:
Subject: BUSINESS PROPOSAL

Good day,

My name is Haifa Al-Aissami from Venezuela and also a reputable woman in Venezuelan government, sister to Tarek Al-Aissami, the former Venezuelan Minister of Interior and Justice, one of the key figures of the Chavez's government.

My family Al-Aissami is Syrian descent in 1980; my father, Carlos Al-Aissami, was the head of the Venezuelan branch of the Baath political party and our family assets/business span through the oil sector, communication, real estate and politics, the family business is mostly manage by my sister Amin Obayda El Aissami, is an executive of Intevep, the Oil Technology arm of Venezuela.

I write this to see if you could help me to take custody money, due to the Death of our beloved President Hugo Chavez, my family might face a great obstacle from the incoming government, thus I have been mandated to solicit for your help. I would like you to help me take custody money $75 million which with a holding/financial company. I will guide through the process of receiving the money as a payment from one of our companies to you, for either the purchase of agricultural or oil exploration/drilling equipment's.

Due to the sensitive nature of my position in Venezuelan Government, I do not want to be directly involved, but be rest assured that you would be directed accordingly. And I strictly advice that the transaction be kept between us only to avoid jeopardizing it. The money would be released legally and necessary precautions have been taken to safe guide the intended beneficiary and I by following all the regulations of the government with regards to foreign payment.

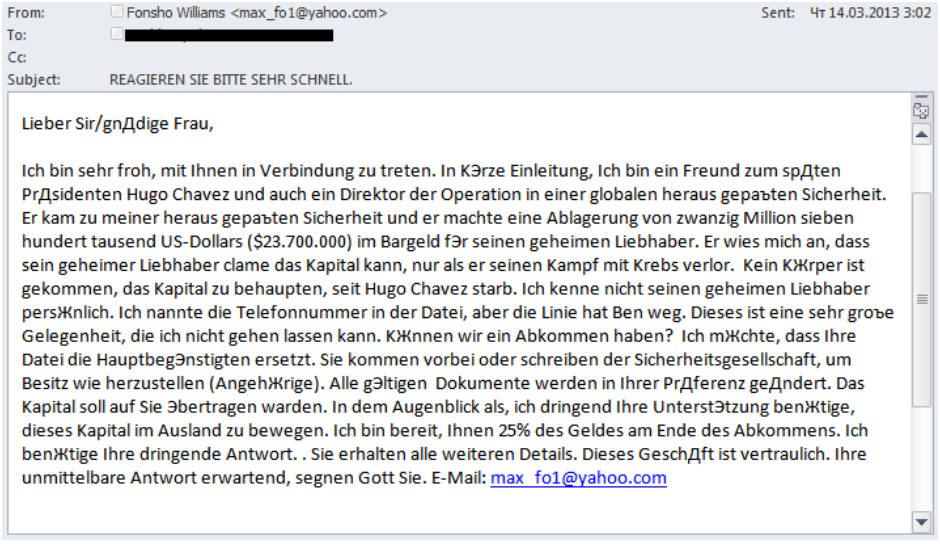
All Arrangement and process to transfer the money is ready.send me your response on this email immediately, to enable us commence this line of discussion. My E-mail:haifaaissami@yahoo.co.jp

Remain Bless.

Haifa Al-Aissami

We registered Nigerian letters with similar content but different names after the demise of the Libyan leader Muammar Gaddafi and after the imprisonment of former Egyptian President Hosni Mubarak.

In a German-language mass mailing the author writes he was a friend of the late Hugo Chavez and, at his request, is looking after $23 million in Chavez's secret lover's bank account. A reward is offered to anyone who can help cash this money.



From: Fonsho Williams <max_fo1@yahoo.com> Sent: Чт 14.03.2013 3:02
To: [redacted]
Cc:
Subject: REAGIEREN SIE BITTE SEHR SCHNELL.

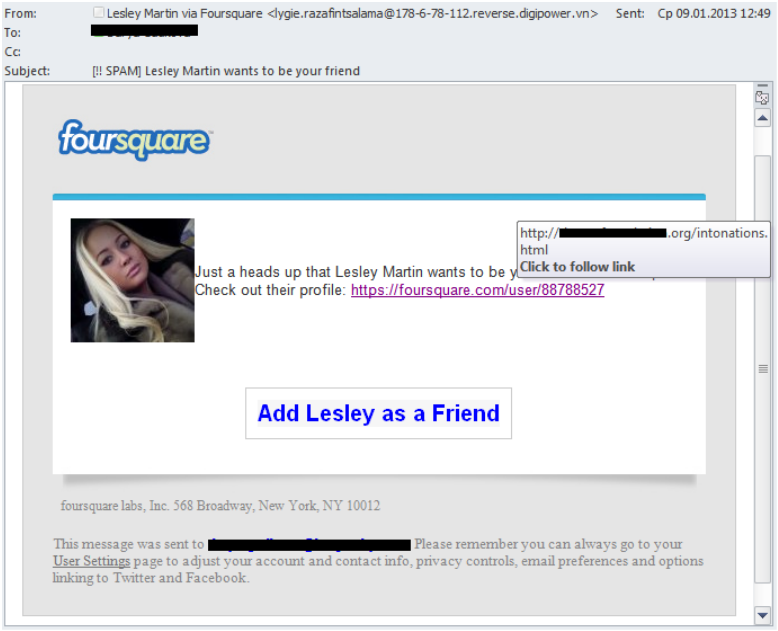
Lieber Sir/gnДdige Frau,

Ich bin sehr froh, mit Ihnen in Verbindung zu treten. In KЭrze Einleitung, Ich bin ein Freund zum spДten PrДsidenten Hugo Chavez und auch ein Direktor der Operation in einer globalen heraus gepaъten Sicherheit. Er kam zu meiner heraus gepaъten Sicherheit und er machte eine Ablagerung von zwanzig Million sieben hundert tausend US-Dollars ($23.700.000) im Bargeld fЭr seinen geheimen Liebhaber. Er wies mich an, dass sein geheimer Liebhaber clame das Kapital kann, nur als er seinen Kampf mit Krebs verlor. Kein KЖrper ist gekommen, das Kapital zu behaupten, seit Hugo Chavez starb. Ich kenne nicht seinen geheimen Liebhaber persЖnlich. Ich nannte die Telefonnummer in der Datei, aber die Linie hat Ben weg. Dieses ist eine sehr groъe Gelegenheit, die ich nicht gehen lassen kann. KЖnnen wir ein Abkommen haben? Ich mЖchte, dass Ihre Datei die HauptbegЭnstigten ersetzt. Sie kommen vorbei oder schreiben der Sicherheitsgesellschaft, um Besitz wie herzustellen (AngehЖrige). Alle gЭltigen Dokumente werden in Ihrer PrДferenz geДndert. Das Kapital soll auf Sie Эbertragen warden. In dem Augenblick als, ich dringend Ihre UnterstЭtzung benЖtige, dieses Kapital im Ausland zu bewegen. Ich bin bereit, Ihnen 25% des Geldes am Ende des Abkommens. Ich benЖtige Ihre dringende Antwort. . Sie erhalten alle weiteren Details. Dieses GeschДft ist vertraulich. Ihre unmittelbare Antwort erwartend, segnen Gott Sie. E-Mail: max_fo1@yahoo.com

How Nigerian scammers interact with potential victims is already well known. The fraudsters' goal at the initial stage is to get the recipient interested and make him respond to the email. In further correspondence the victim is asked to transfer a small sum of money – insignificant when compared with the promised reward – to a certain account. This money will allegedly go to pay the lawyer's services, taxes, etc. Once they receive this money, the fraudsters end all contact with their victim.

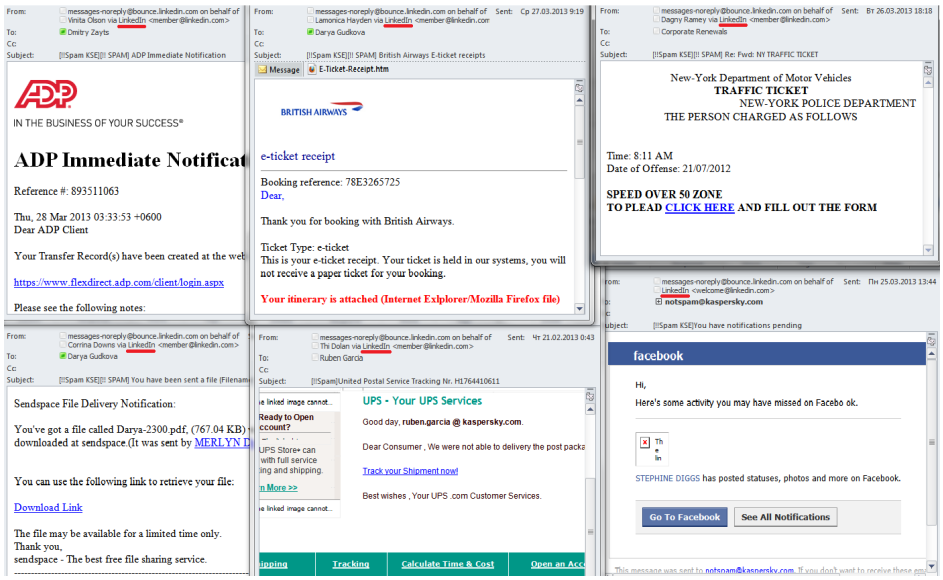
Social fakes

Spammers, especially those whose goal is to infect users' computers, are still using notorious fake notifications from well-known services. In Q1 2013, the "usual suspects" of mass mailings such as Facebook and Twitter were joined by the Foursquare service. Once again, a simple rule was confirmed: the more popular the service, the more likely it is to be imitated by spammers.



Most often these emails are used by cybercriminals to distribute links to sets of exploits that can find a vulnerability on a user's computer and install other malicious programs via this breach. The Blackhole exploit kit is especially popular with the spammers.

Tellingly, the scammers do not always ensure that the heading or the “From” field message of their fake notification matches the content of the email. Interestingly, the same mistake is made by the fraudsters who send fake messages using the names of the media giants CNN and BBC. This may point to the fact that all these mass mailings are controlled by a single group of cybercriminals.



Spammer methods and tricks

It is quite obvious that modern-day spammers can no longer come up with anything new: all the tricks of the trade have already been used in one form or another. As a result, the fraudsters have switched to combinations of several techniques, including those which were once very popular but fell into disuse for some time. In addition, spammers have been exploring the possibilities offered by legitimate services and are now using them to bypass spam filtering.

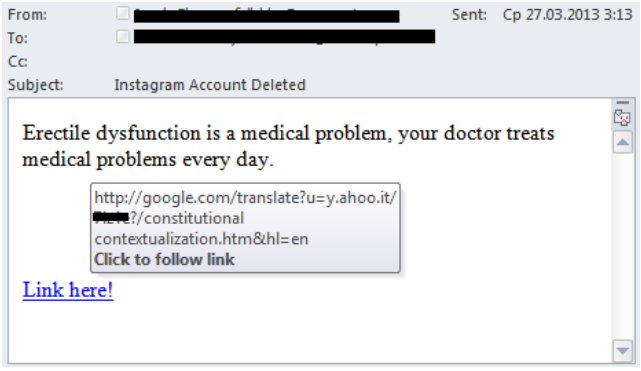
The use of legitimate services

In Q1 2013, we registered a mass mailing which contained standard advertising for male medications, and found the following tricks were being used:

1. The heading “Instagram Account Delete” is a typical example of social engineering. To attract the user’s attention the scammers raise the alarm about a potential problem with a popular online service. If the recipient has an Instagram account, he is likely to open the email rather than immediately delete it.

2. The actual address to which the malicious link leads is simultaneously masked by two legitimate methods. Firstly, the spammers used the Yahoo URL shortening service and then processed the subsequent link through Google Translate. This service can translate web pages in the user-specified link and generate its own link to that translation. The combination of these techniques makes each link in the mass mailing unique and furthermore the use of the two well-known domains adds "credibility" to this link in the eyes of the recipient.

On top of that, in order to further confuse the recipient, the spammers ended the link with a senseless request consisting of random words: «? / Constitutional contextualization».



Spammers often use shortening services. They do this, first of all, to try and bypass spam filtering, making the link in every email unique. Secondly, the use of shortening services does not impose additional costs on the scammers, unlike purchasing domains or hacking legitimate sites. On the other hand, major shortening services try to monitor the content of the websites to which they redirect users and quickly block malicious links.

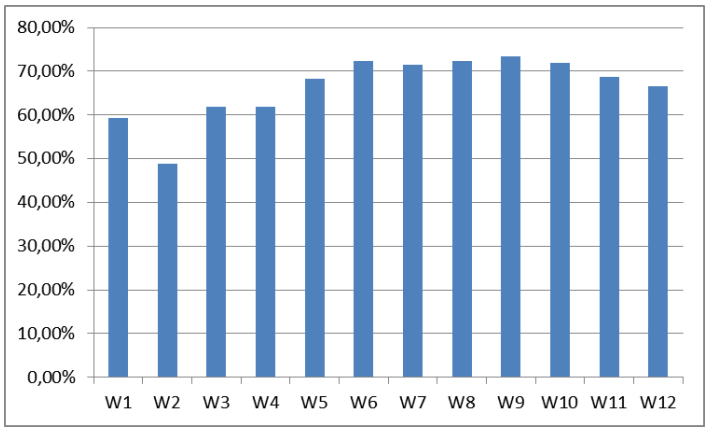
The return of "white text"

In the first quarter of 2013, spammers resumed the use of the once-popular method of creating background noise known as "white text". This method involves adding random pieces of text (this quarter they were sections of news reports) to the email. These insertions are in light gray font against a gray background and are separated from the main text of the ad with a lot of line breaks. The scammers expect content-based spam filters to regard these emails as newsletters and, besides, the use of random news fragments makes each email unique and thus difficult to detect.

Statistics

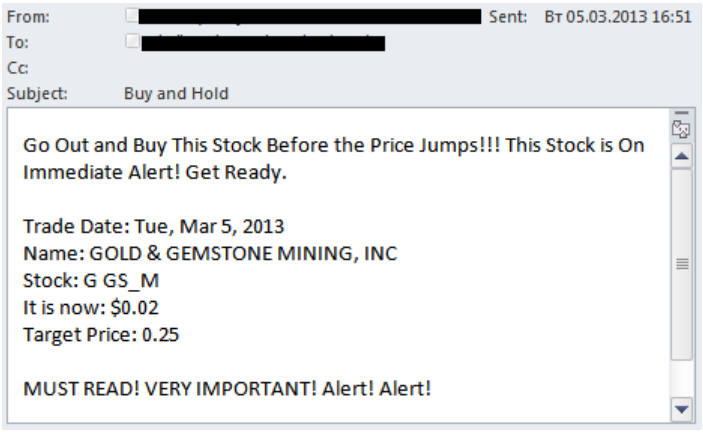
The share of spam in mail traffic

In Q1 2013, the level of spam in mail traffic fluctuated noticeably and finally averaged 66.55%, an increase of 0.53 percentage points compared to Q4 2012.



Proportion of spam in mail traffic in Q1 2013

One of the major mass mailings of Q1 used the fraudulent “pump and dump” scheme. This is a form of manipulation in the stock market when spammers buy shares of small companies and boost stock prices spreading false positive information about the status of these companies in their mass mailings and then selling the shares at the new, higher prices. Due to this mass mailing, the first week of March took the record for the quarter (73.4%)


From: [redacted] Sent: Вт 05.03.2013 16:51
To: [redacted]
Cc:
Subject: Buy and Hold

Go Out and Buy This Stock Before the Price Jumps!!! This Stock is On Immediate Alert! Get Ready.

Trade Date: Tue, Mar 5, 2013
Name: GOLD & GEMSTONE MINING, INC
Stock: G GS_M
It is now: $0.02
Target Price: 0.25

MUST READ! VERY IMPORTANT! Alert! Alert!

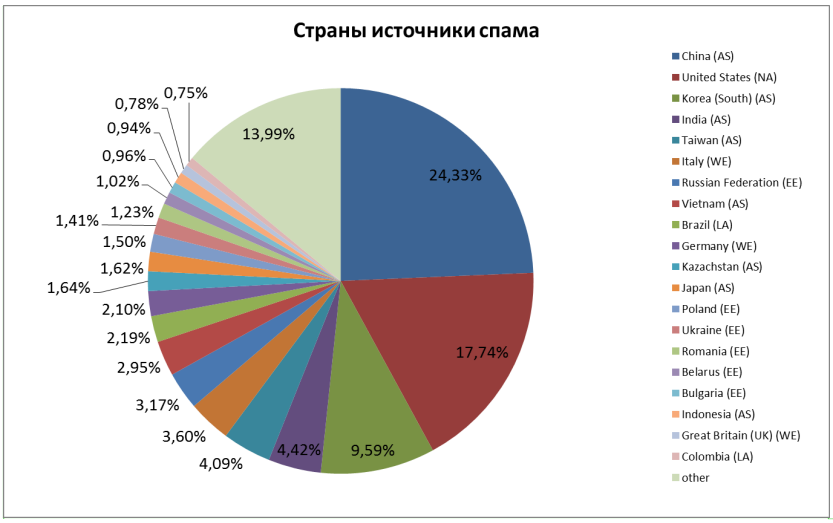
Share-related spam has fallen away from its peak in 2006-2007 and had virtually disappeared from spam flows for several years, only occasionally surfacing since then. Interestingly, when this type of spam was at the height of its popularity, the mass mailings were also very intensive. The whole point of this sort of scam is to do things as quickly as possible, within 2 or 3 days, before the bluff is called. The more emails the fraudsters can spread within this short period of time, the more potential victims will buy the shares.

Tatyana Makarova 4/30/13 5:37 PM
Comment: Link in russian

Sources of spam by country

In Q1 2013 China (24.3%) and the US (17.7%) remained the most active spam distributors. South Korea came third with 9.6% of all distributed spam.

Interestingly, the spam originating from these countries targets different regions: most Chinese spam is sent to Asia while junk mail from the US is mainly distributed in North America, i.e. its major part can be considered internal spam. Unsolicited messages from South Korea, meanwhile, go chiefly to Europe.



Andrew Potts 4/30/13 6:04 PM
Comment: Kazakhstan, not Kazachstan. I'm sure I make this correction on every spam report.

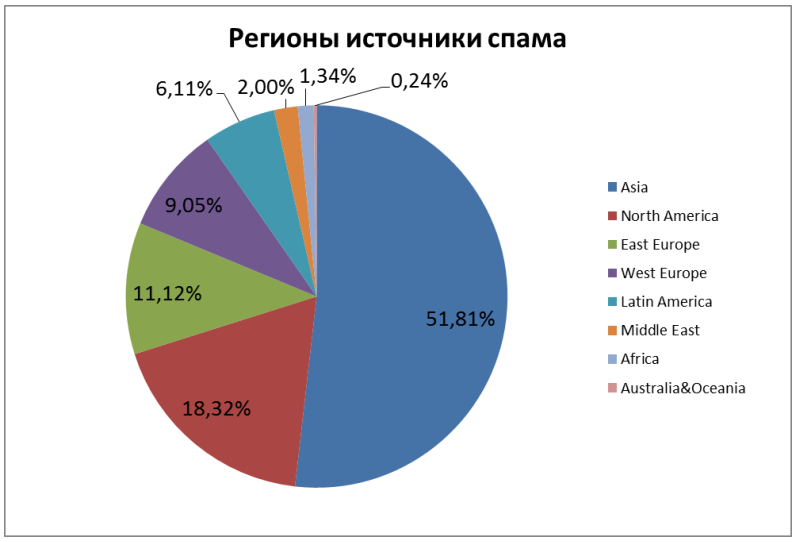
Sources of spam by country in Q1 2013

Brazil dropped from 5th to 9th place as its share halved compared with the end of 2012. This was because at the end of the year Brazil internally closed TCP port 25, which had been the default port for outgoing SMTP traffic. This is the port through which most of the spam from infected computers leaves the country. The closure of 25 TCP is standard practice for Internet providers, but in this case providers were acting on higher instructions.

The Top 5 also included India (4.4%), which was 3rd in the previous quarter, and Taiwan, which doubled last year's score and climbed from 10th to 5th place. Russia (3.2%) produced 1.2 percentage points more spam climbing one place to 7th.

Sources of spam by region

Asia remained the leading source of spam by region, spreading 51.8% of all spam worldwide. It is followed by North America with 18.3% of junk mail distribution.

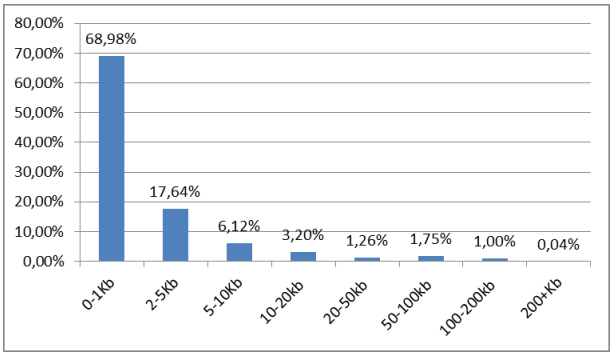


Sources of spam by region in Q1 2013

The share of spam originating from Eastern Europe grew, reaching 11.1%. Although the Top 10 included only one Eastern European country – Russia – 50% of the countries ranked 11-20 came from this region.

Latin America dropped out of the top 20 altogether thanks to a decline in activity from Brazil, Peru and Argentina.

The size of spam emails

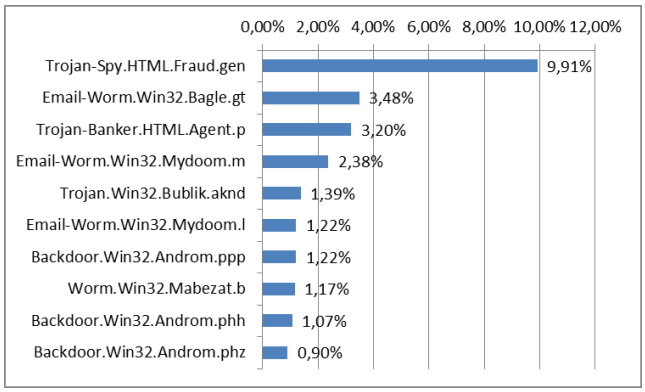


The size of spam emails in Q1 2013

In the first quarter of 2013, spam emails were generally quite small (1 KB or less). Small messages allow spammers to send more emails with less traffic consumption. Additionally, short phrases that change completely from message to message make these emails unique, confusing spam filters.

Malicious attachments in email

The percentage of emails with malicious attachments grew 0.1 percentage points from the previous quarter, averaging 3.3%.



The Top 10 malicious programs spread by email in Q1 2013

In Q1 2013, Trojan-Spy.html.Fraud.gen remained the most widespread malicious program in email traffic. This malicious program appears in the form of HTML pages imitating the registration forms of well-known banks or e-pay systems. These are used by phishers to steal user credentials for online banking systems.

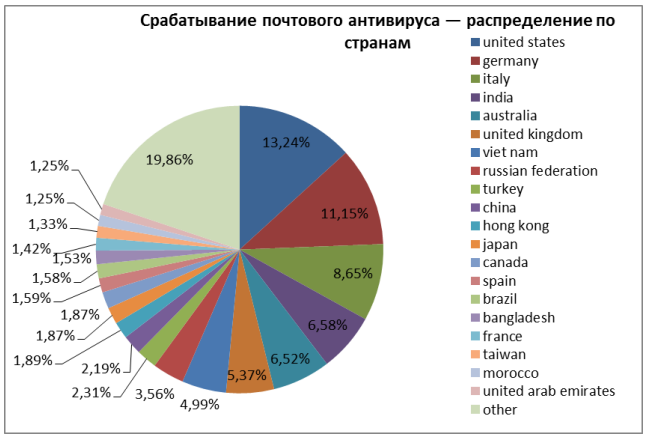
The Bagle family of worms came second. In addition to the main functionality of a mail worm, which is to self-proliferate to addresses in the victim's address book, worms in the Bagle family can also download other malicious programs onto a user's computer.

It was followed by Trojan-Banker.HTML.Agent.p. Like Fraud.gen, this malicious program is executed as an HTML page with a registration form allegedly from a financial organization or some other type of online service.

In addition to old mail worms constantly circulating on the Internet, the Top 10 malicious programs spread by email in Q1 2013 also included Trojan.Win32.Bublik.aknd and a few backdoors of the Androm family.

Bublik harvests user passwords for FTP, email service credentials and certificates from infected computers. It can scour forms in Mozilla Firefox and Google Chrome in search of saved logins and passwords before forwarding the data it finds to malicious users.

This family of backdoor programs allows malicious users to secretly control an infected computer, for example, to download and launch other malicious files which then send various data from the user's computer, etc. In addition, many computers infected by backdoors become part of a botnet. In most cases the backdoors of the Androm family were distributed in fake emails sent allegedly on behalf of Booking.com, DHL, British Airways, etc. The same method has been used in the past to distribute programs belonging to the ZeuS/Zbot family.



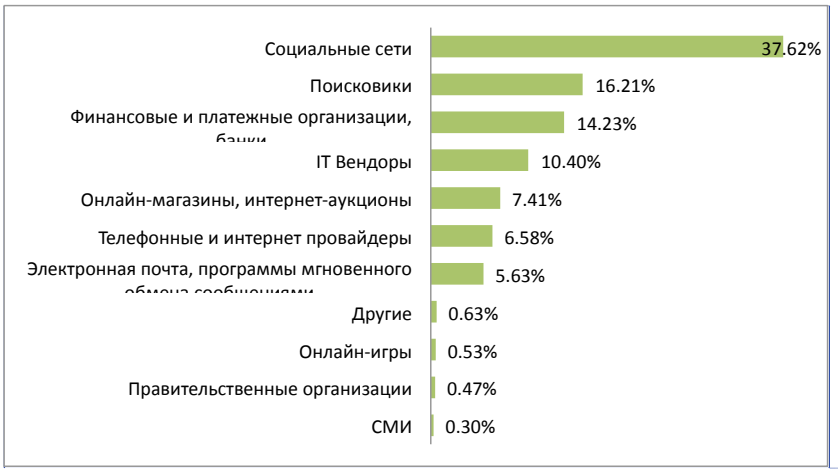
Distribution of email antivirus detections by country in Q1 2013

The US (13.2%) and Germany (11.2%) remained the countries where the majority of email antivirus detections were registered. Their total contribution accounts for a quarter of all malicious emails. Italy (8.7%) came third this quarter though usually it doesn't even make it into the Top 10. However, in February Italy was intensively targeted by Trojan-Banker.HTML.Agent.p, which saw it come first in February's Top 10.

The percentage of spam detected in the other Top 10 countries remained almost unchanged.

Phishing

In Q1 2013, the share of phishing emails in total email traffic decreased 4.25 times compared to the previous quarter and averaged 0.004%.



Tatyana Makarova 4/22/13 12:13 PM

Comment:

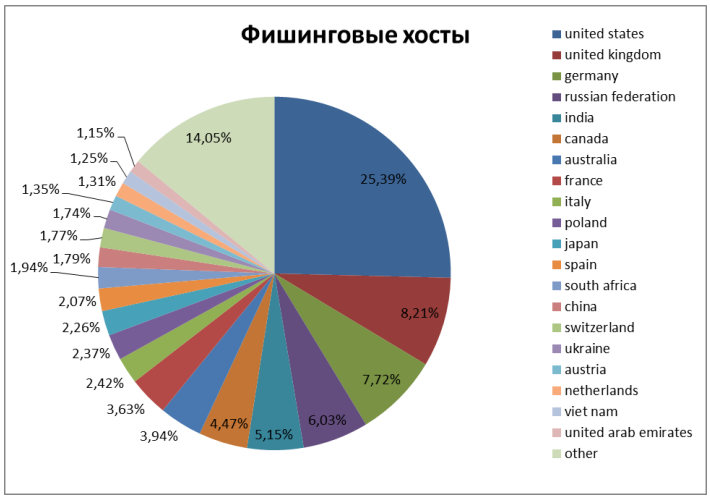
Social networking sites
Search engines
Financial and e-pay organizations and banks
IT vendors
Online stores and e-auctions
Telephone an Internet service providers
Email and IMS
Other
Online games
Government organizations
Mass media

The distribution of the Top 100 organizations targeted by phishers, by category in Q1 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.

Social networking sites continued to bear the brunt of phishing attacks (37.6%), with the fraudsters actively imitating Facebook and LinkedIn notifications. Search engines (16.2%) came second, mostly because the owners of the search engines also offer many other services including virtual disk space, email, social networking sites, etc. One account is often the key to all services, so search engines are very attractive for cybercriminals.

Financial and e-pay organizations (14.2%) were in third place. Noticeably, unlike Social networking sites, where the majority of attacks fall on one or two organizations, the distribution of attacks on banks is more even: a huge number of different banks are targeted, from big, internationally known names to small local services.



The distribution of phishing site hosting by country in Q1 2013

In the first quarter of 2013 the US (25.4%) topped the rating of countries which host phishing sites. The UK (8.2%) and Germany (7.7%) occupied 2nd and 3rd places respectively. They are followed by Russia (6%). India (5.2%) completed the Top 5.

Interestingly, the Top 10 countries which host the majority of phishing sites also included Canada (4.5%) and Australia (3.9%). These two countries are considered quite safe in terms of cybercrime and the amount of spam originating from them is 1% or less.

Conclusion

In 2012 the amount of spam dropped steadily throughout the year. In Q1 2013 the percentage of unsolicited correspondence in mail traffic fluctuated from month to month, although the average figure remained practically unchanged from the previous quarter. We expect the share of spam to maintain its present level in the future or grow slightly due to the recent increase in the number of multimillion mass mailings.

Spammers keep trying to draw the users' attention to their messages: they use famous names, world events or fake notifications from popular online resources. Many emails contain links to malicious programs, including exploits. We would like once again to remind users not to click links in emails even if the sender seems familiar to you. It is much safer to enter the address in the browser manually.

The most active spam distributors – the US and China – are unlikely to change in the near future unless the command centers of botnets in these countries are closed down. In the first quarter of 2013 the leading three sources of spam worldwide included South Korea, which mostly sent spam to European users.

In Q1 2013, the most common malicious attachments spread via email were programs designed to steal users' logins and passwords. The fraudsters were especially keen on Trojans that targeted user credentials for online banking systems. In addition, many mass mailings contained links leading to exploit kits, with Blackhole being the most popular.