Spam and Phishing in the First Quarter of 2016

Bitdefender®

Author

Alexandra Gheorghe - Securiy Specialist

Technical information provided courtesy of Bitdefender researchers Adrian Miron and Adrian Popescu.

Introduction into the current spam landscape

When it comes to persistent Internet pests, spam is a veteran. Seemingly innocent, this old threat now delivers one of the newest, and most dangerous payloads yet – crypto ransomware.

In the first three months of 2016, spam email containing attached files increased by 50%, according to data from Bitdefender Antispam Lab. Partially responsible for the large volumes of infected email attachments is the proliferation of crypto-ransomware. Locky and Petya, two emerging ransomware threats, are aggressively hunting for victims via massive spam campaigns spreading Word documents disguised as invoices and Dropbox links to malicious applications.

Petya ransomware

Spam features of the quarter

A closer look at the spam landscape of Q1 2016 reveals a few notable tendencies.

- Spammers are deploying clever tactics like whaling and spear-phishing. While attacks in recent years have primarily targeted the masses, scammers are now focusing on specific targets such as corporate accounts. They are crafting ingenious emails to persuade company employees to download malicious files or transfer money to foreign bank accounts.

- In terms of cyber-threats propagating through spam emails, ransomware attacks have risen with 5% in the United States, reinforcing its position as most targeted country.

- Voluminous spam campaigns, especially dating email mailshots, are being sent in multiple languages at the same time.

- An analysis of phishing in different industries reveals that file-sharing and cloud storage services have taken the lead as the most targeted sector. Spammers are impersonating popular content sharing services to spread infected links and host fraudulent websites.

Malicious email attachments

In the first quarter of 2016, downloaders were the most commonly blocked malicious files. VBS Downloader, Upatre, Andromeda and JS Downloader were among the downloaders most identified and blocked by Bitdefender antispam filters. This type of software camouflages in malicious attachments and installs additional malware on systems.

"Attackers are separating the task of infecting victim systems from the actual exploitation," Adrian Popescu, Team Lead at Bitdefender Labs says. *"Downloaders are a simple way to spread new malware as they help reduce the risk of the actual payload being detected by AV and network-detection systems. Evasion is done through the deployment of a wide set of schemes that obfuscate or encrypt communication channels".*

Once executed, a downloader contacts its command-and-control (C&C) server or servers via C&C channels. After receiving download instructions, it establishes the download channel(s) for loading malware via the network.

UK users were particularly urged to install downloaders (53.6%), significantly more than users from the US, France, Denmark and Australia.

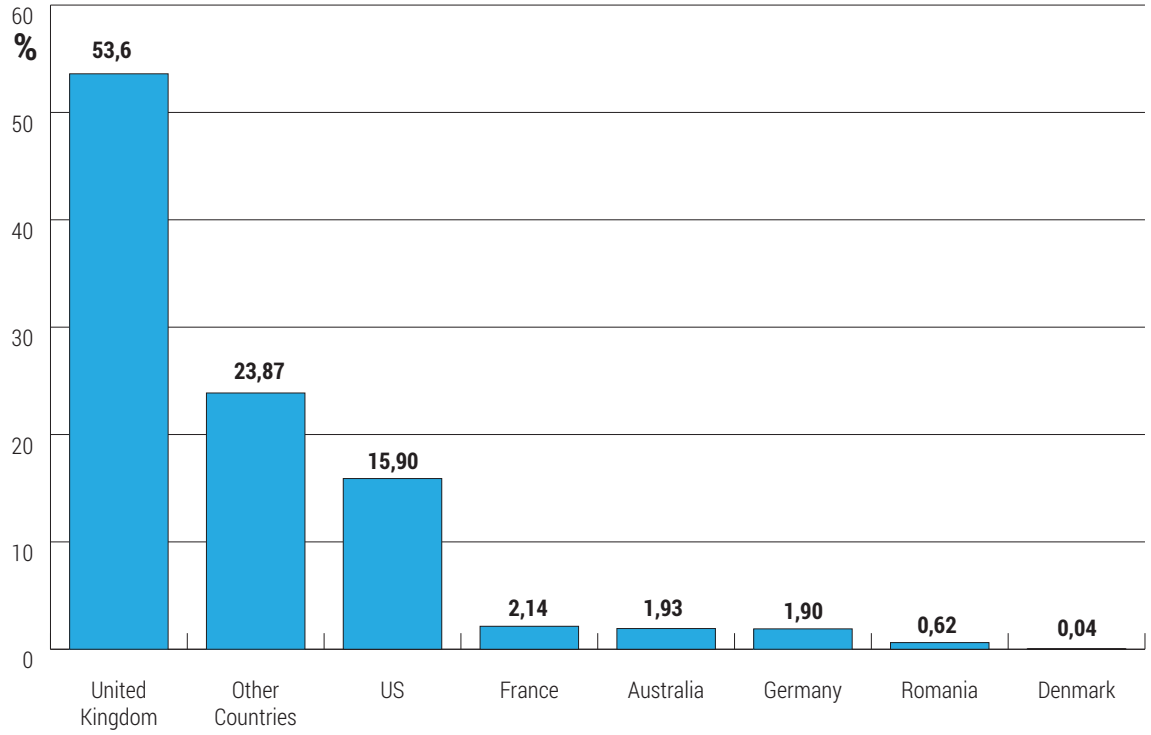


Fig. 1 Propagation of downloaders per country

Ransomware accounts for **15.5%** of all measured e-mail antivirus detections. That means that globally, one in seven email attachments delivered in Q1 contained some form of ransomware.

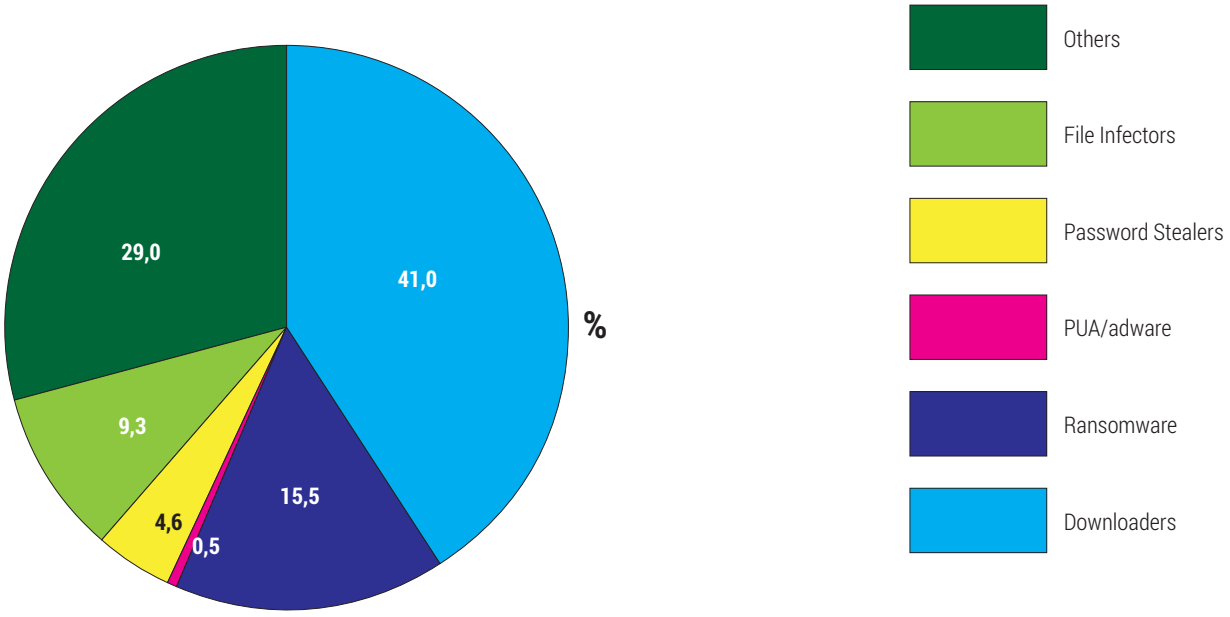


Fig. 2 Main categories of attached files by malicious content

The US remains a top target for cyber-extortionists as **26.6%** of all ransomware email messages detected in Q1 were aimed at US users. This represents a 5% increase compared with 2015, as Bitdefender reported at the end of the year.

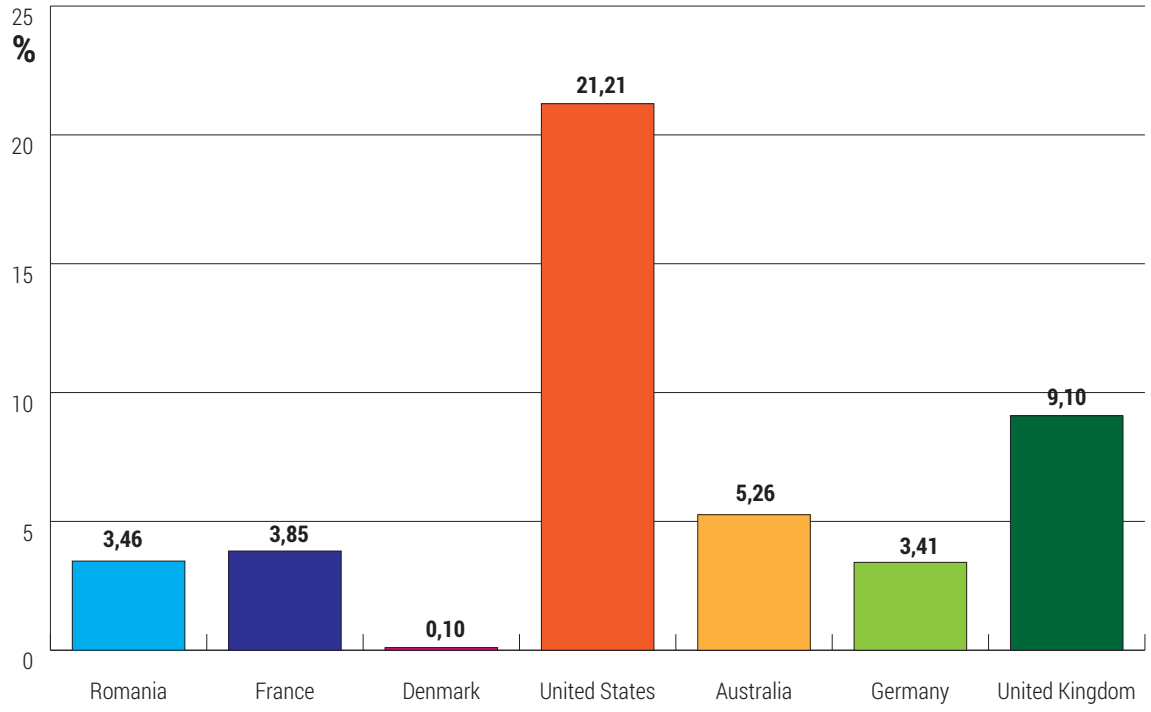


Fig.3 2015 global ransomware statistics on most representative countries, according to Bitdefender

Message themes

Pharma and diet-themed messages are still among the most popular baits (44.2%), followed by dating spam (11.6%) and malware-infected spam (8.4%).

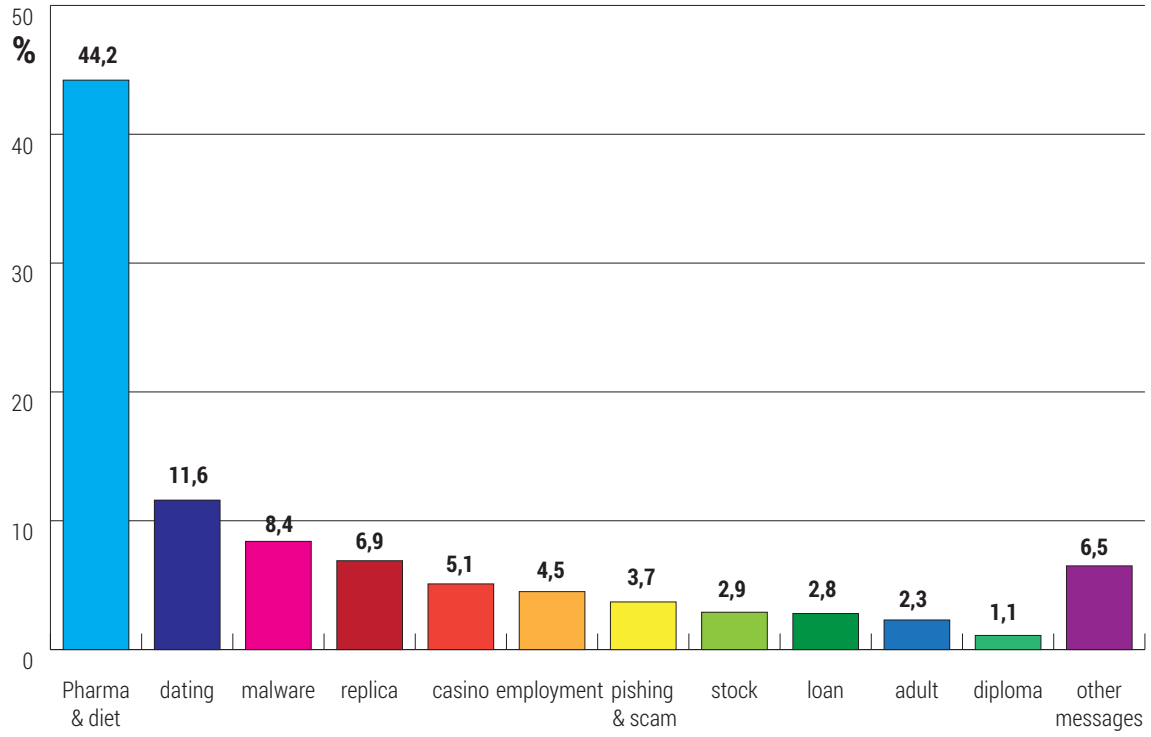


Fig.4 Spam by message theme

Types of files

Looking at the extensions of the attached files, Bitdefender researchers observed that compressed files are the most common type of files .Zip, .rar, .z, .7z, .gz, .gzip, .bz2, .jar, .arj, .ace, .cab make up 75% of all the unique file extensions. They are followed by Microsoft Word files (13.2%) and Excel files (5.4%).

"Random generated strings are used as comments in the malicious code, resulting in slightly different attached files from one email sample to another in the same spam wave", says Adrian Miron, Head of Antispam Lab at Bitdefender. *"This shows attackers are looking to avoid spam filters."*

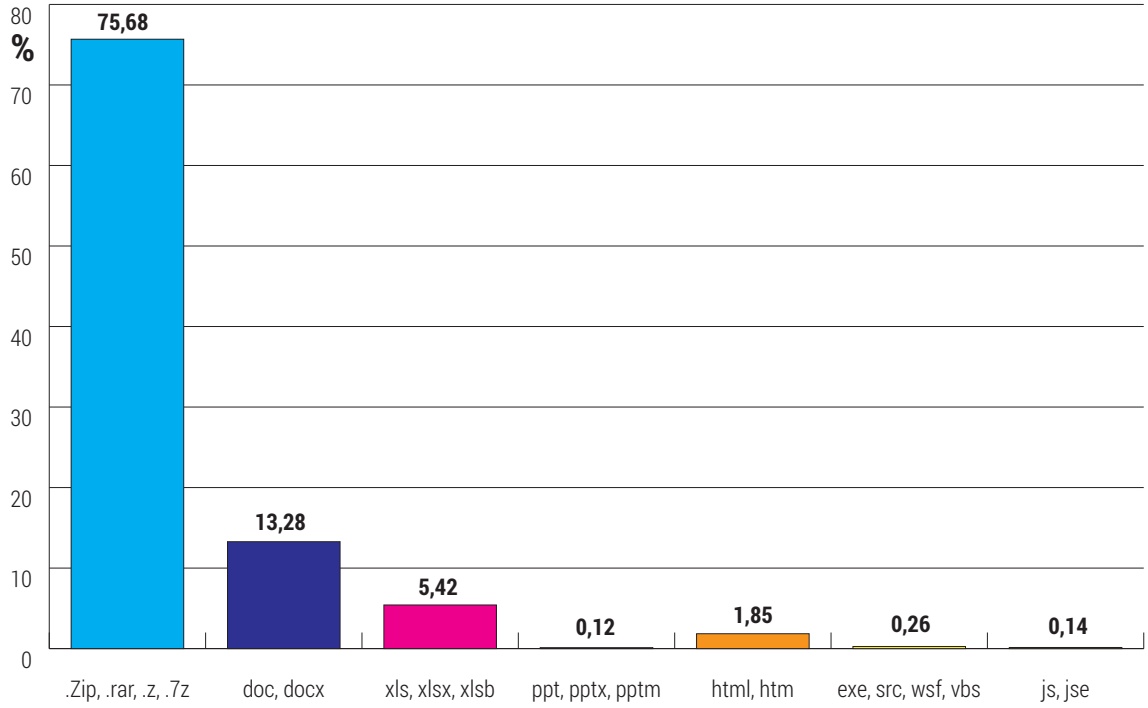


Fig.5 Percentage of unique file types attached to spam emails

Example of email spam with .zip file attachment

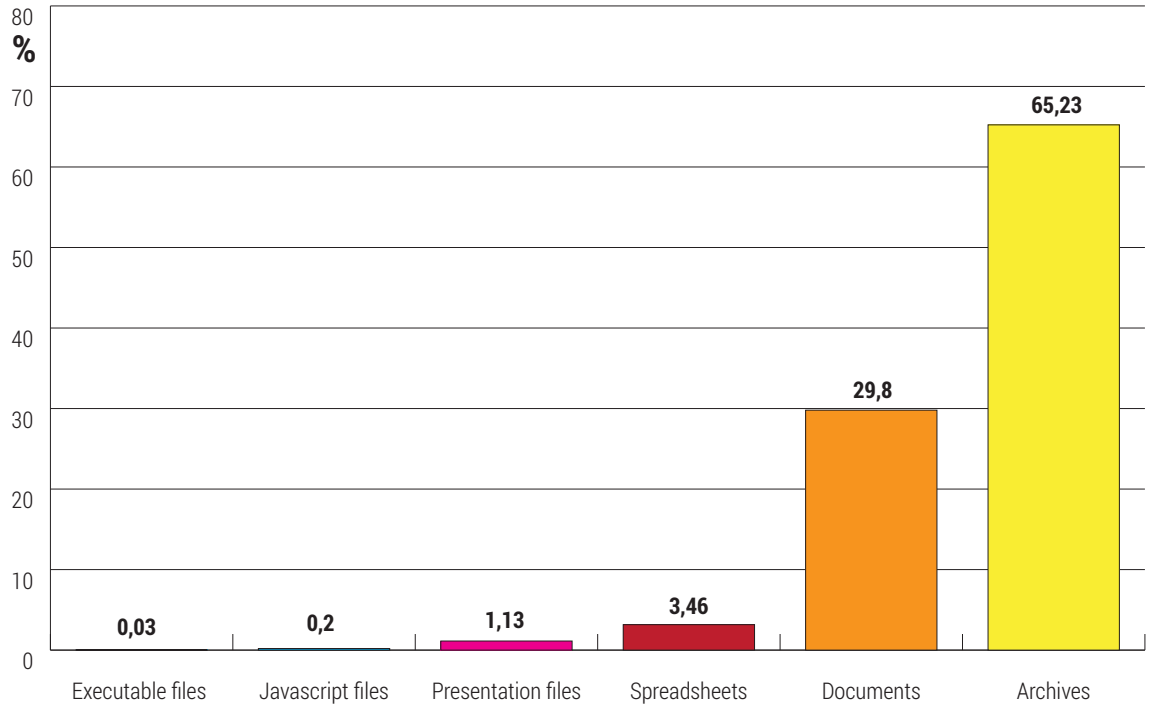


Fig.6 Percentage of file types attached to spam emails

95% of the compressed (.zip) files reveal files written in JavaScript. The spam email usually contains a .zip file attachment containing only one JavaScript file, but there are also exceptions.

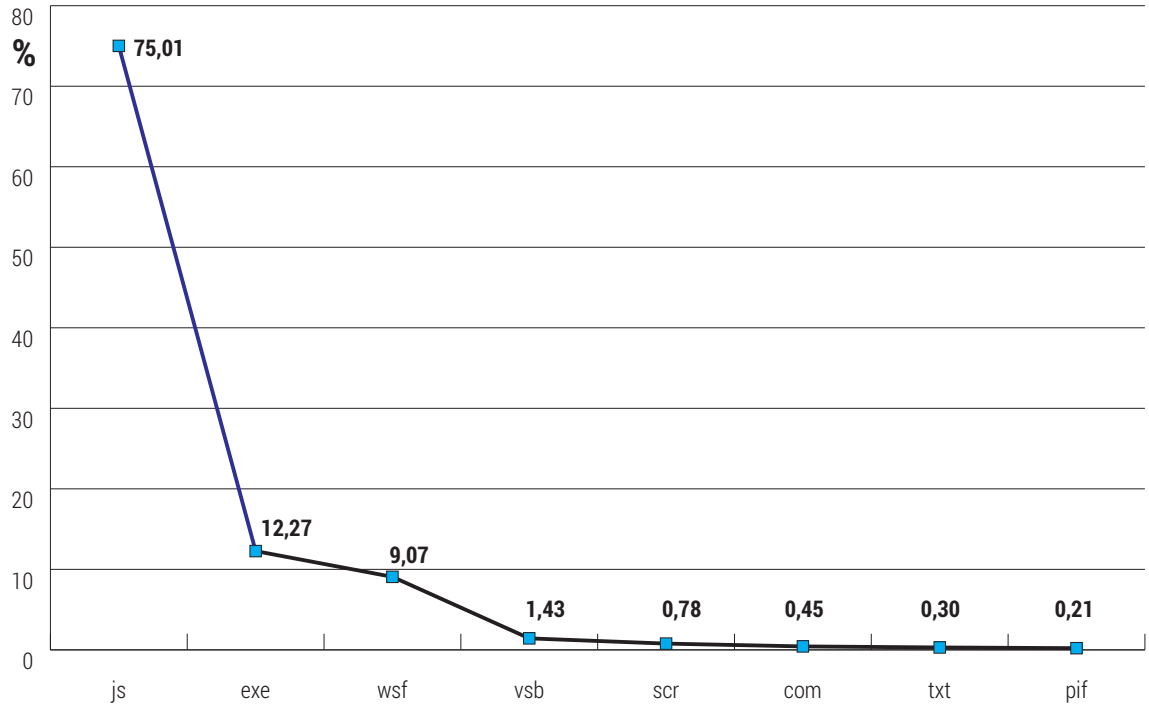


Fig.7 Percentage of file types attached to spam emails

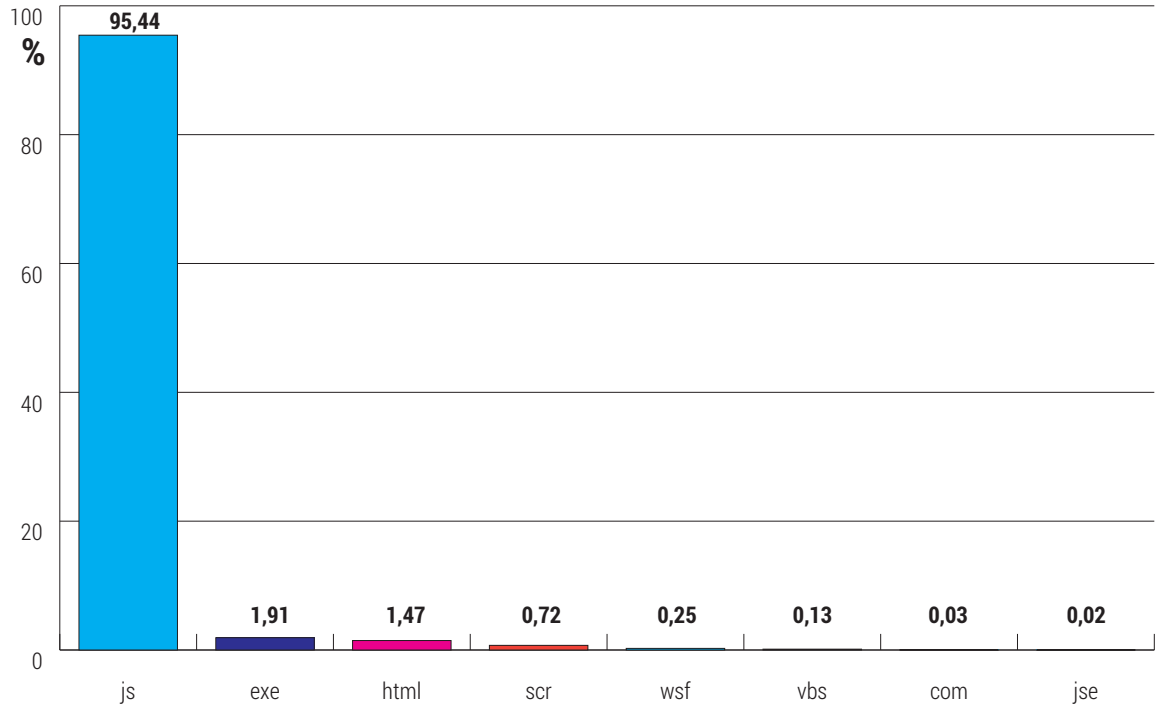
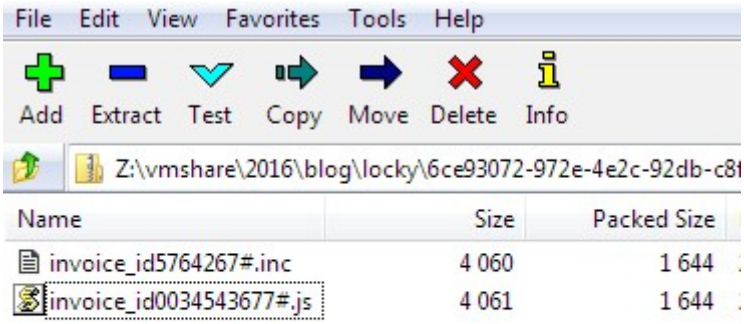


Fig.8 Percentage of extensions found in compressed files

"We are currently seeing significant volumes of JavaScript attachments being spammed out," Miron says. ***"It's not unexpected as JavaScript is widely supported by websites and browsers, and can be easily obfuscated to hide malicious code."***



Locky ransomware spreading via extracted .js files

Spam Languages

Most spam messages are delivered in English, Russian and Asian languages.

"We have seen some big botnet-generated campaigns (spreading malware, dating, and employment spam) translated into European languages, yet English remains the most-used spam language," Miron says.

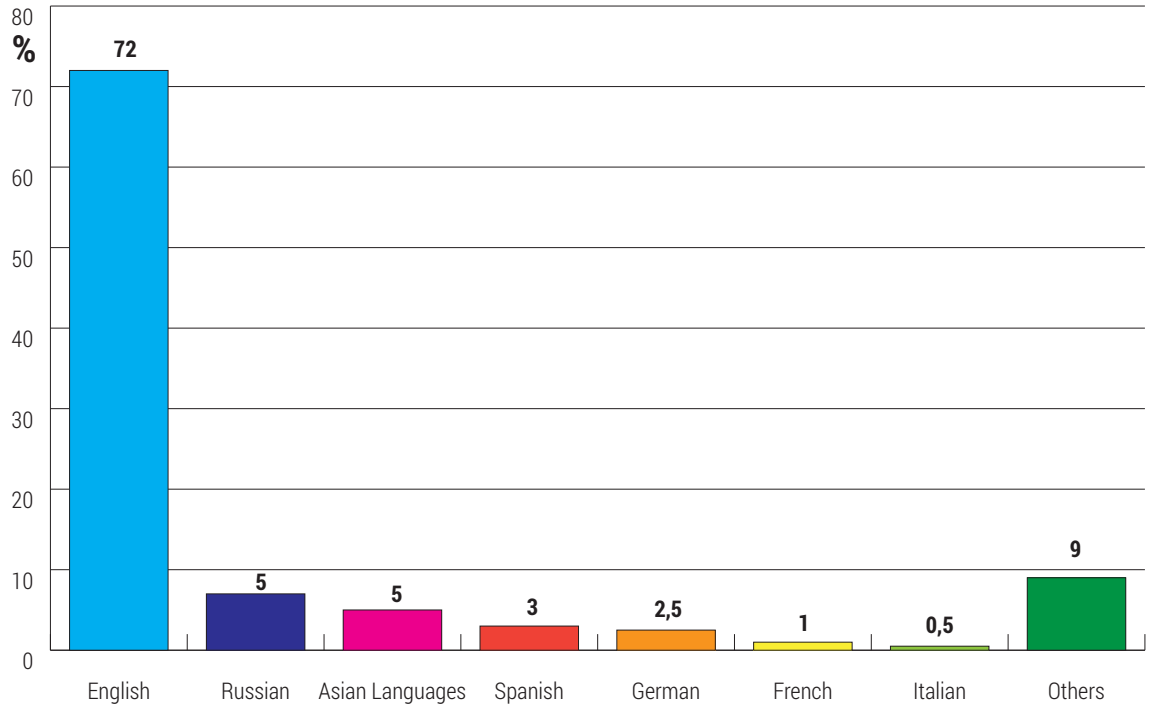
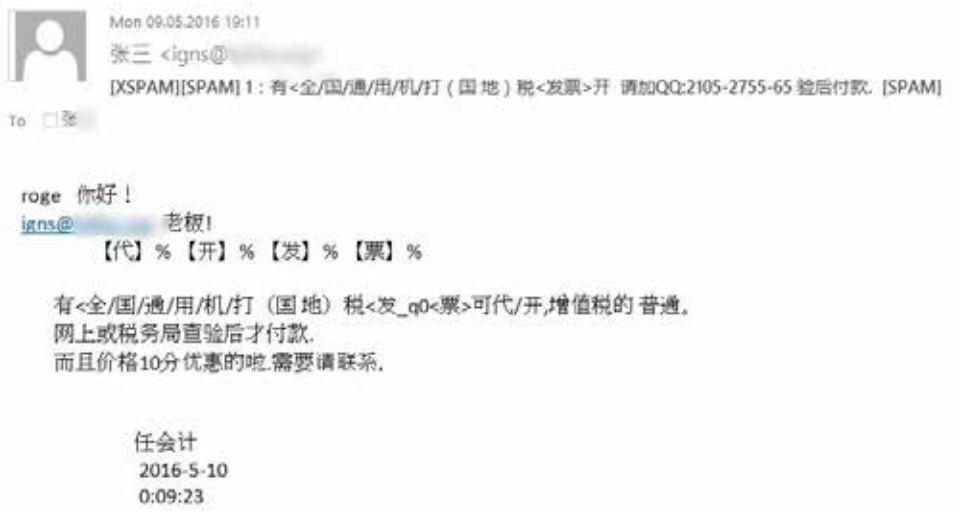


Fig.9 Percentage of top spam languages

.com remains the top domain source of spam emails, generating **19.9%** of all spam carrying URLs seen in 2016. It is closely followed by more exotic TLDs like .top, .xyz, .biz and .tk.

Usually, the target or redirecting domains used by spammers remain live for one month, at most. However, we have also seen more resilient domains – appearing in spam campaigns for almost a year.


Mon 09.05.2016 19:11
张三 <igns@
[XSPAM][SPAM] 1：有<全/国/通/用/机/打（国地）税<发票>开 请加QQ:2105-2755-65 验后付款. [SPAM]
To 张

roge 你好！
igns@ 老板!
【代】%【开】%【发】%【票】%

有<全/国/通/用/机/打（国地）税<发_q0<票>可代/开,增值税的普通。
网上或税务局查验后才付款.
而且价格10分优惠的啦.需要请联系.

任会计
2016-5-10
0:09:23

Example of email spam in Chinese

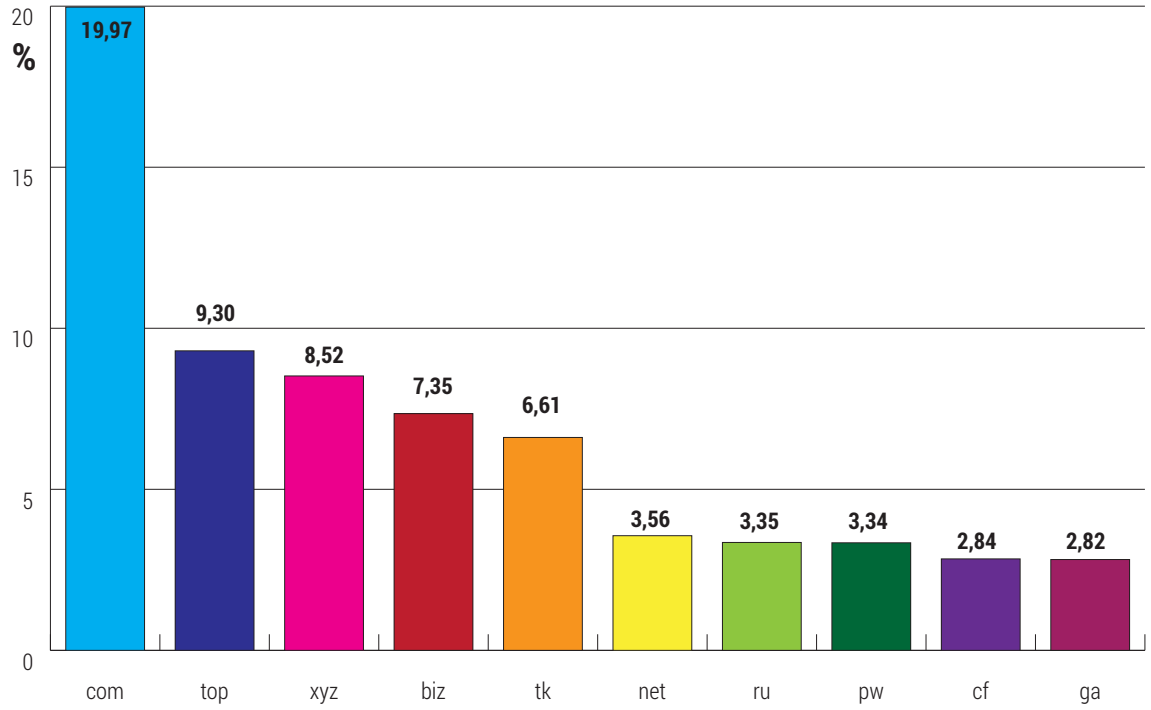


Fig.10 Percentage of top spam-generating domains

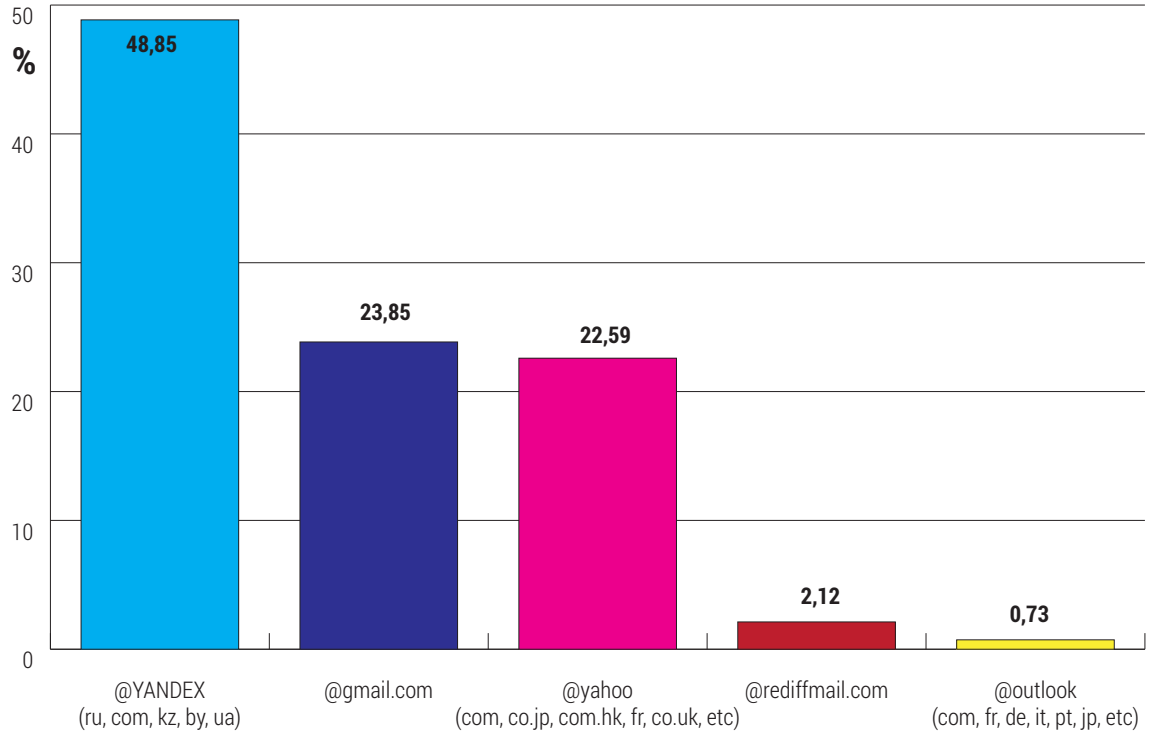


Fig. 11 Percentage of webmail domains by unique samples

Part of the email addresses registered on the above domains are used in dating, lottery and employment spam and Nigerian scams.

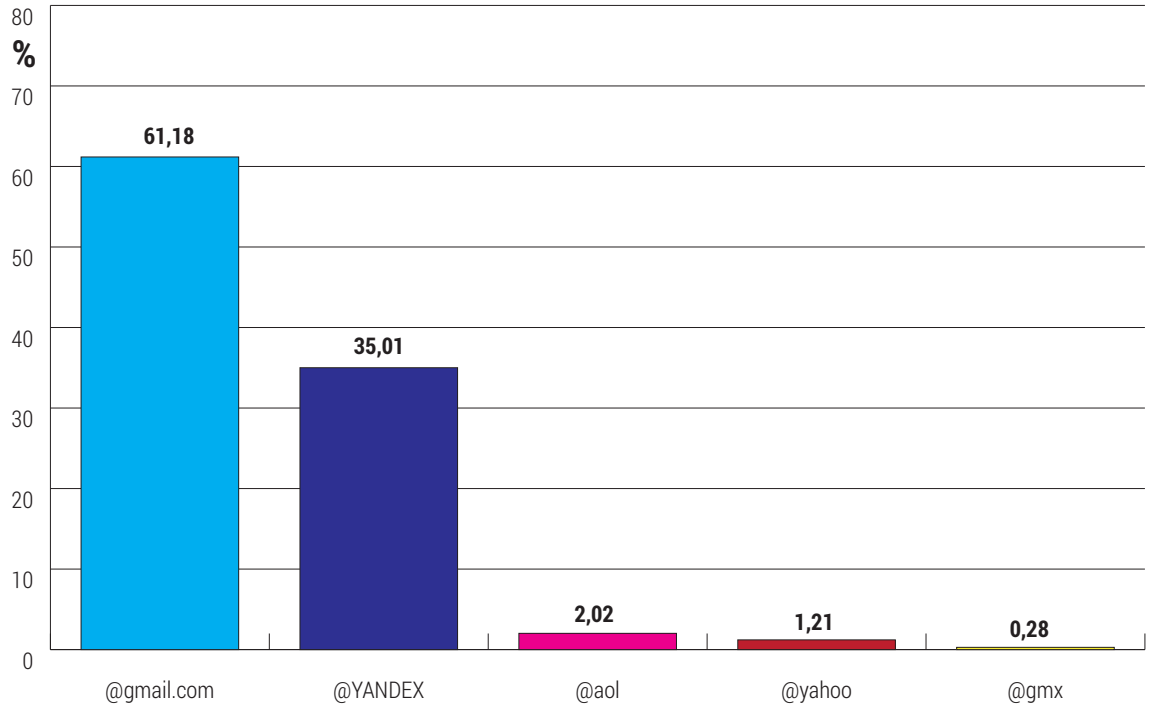


Fig. 12 Percentage of webmail domains by volume

Phishing overview

In the first quarter of 2016, phishing schemes involving file-sharing and cloud storage services have soared. Cloud-based file distribution services have taken the lead as the most-targeted sector of the first quarter of the year, surpassing the retail and payment industries, the traditional favorites of hackers.

One in five malicious URLs uses a file-sharing service to deliver malicious payloads to users. The typical infection flow goes like this: the user receives a genuine-looking email that advises users to click on an embedded link to view an attached document. The link redirects the user to a phishing page hosted on the provider's domain. The page asks for the user's credentials, then captures and sends the data to cyber-criminals over SSL.

The most impersonated companies are PayPal, Apple and Google.

"Phishing remains a highly effective attack vector that is responsible for an increasingly significant percentage of data loss incidents affecting both end users and companies," says Adrian Popescu, Team Leader at Bitdefender's Antimalware Lab.

Email impact on business environment

Email spam has evolved from a mere nuisance to a full-blown IT nightmare, becoming one of the biggest threats to enterprise security.

Vital for corporate operations, email communications can expose a company to time-consuming disruptions that harm productivity and, most importantly, to data loss as a result of ransomware targeting employees, key loggers, data-grabbing spyware, spear-phishing and other email-based threats.

To effectively combat the rising threats and meet the increasing demands of corporate regulations, companies are looking for the most comprehensive email security solutions to protect their enterprises.

Fighting spam

"Spam is changing continually, both in quality and quantity, and to protect inboxes and networks an anti-spam solution must be able to keep up with these changes" (Virus Bulletin).

When it comes to detecting sophisticated spam, the classic approach based on local content filtering is no longer 100% effective.

Bitdefender combines the latest antispam technologies with cloud computing to provide outstanding protection and instantly react to new spam outbreaks. Cloud-based intelligence complements Bitdefender's anti-spam engine to analyze pieces of email information such as SMTP connection information (sender IP address/sender domain), email header information and content information (text fingerprints, URLs, phone numbers, images, attachments).

Machine learning algorithms are also a key in proactively analyzing huge amounts of data and blocking outbreaks within seconds.

Bitdefender is:

- The only antispam product to have achieved the VBSpam certification in all 42 Virus Bulletin tests ever performed.
- The only recipient of 12 consecutive VBSpam+ awards.

To qualify for VBSpam+ certification, security solutions need to combine a spam catch rate of 99.50% or higher with no false positives.

Spam trends for 2016

The first months of 2016 set the stage for a broader and more complex threat landscape than ever before. Spam carrying malicious attachments is expected to remain at a high level, as cyber-criminals will continue to use email as a primary vector to break into organizations and compromise systems. Banking Trojans and ransomware will remain a major concern.

Spear-phishing will likely increase in volume, as high-profile data breaches expose the private details of government officials, heads of state, politicians and key members of organizations.

Major world events, such as the 2016 presidential US elections and the European Soccer Championship, will be featured in spam messages. Fear over terrorist threats will also be leveraged to trick users into supporting different humanitarian causes or actions.

And of course, "classic phishing schemes" show no sign of aging or stopping. For instance, dating scams will extend to lesser known social media platforms and will keep using US-based phone numbers for contact.

About Bitdefender

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.

B