СПАМ И ФИШИНГ ВО ВТОРОМ КВАРТАЛЕ 2015

Татьяна Щербакова,
Мария Вергелис,
Надежда Демидова

ОГЛАВЛЕНИЕ

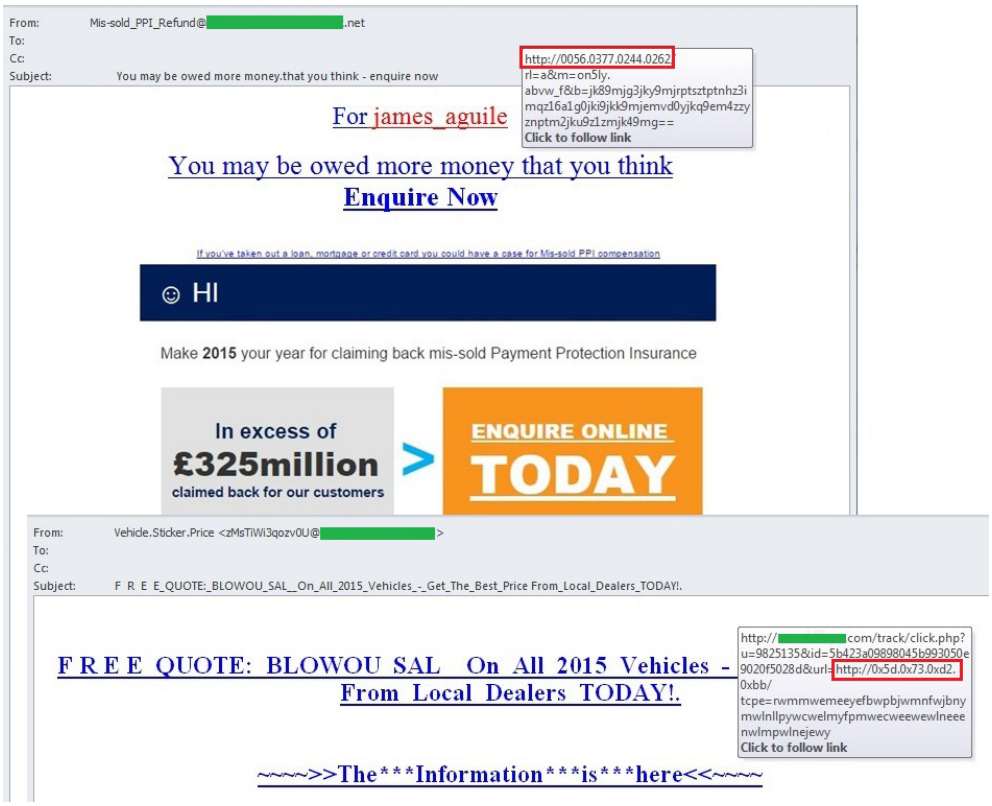
СПАМ: ОСОБЕННОСТИ КВАРТАЛА

Зашумление доменов

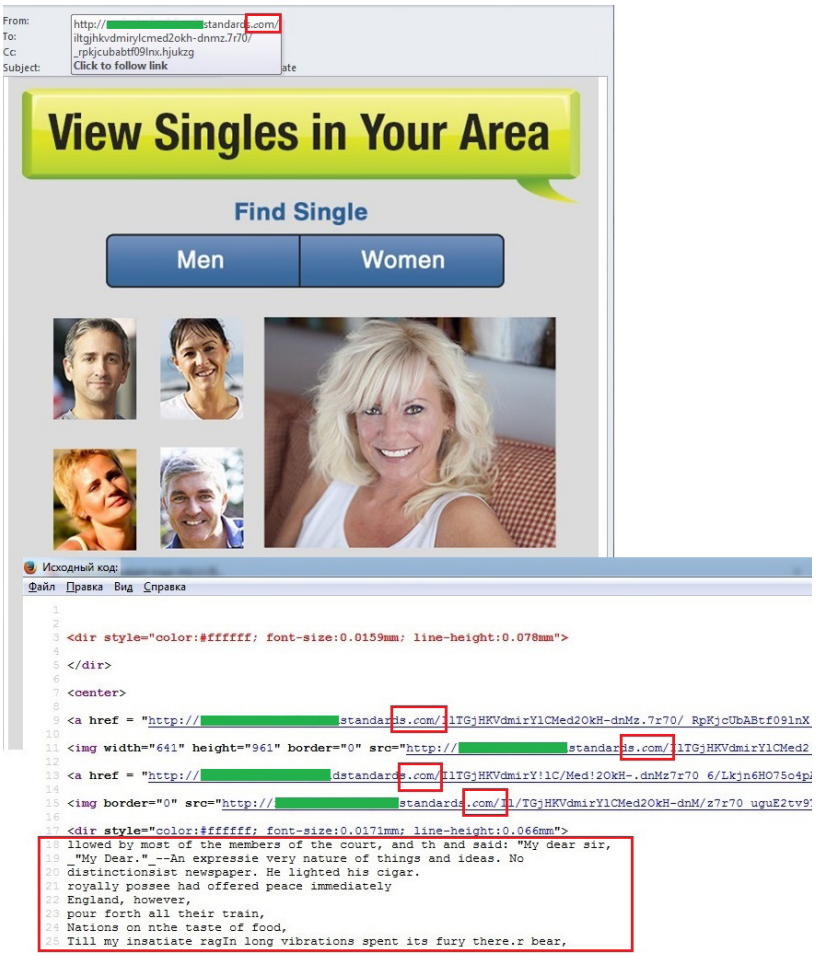
Мы уже подробно анализировали ситуацию с большим количеством новых доменных зон, а также массовым созданием в этих зонах спамерских доменов, предназначенных специально для проведения нелегитимных рассылок. Дальнейший анализ спам-рассылок показал, что спамеры делают ставку не только на огромное количество новых доменов, которые они могут менять внутри даже одной тематической рассылки, но также и на способы их текстовой реализации. Так, в прошлом квартале мы фиксировали различные случаи зашумления доменов в ссылках, использованных для перехода на спамерские ресурсы, а также случаи обфускации кода в HTML-структуре рассылаемых сообщений.

- Mis-sold PPI's Affected Millions. See if you Are Due a Refund {http://0000000000000271.0000000000000000053.0000000000000000000000000000317.00000000000000000214/
- You May Qualify for a Reverse Mortgage {http://0x45a27efd/
- http://0x6C.0x3B.0x9.0xBC/
- Dr. Oz suggests this weight loss ingredient {http://0242.0336.0xC122/604/3363.jpg}
- {http://0xC2.2188528?HTslccs2oLdsqX4YiqsMjccixlFC4j3Vn5bt3oDM4ccsH9br9OGokdlDmXGo3JLBkSN72fz10JlS7rC0UaTKePJ0PbUwamjNd4q1rVUlYyRDVsjNTmz84PD-wlPXr1HZQiLlP7wQn6w5vPLdps8MwOxs9bl8zoYm_B05f5g1B8UYneruL7K9REGkF5brqhr2M9f_ccqnZUN2r5xq4gfDgKxUUrwl0r1E_0LsG-pHqH9hurTD

Во многих рассылках в записи ссылок на рекламные ресурсы вместо домена спамеры использовали IP-адреса сайтов. Но при этом давали не прямой, а видоизмененный IP-адрес: представляли его в восьмеричной или шестнадцатеричной системе счисления, добавляли в начало произвольное количество нулей. От этого сам IP-адрес не меняется, зато увеличивается количество возможных вариантов его записи (вариативность внутри одной спам-рассылки), что, как надеются спамеры, должно ввести в заблуждение антиспам-фильтр. Такие альтернативные способы записи IP-адресов спамеры использовали как в прямых ссылках, так и в зашумленных редиректами.



Зашумляли спамеры и имена доменов. Например, записывая имя с использованием одновременно заглавных и строчных символов (NEEDHosT.niNjA), а также используя несколько разных кодировок в HTML-структуре сообщений. Спамеры пытались скрывать свои домены, меняя один из символов в имени доменной зоны на тот же из другой кодировки, либо на похожий на него. Выглядело это, например, так - domainname.*c*om, domainname.cⓞ.

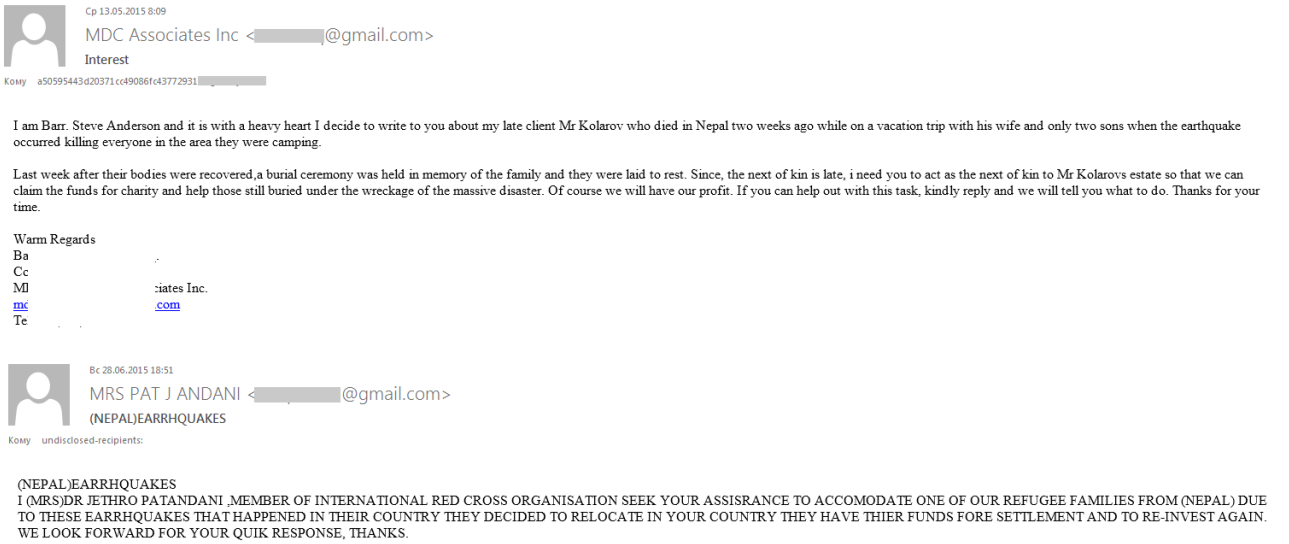


При этом нередко в одном письме использовалось сразу несколько методов зашумления: альтернативная запись IP-адреса или искажение названия домена, а также традиционное заполнение тела письма бессмысленным «мусорным» текстом с целью полностью завуалировать спамерскую тематику письма.

Мировые события в нигерийском спаме

Во втором квартале нигерийские письма были посвящены землетрясению в Непале, выборам президента Нигерии и Олимпиаде в Рио-де-Жанейро. Трагические события, широко освещаемые в мировых СМИ, из в года в год используются мошенниками для обмана пользователей, а придуманные ими сюжеты практически не меняются.

В письме от имени адвоката, клиент которого якобы погиб в Непале, мошенники просят получателя сыграть роль родственника погибшего и за вознаграждение помочь в получении наследства. в других рассылках мошенники распространяли письма от имени различных организаций с просьбой оказать помощь пострадавшим от землетрясения. Например, в одном из писем «представитель Красного Креста» просил получателя помочь в размещении семьи беженцев, которая решила переехать в другую страну и там вложить имеющиеся у них средства.



Ср 13.05.2015 8:09
MDC Associates Inc <[redacted]@gmail.com>
Interest
Кому a50595443d20371cc49086fc43772931[redacted]

I am Barr. Steve Anderson and it is with a heavy heart I decide to write to you about my late client Mr Kolarov who died in Nepal two weeks ago while on a vacation trip with his wife and only two sons when the earthquake occurred killing everyone in the area they were camping.

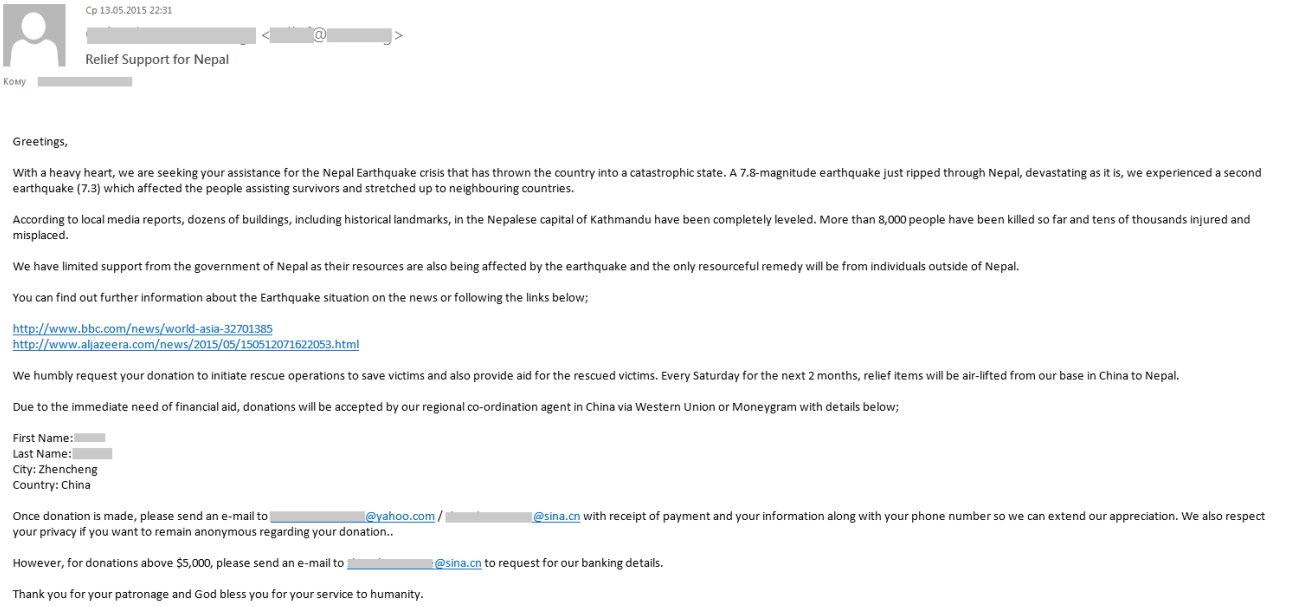
Last week after their bodies were recovered,a burial ceremony was held in memory of the family and they were laid to rest. Since, the next of kin is late, i need you to act as the next of kin to Mr Kolarovs estate so that we can claim the funds for charity and help those still buried under the wreckage of the massive disaster. Of course we will have our profit. If you can help out with this task, kindly reply and we will tell you what to do. Thanks for your time.

Warm Regards
Ba
Cc
Ml :iates Inc.
mc .com
Te

Вс 28.06.2015 18:51
MRS PAT J ANDANI <[redacted]@gmail.com>
(NEPAL)EARRHQUAKES
Кому undisclosed-recipients:

(NEPAL)EARRHQUAKES
I (MRS)DR JETHRO PATANDANI ,MEMBER OF INTERNATIONAL RED CROSS ORGANISATION SEEK YOUR ASSISRANCE TO ACCOMODATE ONE OF OUR REFUGEE FAMILIES FROM (NEPAL) DUE TO THESE EARRHQUAKES THAT HAPPENED IN THEIR COUNTRY THEY DECIDED TO RELOCATE IN YOUR COUNTRY THEY HAVE THIER FUNDS FORE SETTLEMENT AND TO RE-INVEST AGAIN. WE LOOK FORWARD FOR YOUR QUIK RESPONSE, THANKS.

В основном адреса отправителей нигерийских писем были зарегистрированы на бесплатных почтовых сервисах, даже если автором письма являлся представитель какой-либо организации, как в вышеописанном случае. Однако встречались и мошенники похитрее, которые стремились придать имени и адресу отправителя более легитимный вид. Они рассылали поддельные сообщения с просьбой сделать добровольное пожертвование для оказания помощи пострадавшим от землетрясения в Непале.



Ср 13.05.2015 22:31
[redacted] <[redacted]@[redacted]>
Relief Support for Nepal
Кому [redacted]

Greetings,

With a heavy heart, we are seeking your assistance for the Nepal Earthquake crisis that has thrown the country into a catastrophic state. A 7.8-magnitude earthquake just ripped through Nepal, devastating as it is, we experienced a second earthquake (7.3) which affected the people assisting survivors and stretched up to neighbouring countries.

According to local media reports, dozens of buildings, including historical landmarks, in the Nepalese capital of Kathmandu have been completely leveled. More than 8,000 people have been killed so far and tens of thousands injured and misplaced.

We have limited support from the government of Nepal as their resources are also being affected by the earthquake and the only resourceful remedy will be from individuals outside of Nepal.

You can find out further information about the Earthquake situation on the news or following the links below;

http://www.bbc.com/news/world-asia-32701385
http://www.aljazeera.com/news/2015/05/150512071622053.html

We humbly request your donation to initiate rescue operations to save victims and also provide aid for the rescued victims. Every Saturday for the next 2 months, relief items will be air-lifted from our base in China to Nepal.

Due to the immediate need of financial aid, donations will be accepted by our regional co-ordination agent in China via Western Union or Moneygram with details below;

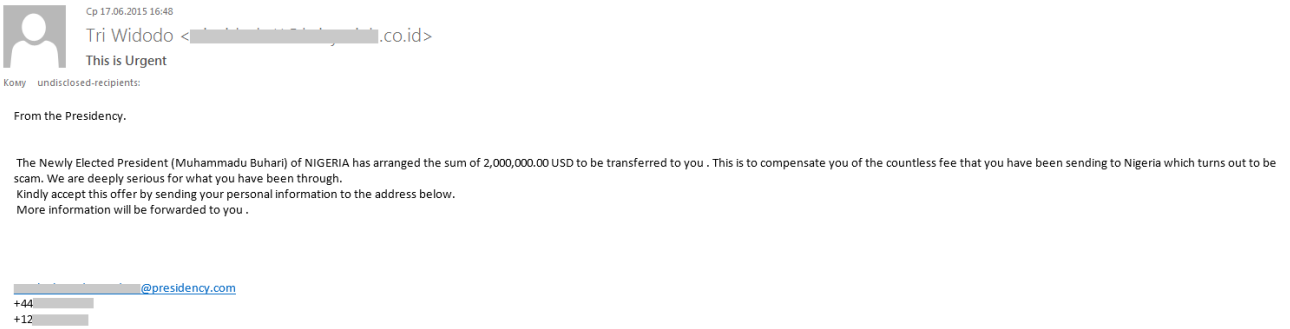
First Name: [redacted]
Last Name: [redacted]
City: Zhencheng
Country: China

Once donation is made, please send an e-mail to [redacted]@yahoo.com / [redacted]@sina.cn with receipt of payment and your information along with your phone number so we can extend our appreciation. We also respect your privacy if you want to remain anonymous regarding your donation..

However, for donations above $5,000, please send an e-mail to [redacted]@sina.cn to request for our banking details.

Thank you for your patronage and God bless you for your service to humanity.

Политические события также не остались без внимания «нигерийцев». в одной из рассылок мошенники пытались заинтересовать получателя суммой в 2 млн долларов, которую новоизбранный президент Нигерии якобы готов перечислить пользователю в качестве компенсации за мошенничество, совершенное по отношению к получателю жителями его страны.



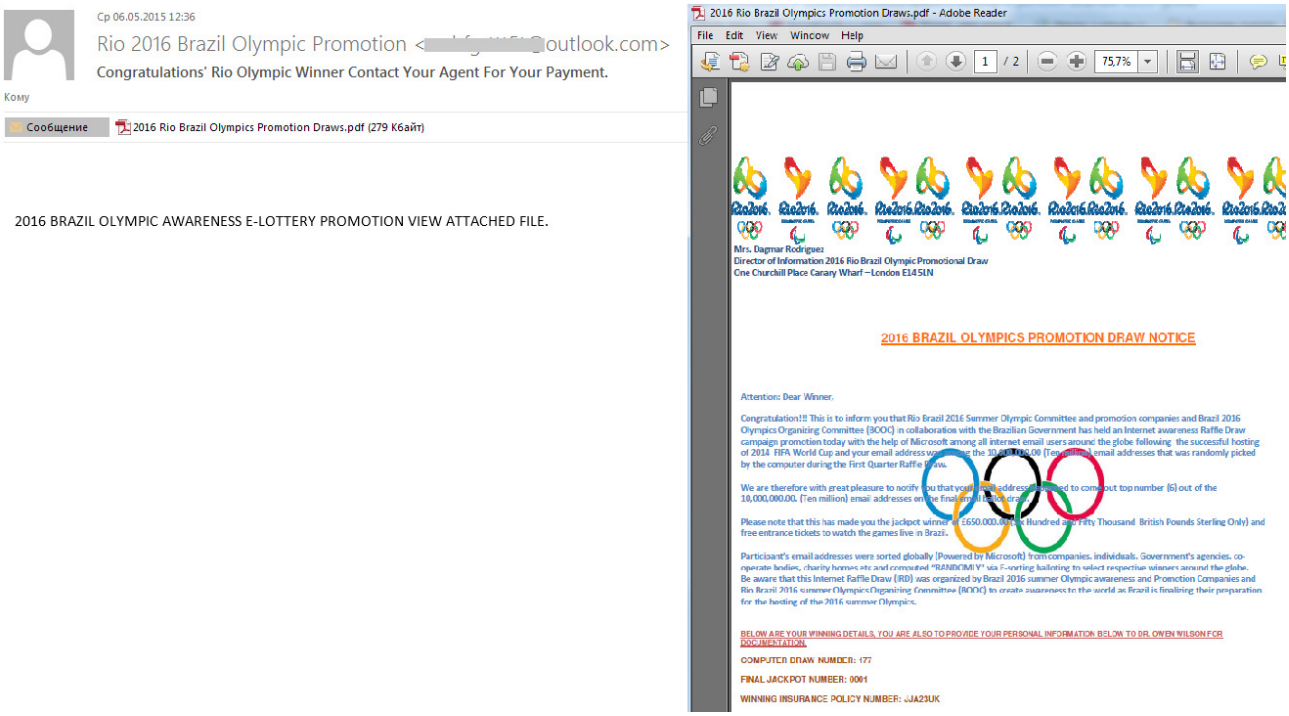
Ср 17.06.2015 16:48
Tri Widodo <[redacted].co.id>
This is Urgent
Кому undisclosed-recipients:

From the Presidency.

The Newly Elected President (Muhammadu Buhari) of NIGERIA has arranged the sum of 2,000,000.00 USD to be transferred to you . This is to compensate you of the countless fee that you have been sending to Nigeria which turns out to be scam. We are deeply serious for what you have been through.
Kindly accept this offer by sending your personal information to the address below.
More information will be forwarded to you .

[redacted]@presidency.com
+44[redacted]
+12[redacted]

До следующих Олимпийских игр в Бразилии еще далеко, однако мы уже фиксируем мошеннические уведомления о выигрыше в лотерею, посвященную популярному спортивному событию. Отметим, что большое количество подобных писем рассылалось в преддверии Чемпионата мира по футболу, упоминание Олимпиады ранее практически не встречалось. Содержание писем стандартное: лотерея была проведена официальной организацией, адрес получателя был случайно выбран из миллионов электронных адресов, для получения выигрыша необходимо ответить на письмо и предоставить указанную персональную информацию.



Ср 06.05.2015 12:36
Rio 2016 Brazil Olympic Promotion <[redacted]outlook.com>
Congratulations' Rio Olympic Winner Contact Your Agent For Your Payment.
Кому
Сообщение 2016 Rio Brazil Olympics Promotion Draws.pdf (279 Кбайт)

2016 BRAZIL OLYMPIC AWARENESS E-LOTTERY PROMOTION VIEW ATTACHED FILE.

2016 Rio Brazil Olympics Promotion Draws.pdf - Adobe Reader
File Edit View Wincow Help
1 / 2 75,7%

Mrs. Dagmar Rodriguez
Director of Information 2016 Rio Brazil Olympic Promotional Draw
One Churchill Place Canary Wharf – London E14 5LN

2016 BRAZIL OLYMPICS PROMOTION DRAW NOTICE

Attention: Dear Winner,

Congratulation!!! This is to inform you that Rio Brazil 2016 Summer Olympic Committee and promotion companies and Brazil 2016 Olympics Organizing Committee (BOOC) in collaboration with the Brazilian Government has held an Internet awareness Raffle Draw campaign promotion today with the help of Microsoft among all internet email users around the globe following the successful hosting of 2014 FIFA World Cup and your email address was [redacted] email addresses that was randomly picked by the computer during the First Quarter Raffle Draw.

We are therefore with great pleasure to notify you that your [redacted] to come out top number (6) out of the 10,000,000.00. (Ten million) email addresses on the final draw [redacted]

Please note that this has made you the jackpot winner of £650,000.00 [redacted] Hundred and Fifty Thousand British Pounds Sterling Only) and free entrance tickets to watch the games live in Brazil.

Participant's email addresses were sorted globally (Powered by Microsoft) from companies, individuals, Government's agencies, co-operate bodies, charity homes etc and computed "RANDOMLY" via E-sorting balloting to select respective winners around the globe. Be aware that this Internet Raffle Draw (RD) was organized by Brazil 2016 summer Olympic awareness and Promotion Companies and Rio Brazil 2016 summer Olympics Organizing Committee (BOOC) to create awareness to the world as Brazil is finalizing their preparation for the hosting of the 2016 summer Olympics.

BELOW ARE YOUR WINNING DETAILS, YOU ARE ALSO TO PROVIDE YOUR PERSONAL INFORMATION BELOW TO DR. OWEN WILSON FOR DOCUMENTATION.

COMPUTER DRAW NUMBER: 177

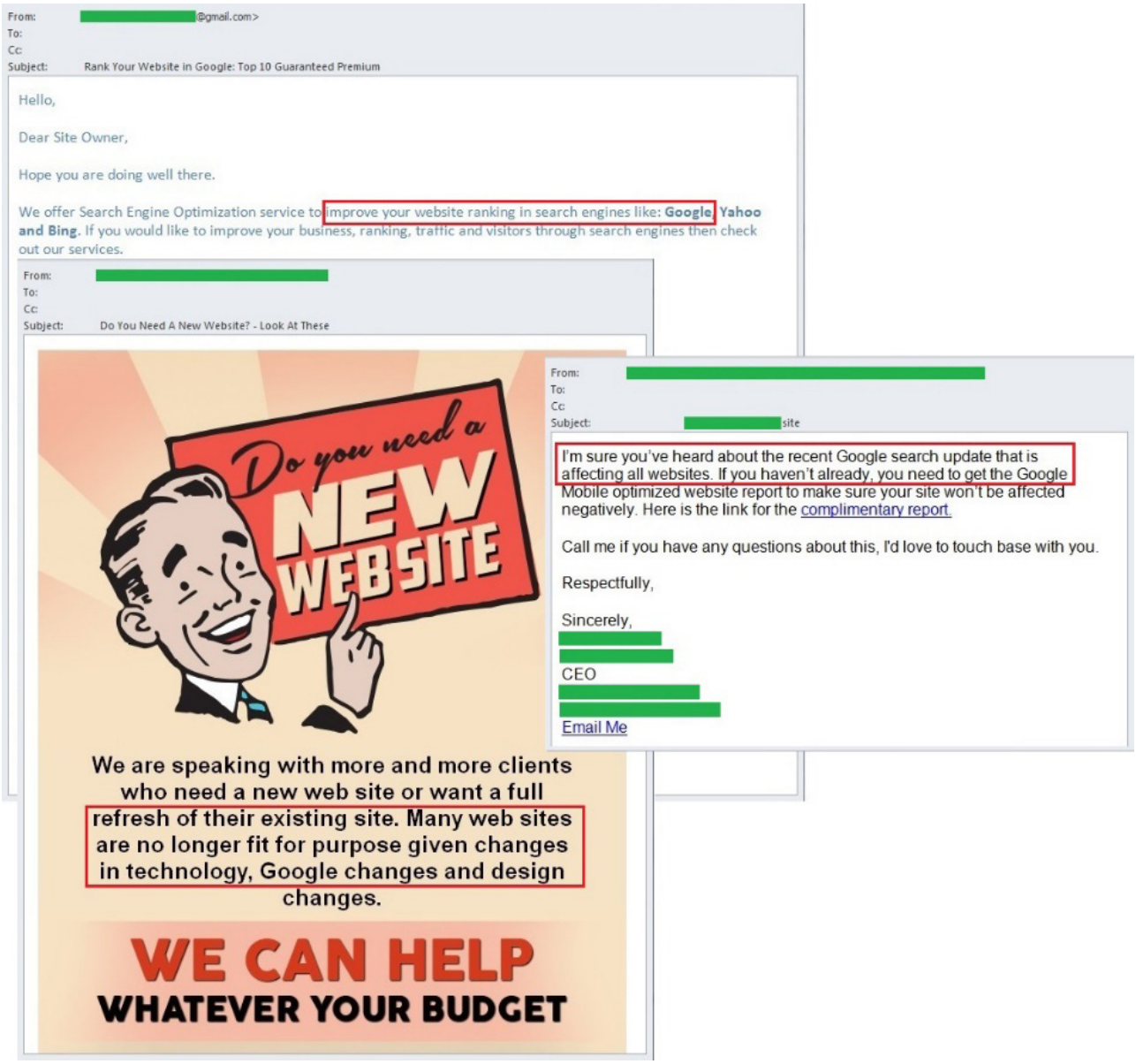
FINAL JACKPOT NUMBER: 0001

WINNING INSURANCE POLICY NUMBER: JJA23UK

Письма, в теле которых содержится только краткий текст, а подробная информация находится во вложенном файле .pdf или .doc, приобретают все большую популярность у спамеров. Это может быть связано с тем, что письмо с коротким текстом спам-фильтр с больше й вероятностью может принять за легитимное. Письма с вложенными файлами особенно опасны, поскольку пользователю придется открыть вложение, чтобы узнать содержание письма, и это может привести к заражению компьютера.

Обновления алгоритма поиска Google

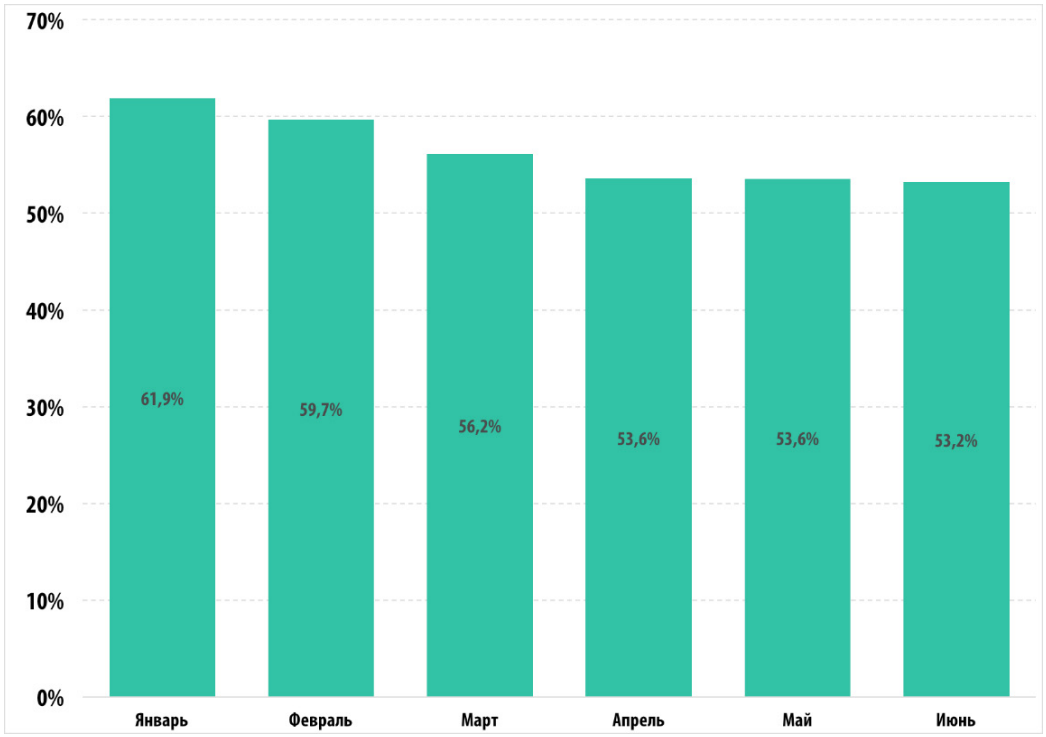
Еще одним информационным поводом квартала, так или иначе повлиявшим на тематику спама, стало очередное обновление алгоритма поиска Google Search. Оно изменило результаты мобильного поиска таким образом, что на верхние позиции стали выводиться сайты, адаптированные для мобильных телефонов.



В связи с этой новостью заметно выросло количество спама на тему SEO – поискового продвижения и раскрутки сайтов. Спамеры традиционно предлагали рекламу по созданию сайтов любой сложности и назначения, привлечению на них новых клиентов. Упор при этом зачастую делался именно на необходимость соответствия сайтов новым критериям популярной поисковой системы. Сомневающихся владельцев сайтов спамеры пугали позициями на последних страницах в результатах поиска и, как следствие, потерей большей части потенциальных клиентов.

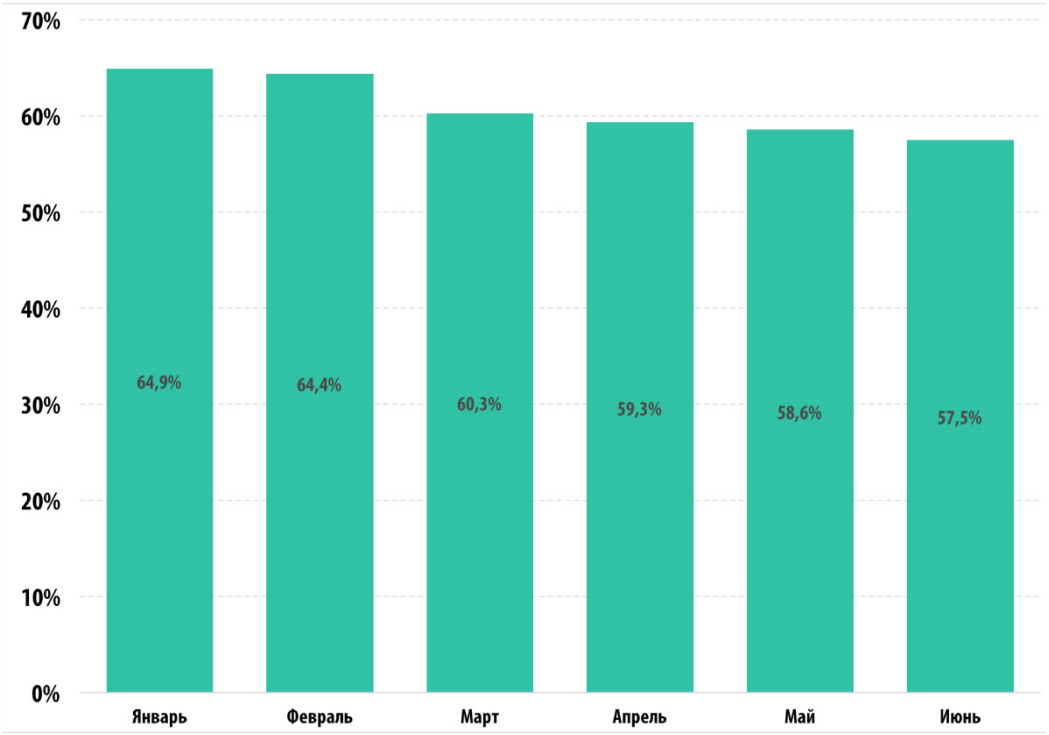
СТАТИСТИКА

Доля спама в почтовом трафике



Доля спама в мировом почтовом трафике, январь – июнь 2015 года

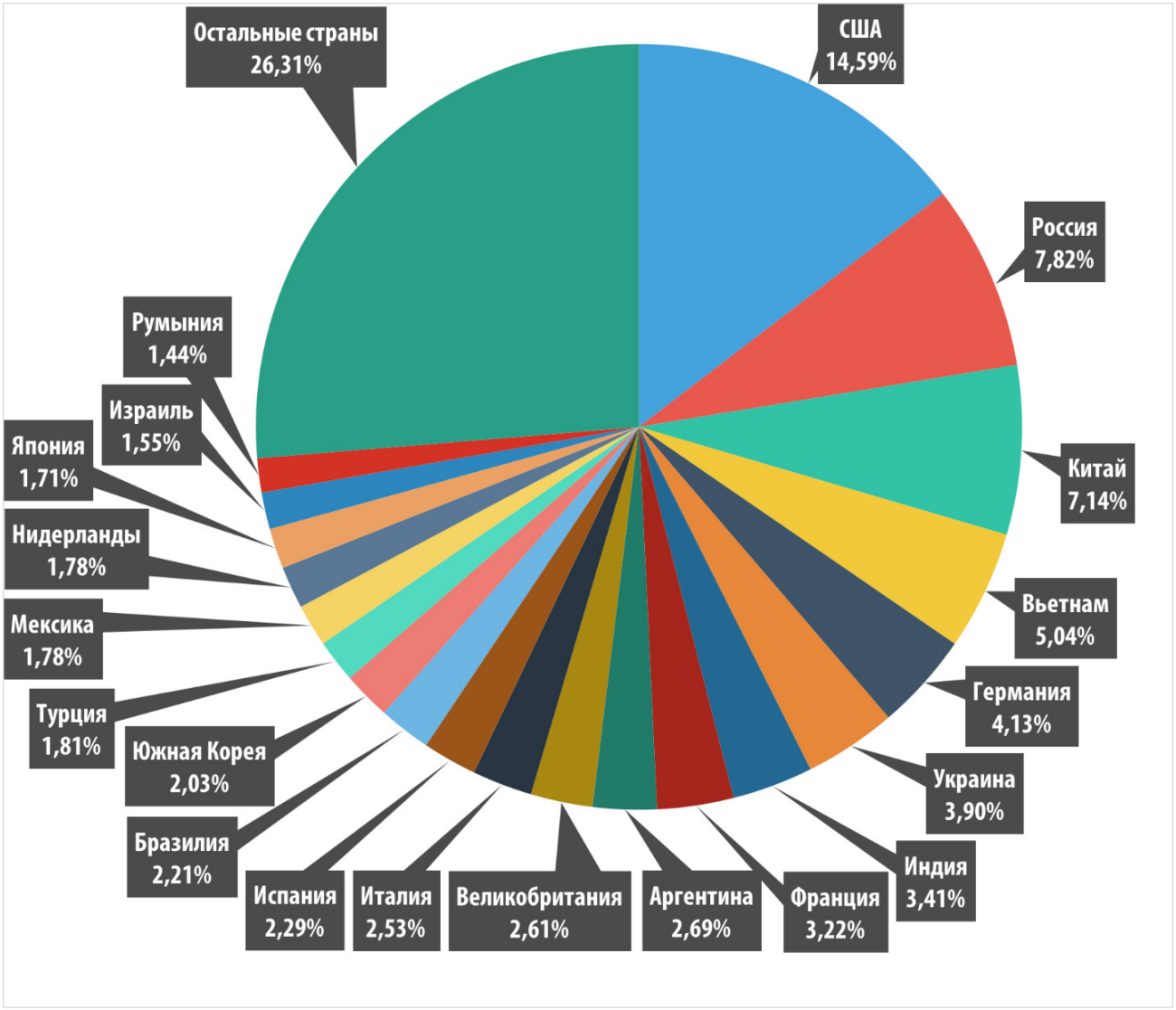
Уменьшение доли спама в мировом почтовом трафике, наблюдавшееся с начала года, почти остановилось. Во втором квартале 2015 года показатель стабилизировался в районе 53,5%, от 53,63% в апреле до 53,23% в июне.



Доля спама в российском почтовом трафике, январь – июнь 2015 года

Ситуация со спамом в российском почтовом трафике в целом повторяет ситуацию в мире. На протяжении второго квартала доля спама уменьшалась примерно на 1 п.п. месяц. Таким образом, максимальное число спамовых писем во втором квартале было разослано в апреле (59,32%), минимальное – в июне (57,47%)

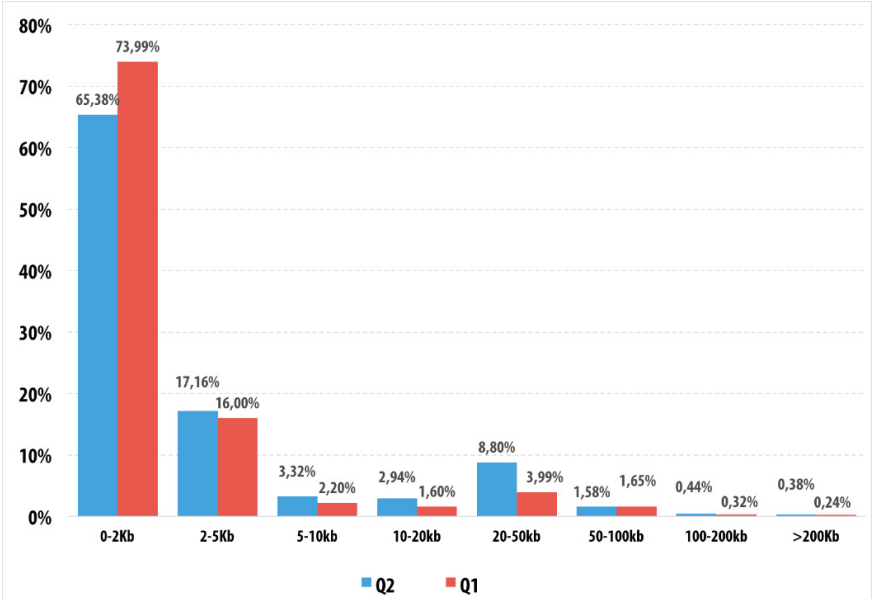
Страны – источники спама



Страны – источники спама в мире, второй квартал 2015 г.

Во втором квартале 2015 года среди стран-источников спама первые места по-прежнему занимали США (14,59%) и Россия (7,82%), а на третью строчку, вытеснив Украину, поднялся Китай (7,14% против 3,23% в первом квартале). Вслед за ними расположились Вьетнам (5,04% против 4,82% в первом квартале), Германия (4,13% против 4,39% в первом квартале) и Украина (3,90% против 5,56% в прошлом квартале).

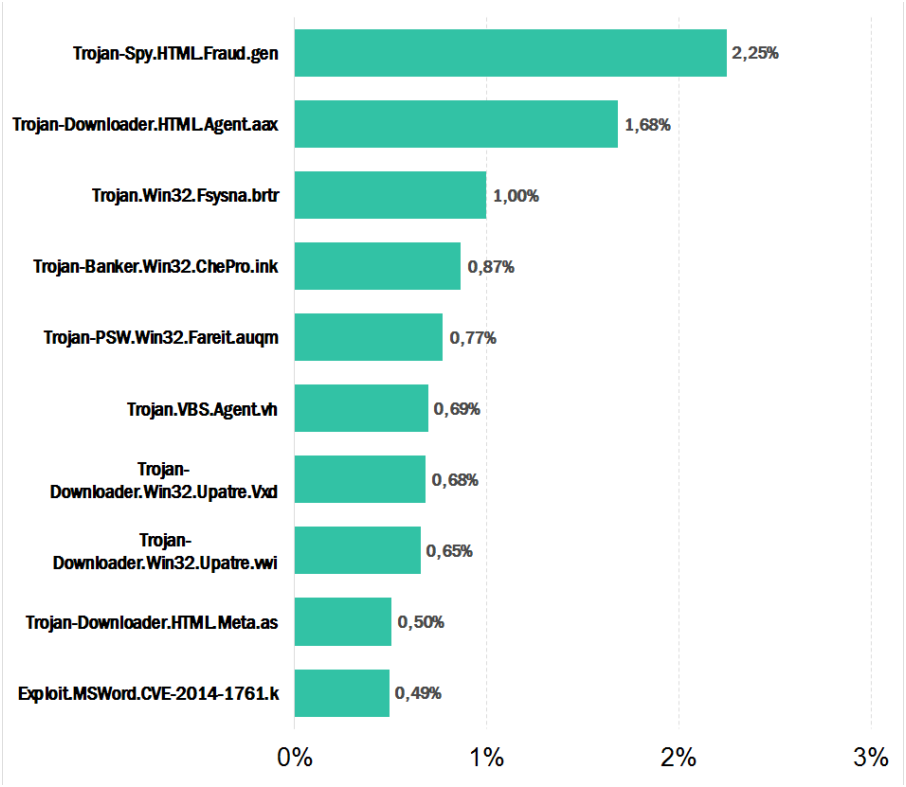
Размеры спамовых писем



Размеры спамовых писем, первый и второй кварталы 2015 г.

Распределение спамовых писем по объему во втором квартале изменилось незначительно. Самыми популярными остаются очень маленькие письма размером менее 2 КБ (65,38%), но их доля понемногу уменьшается (с 73,99% в первом квартале). На 4,81 п.п. увеличилась доля писем объемом от 20 до 50 КБ (8,80%), и немного, примерно по 1 п.п. прибавили доли писем объемом от 2 до 5 КБ (17,16%), от 5 до 10 КБ (3,32%) и от 10 до 20 КБ (2,94%).

ВРЕДОНОСНЫЕ ВЛОЖЕНИЯ В ПОЧТЕ



TOP 10 вредоносных программ, распространенных в почте, второй квартал 2015 г.

Лидирует во втором квартале хорошо знакомый нам Trojan-Spy.HTML.Fraud.gen из семейства троянских программ, реализованных в виде поддельных HTML-страниц. Зловред рассылается по электронной почте под видом важного сообщения от крупных коммерческих банков, интернет-магазинов, софтверных компаний и т.д. На предложенной поддельной HTML-странице пользователь вводит свои конфиденциальные данные, после чего введённая информация отправляется киберпреступникам.

На второй и девятой позициях располагаются Trojan-Downloader.HTML.Agent.aax и Trojan-Downloader.HTML.Meta.as - зловреды, представляющие собой HTML-страницы с кодом для переадресации пользователя на сайт злоумышленника. Там жертву обычно ждет фишинговая страничка или предложение скачать распространённый в последнее время Binbot — приложение для работы с сервисом автоматической торговли бинарными опционами. Распространяются зловреды через почтовые вложения и различаются только ссылкой, перенаправляющей пользователя на сайт злоумышленников.

Замыкает первую тройку зловред Trojan.Win32.Fsysna.brtr, который представляет собой простой спам-бот. Он от имени инфицированной машины перенаправляет спам от командного центра на mail-сервер.

На четвёртой позиции расположился Trojan-Banker.Win32.ChePro.ink. Зловред выполнен в виде CPL-апплета (компонента панели управления) и занимается загрузкой на компьютер жертвы троянцев, предназначенных для кражи конфиденциальной финансовой информации. в основном зловреды этого типа нацелены на бразильские и португальские банки.

Далее следует Trojan-PSW.Win32.Fareit.auqm. Зловреды семейства Fareit крадут куки браузеров, пароли от FTP-клиентов и почтовых программ, а затем отсылают эти данные на удаленный сервер злоумышленников.

Седьмую и восьмую строки занимают троянцы-загрузчики семейства Upatre: Trojan-Downloader.Win32.Upatre.Vxd и Trojan-Downloader.Win32.Upatre.vwi. Их основная задача – загрузить, распаковать и запустить другую вредоносную программу. Зловред обычно маскируется под PDF- или RTF-документ.

Замыкает десятку Exploit.MSWord.CVE-2014-1761.k. Это документ Word, который содержит эксплойт и, при наличии соответствующей уязвимости, загружает на компьютер жертвы другие вредоносные программы, занимающиеся кражей персональных данных.

Семейства вредоносных программ

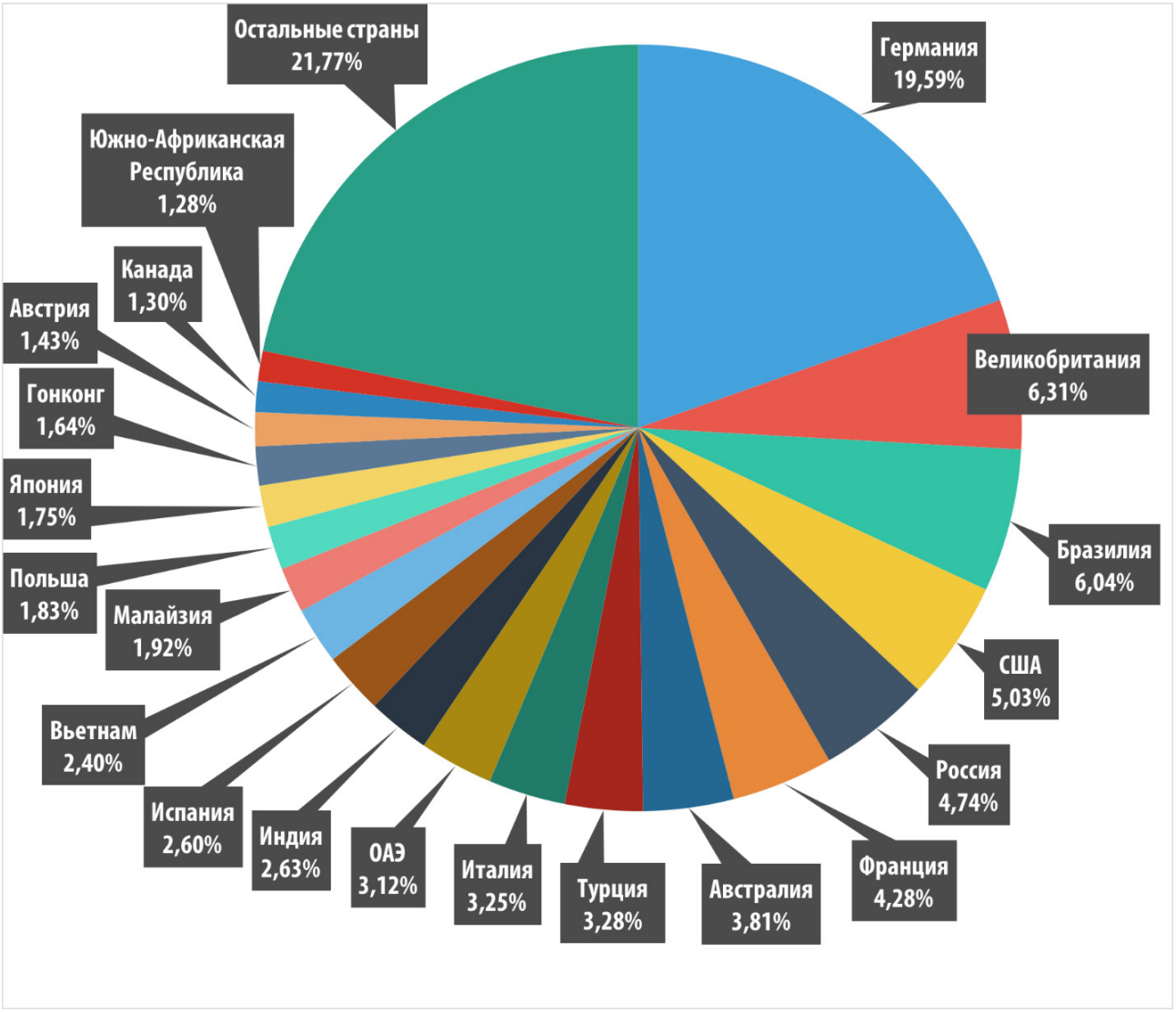
Если говорить о популярных во втором квартале семействах вредоносных программ, то, как и в первом квартале, возглавило этот список Upatre. Зловреды этого семейства обычно скачивают на компьютеры жертв троянца-банкера, известного как Dyre/Dyzap/Dyreza. Список атакуемых этим банкером финансовых учреждений зависит от файла конфигурации, который загружается из командного центра.

Набирают популярность и зловреды семейства MSWord.Agent, в первом квартале они были лишь третьими. Напомним, что эти представляют собой файл .doc со встроенным макросом, написанным на Visual Basic for Applications (VBA), который

выполняется при открытии документа. Зловред загружает и запускает другое вредоносное ПО, например одного из представителей семейства Andromeda.

Снова вернулись в тройку лидеров банкеры ZeuS/Zbot. Представители этого семейства предназначены для атаки на серверы и пользовательские компьютеры, а также для перехвата данных. Хотя ZeuS/Zbot способен выполнять различные вредоносные действия, чаще всего он используется для кражи банковской информации. Также он может устанавливать CryptoLocker – вредоносную программу, вымогающую деньги за расшифровку данных пользователя.

Страны — мишени вредоносных рассылок



Распределение срабатываний почтового антивируса по странам, второй квартал 2015 г.

Тройка лидеров стран, на территорию которых рассылается наибольшее количество вредоносного спама, снова претерпела изменения. Германия (19,59%), которая в первом квартале была лишь четвёртой, поднялась на первую строчку: на территории этой страны мы зафиксировали пятую часть всех срабатываний антивируса. Великобритания (6,31%), занимавшая по итогам первого квартала лидирующую позицию, сместилась на второе место, на третьей строчке расположилась Бразилия (6,04%).

США (5,03%), на территорию которых традиционно рассылалось большое количество писем с вредоносными вложениями, в результате оказались лишь на четвёртой позиции.

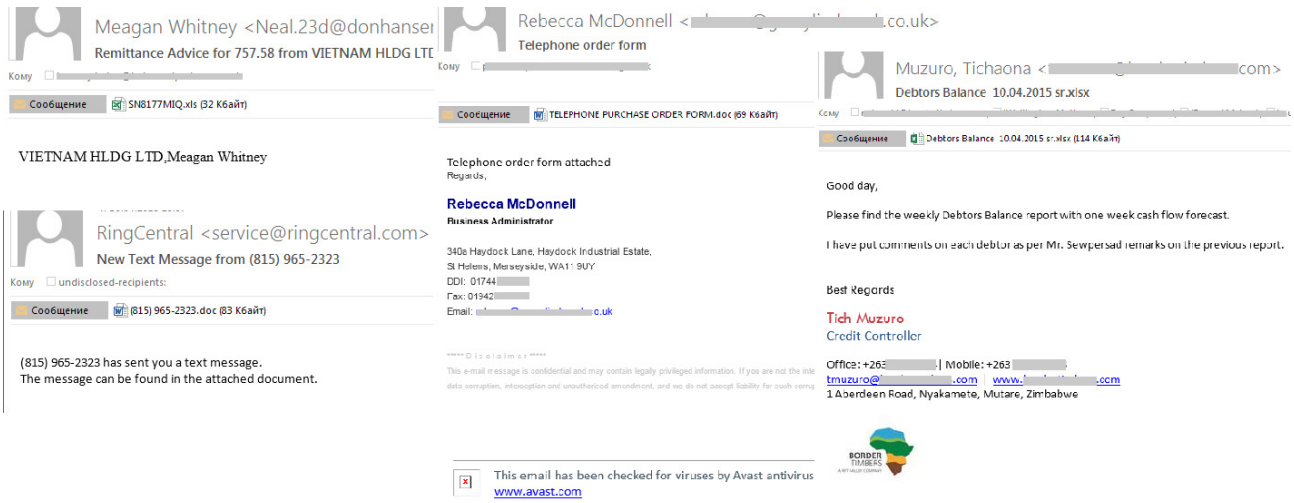
Также стоит отметить, что Россия (4,74%), занимавшая по итогам первого квартала лишь 10-ю строку, во втором квартале поднялась на 5-е место.

Особенности вредоносного спама

Во втором квартале в спам-трафике мы продолжали фиксировать вредоносные письма с макровирусами, пик рассылки которых пришелся на прошлый квартал. Отметим, что их количество снизилось, однако они по-прежнему представляют серьезную опасность: обнаруженные нами макровирусы принадлежали к категории троянцев-загрузчиков и предназначались для скачивания других зловреды. Мошенники, пытаясь убедить получателя в легитимности письма, маскировали сообщения под деловую переписку и выдавали вредоносные вложения за финансовые документы или заказы.

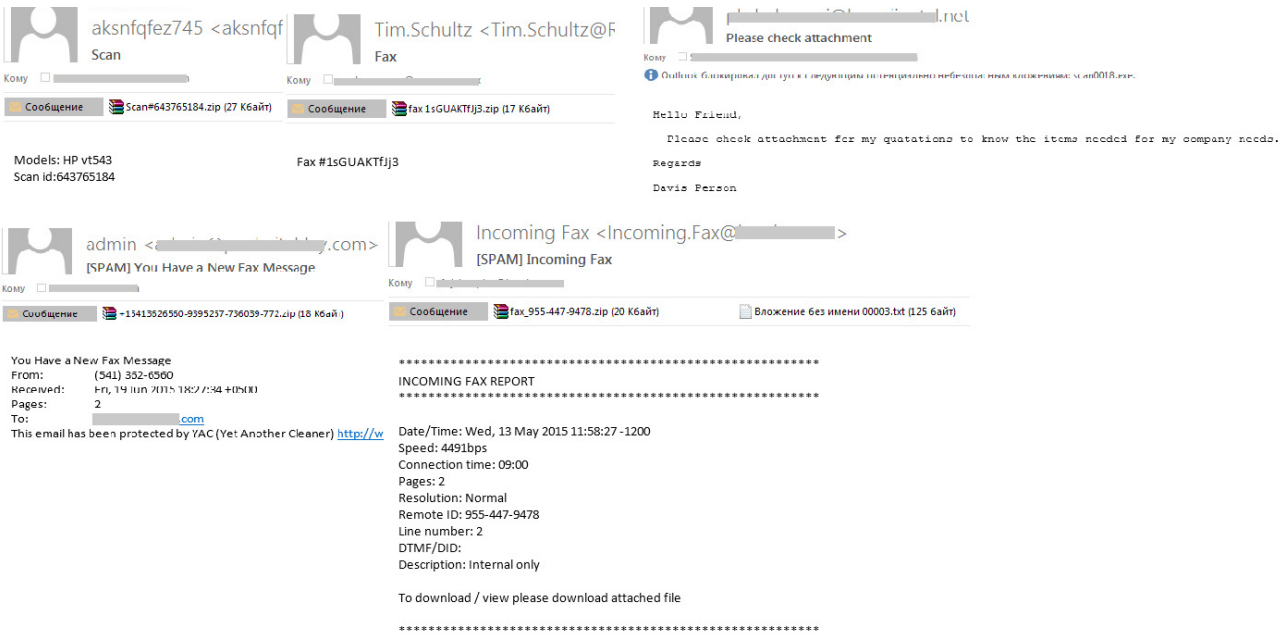
В некоторых письмах злоумышленники указывали подробные контактные данные отправителя, вставляли логотипы для придания письму официального вида, а указанные в письме электронные адреса брали из поля From. Перечисленное делало мошенническое письмо еще более убедительным для получателя.

Нам также встречались письма, которые имитировали официальные сообщения от реальных компаний, причем злоумышленники старались, чтобы содержание сообщения было связано со сферой деятельностью компании. Например, письма одной из обнаруженных рассылок выдавали себя за уведомления о получении текстового сообщения, написанные от имени компании, предоставляющей услуги в сфере телекоммуникаций. Текст сообщения получатель мог прочитать, открыв вложение в формате Microsoft Word, но в действительности вместо обещанной информации в сообщении содержался Trojan-Downloader.VBS.Agent.amj.

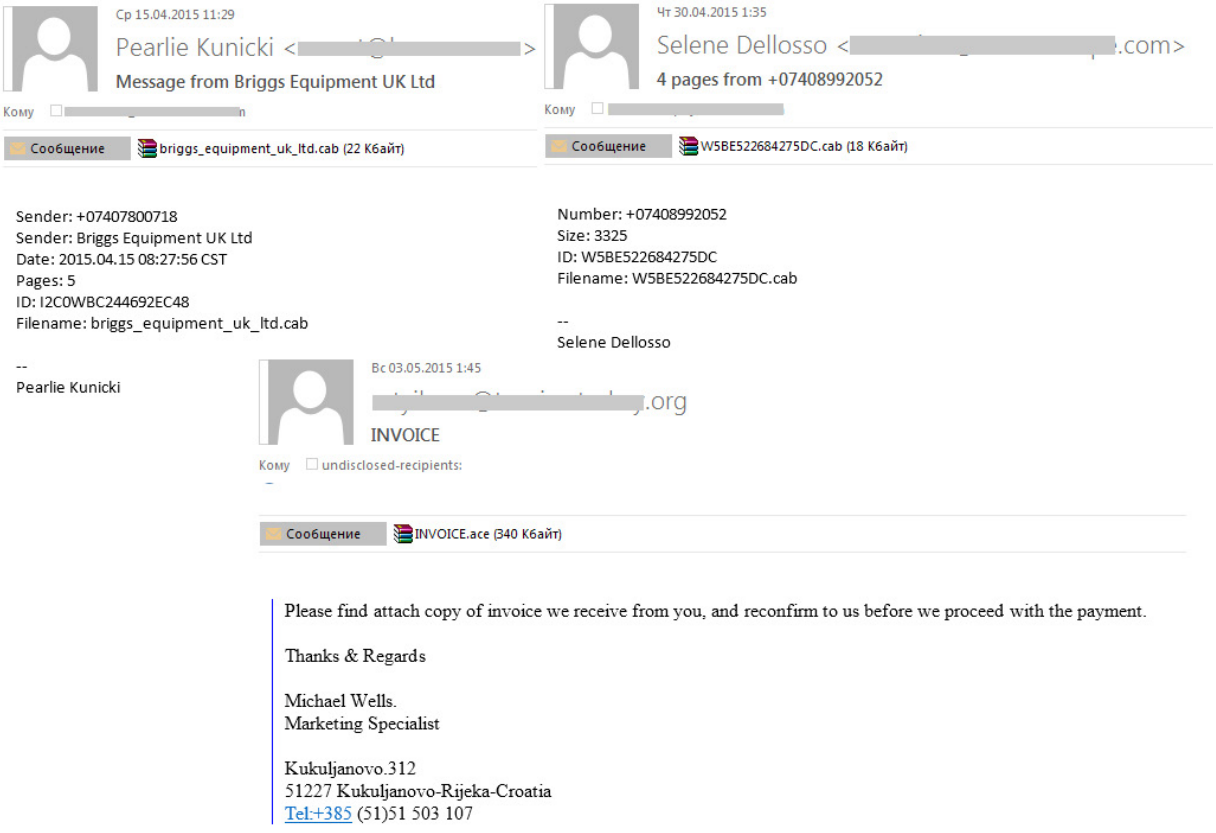


Еще одной не теряющей своей популярности тематикой для киберпреступников, рассылающих вредоносный спам, является маскировка писем под уведомления о получении факсов или сканов различных документов. Такие подделки рассылаются в основном на английском и немецком языках, а вложения, которые выдаются мошенниками за файлы с факсами и сканами, содержат различные виды зловредов: загрузчики Trojan.Upatre и Trojan.Downloader, а также кейлоггер HawkEyePHPLogger.

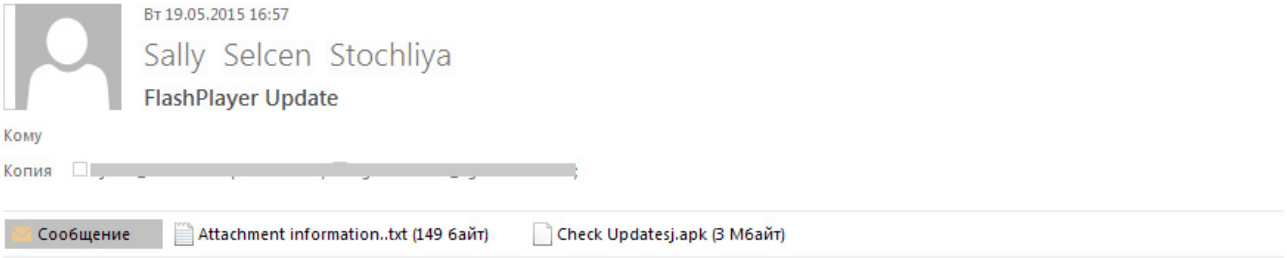
Текст в теле подобных писем мог быть предельно кратким или, наоборот, содержать детальную информацию о полученном документе.

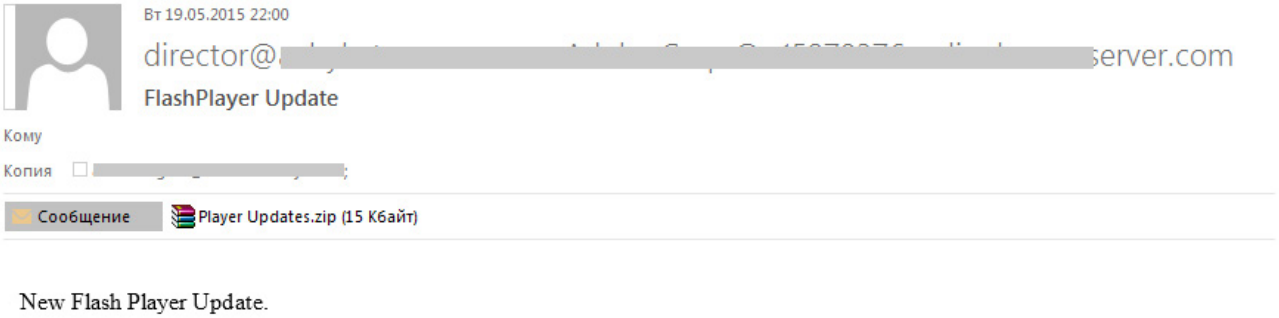


В сентябре 2014 года мы зафиксировали вредоносную рассылку с нетипичным для спама вложением – архивом в формате ARJ. в 2015 году мошенники продолжили использовать нетрадиционные архивы для распространения зловредов: в апреле и мае в спам-трафике рассылались письма с вложениями .cab и .ace, также являющимися файлами архивов непопулярного сейчас формата. в архивах содержались троянец Trojan-Downloader.Win32.Cabby и кейлоггер HawkEye Keylogger. в отличие от популярных в спаме расширений .zip и .rar, вложения .cab и .ace могут быть незнакомы пользователям и потому вызывать меньше подозрений.



Во втором квартале 2015 года мошенники в рамках одной рассылки распространяли вредоносные файлы во вложениях в формате ZIP и APK. Если ZIP-архивы встречаются в подавляющем большинстве спам-сообщений, то вложения формата APK сравнительно редки, так как являются архивными исполняемыми файлами-приложениями для Android. в обнаруженных нами ZIP-архивах находился троянец семейства Upatre, а файл Check_Updatesj.apk детектировался как троянец-шифровальщик SLocker для системы Android, при запуске которого происходило шифрование изображений, документов и видеофайлов, находящихся на устройстве. После этого пользователю показывалось сообщение с требованием заплатить денежную сумму за расшифровку файлов. Рассылая зловреды во вложениях формата ZIP и APK в рамках одной рассылки, мошенники, возможно, рассчитывали, что их жертвами станут не только пользователи ПК, но и владельцы смартфонов и планшетов на Android, работающие с электронной почтой с этих устройств.

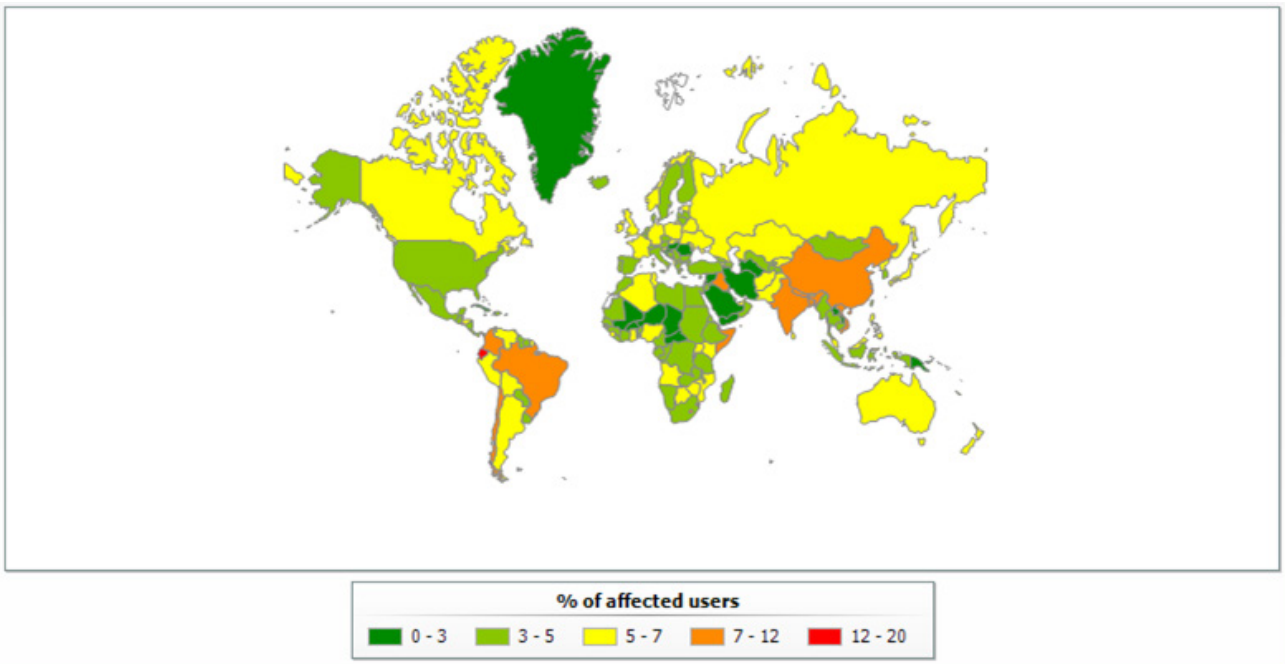




ФИШИНГ

Во втором квартале 2015 года на компьютерах пользователей продуктов «Лаборатории Касперского» было зафиксировано 30 807 071 срабатываний системы «Антифишинг». в базы «Лаборатории» Касперского за этот период добавлено 509 905 масок фишинговых URL.

На протяжении уже нескольких кварталов наибольший процент атакованных фишерами пользователей наблюдается в Бразилии. Однако во втором квартале 2015 года этот показатель снизился почти в два раза по сравнению с предыдущим кварталом. То же самое произошло с показателями многих других стран.



География фишинговых атак, второй квартал 2015 года*

* Процент пользователей, на компьютерах которых сработала система «Антифишинг», от всех пользователей продуктов «Лаборатории Касперского» в стране.

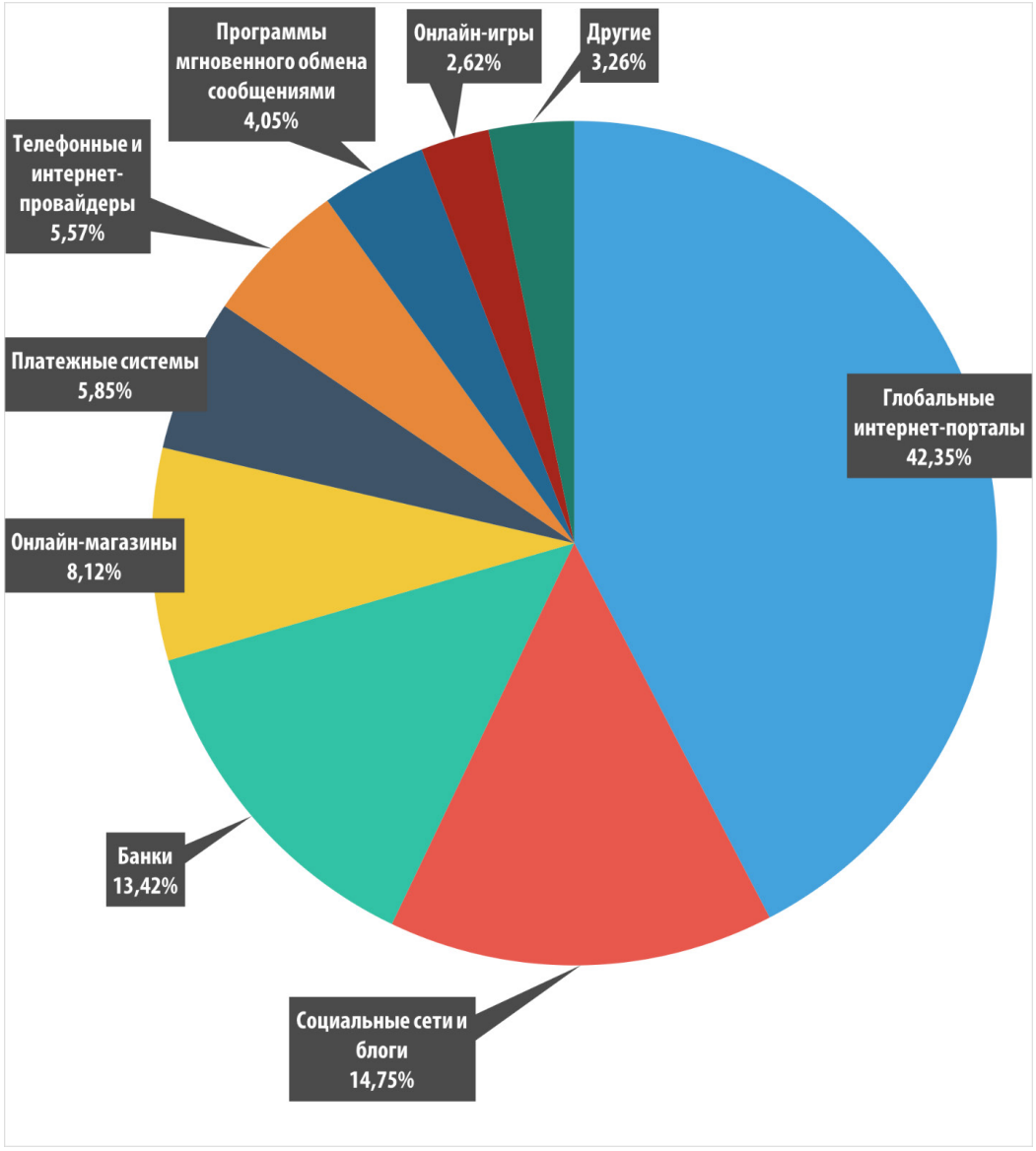
ТОР 10 стран по проценту атакованных пользователей:

	Страна	% Пользователей
1	Бразилия	9,74
2	Индия	8,3
3	Китай	7,23
4	Россия	6,78
5	Франция	6,54
6	Япония	5,93
7	Малайзия	5,92
8	Польша	5,81
9	Казахстан	5,79
10	ОАЭ	5,75

Организации - мишени атак

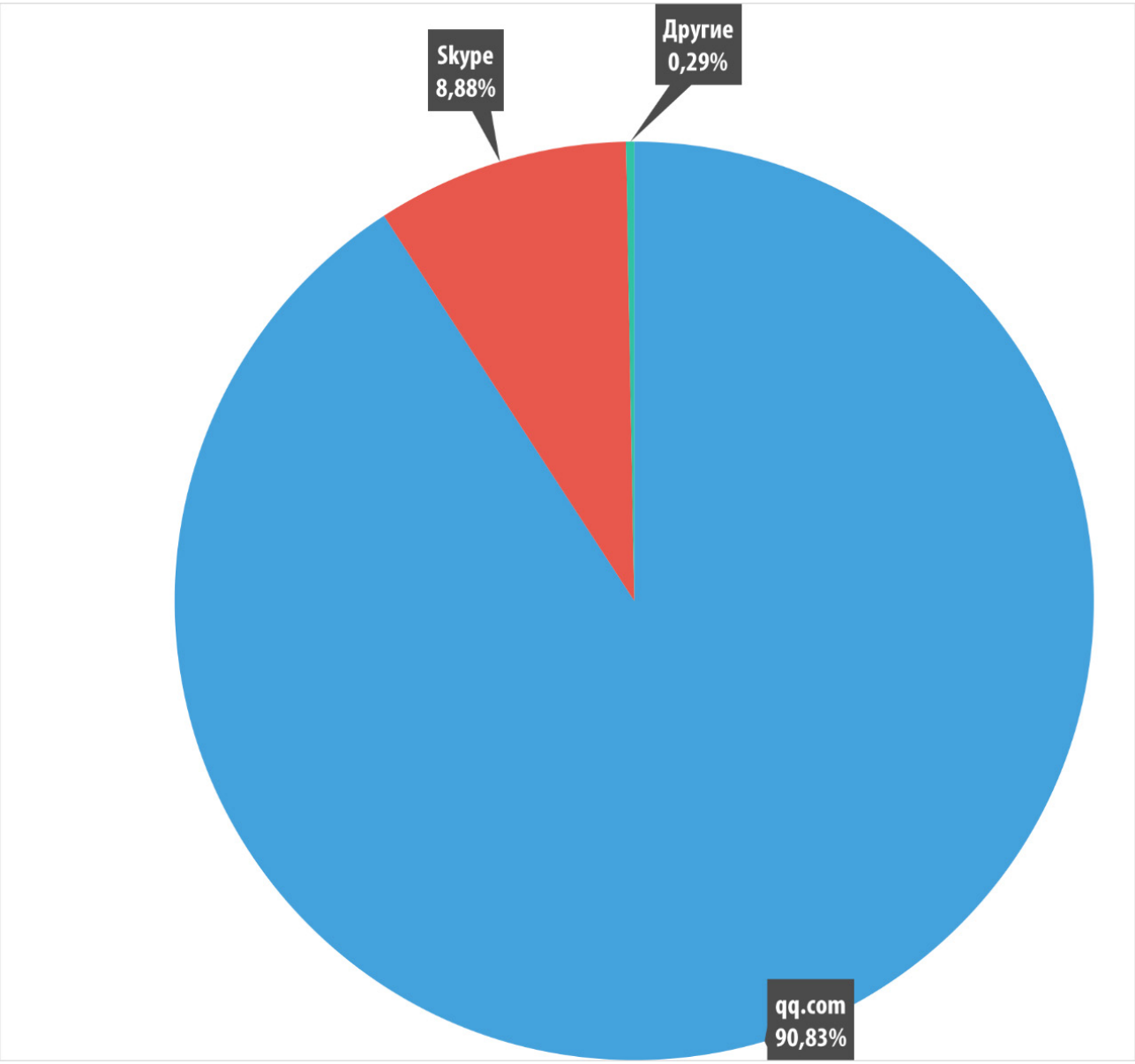
Статистика по мишеням атак фишеров основана на срабатываниях эвристического компонента системы «Антифишинг». Эвристический компонент системы «Антифишинг» срабатывает, когда пользователь переходит по ссылке на фишинговую страницу, а информация об этой странице еще отсутствует в базах «Лаборатории Касперского». При этом неважно, каким образом совершается данный переход: в результате нажатия на ссылку в фишинговом письме, в сообщении в социальной сети или, например, в результате действия вредоносной программы. в результате срабатывания в браузере пользователь видит предупреждающий баннер о возможной угрозе.

Категория «Глобальные порталы» вновь перетянула на себя большую долю срабатываний - во втором квартале 2015 года ей соответствовало 42,35%, что на 16,69 п.п. больше, чем в первом квартале. Также немного выросла (на 0,13 п.п.) доля категории «Программы мгновенного обмена сообщениями» (4,05%). Процент остальных категорий понизился: «Социальные сети и блоги» потеряли 2,6 п.п., «Банки» - 5,56 п.п., «Онлайн-магазины» - 1,56 п.п., «Платежные системы» - 2,84 п.п., «Телефонные и интернет провайдеры» - 1,33 п.п., «Онлайн-игры» - 0,78 п.п.



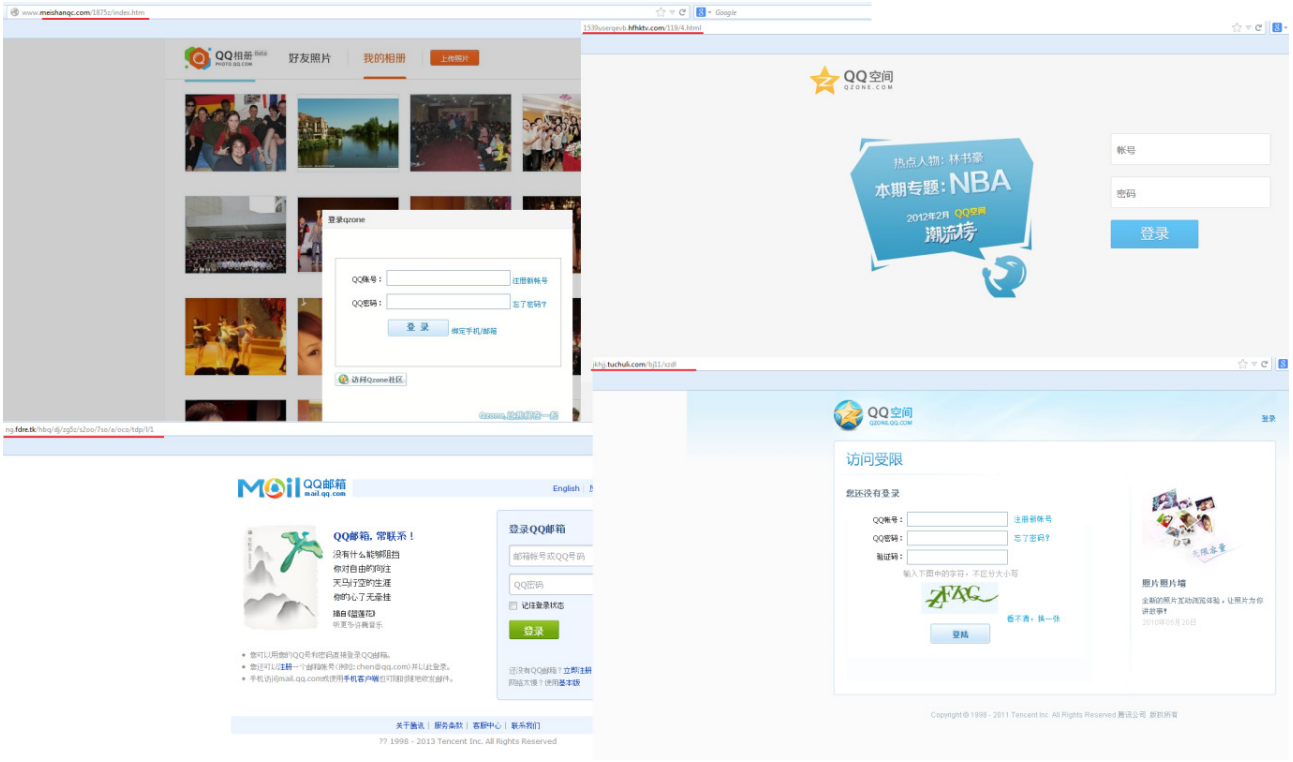
Распределение организаций, атакованных фишерами по категориям, второй квартал 2015 г.

Программы мгновенного обмена сообщениями пользуются популярностью у мошенников по множеству причин. Например, киберпреступники часто используют украденные аккаунты для дальнейшей рассылки фишинговых сообщений или ссылок на вредоносные программы по списку контактов жертвы, рассылки спама, вымогания денег и других мошеннических схем.



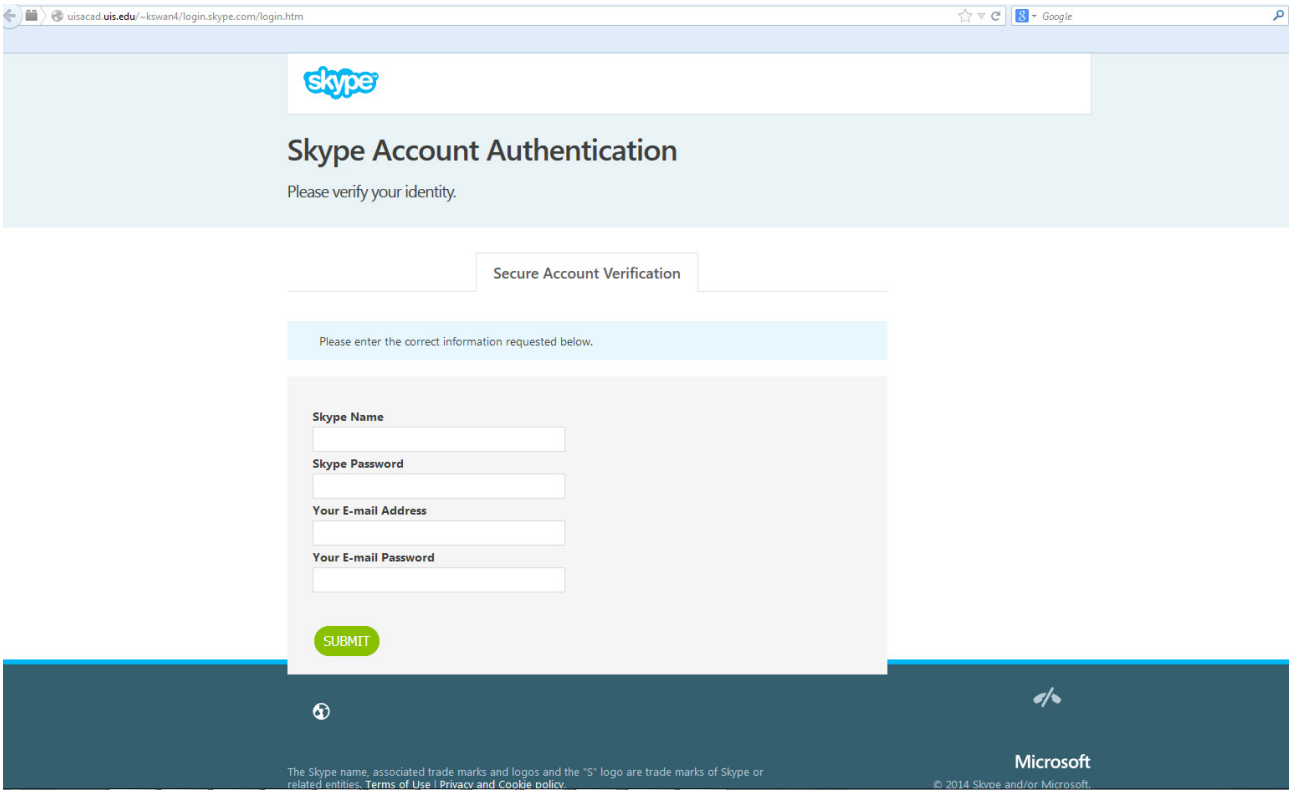
Распределение фишинговых атак на пользователей программ мгновенного обмена сообщениями, второй квартал 2015 года

Большая часть срабатываний в данной категории приходится на популярный китайский сервис мгновенного обмена сообщениями QQ, поддерживаемый телекоммуникационной компанией Tencent.



Примеры фишинговых страниц, имитирующих страницы входа в сервисы QQ

На втором месте программа Skype (8,88%), принадлежащая Microsoft. Ее доля более чем на порядок меньше доли лидера.



Пример фишинговой страницы, предлагающей пользователям Skype верифицировать свой аккаунт.

TOP 3 атакуемых организаций

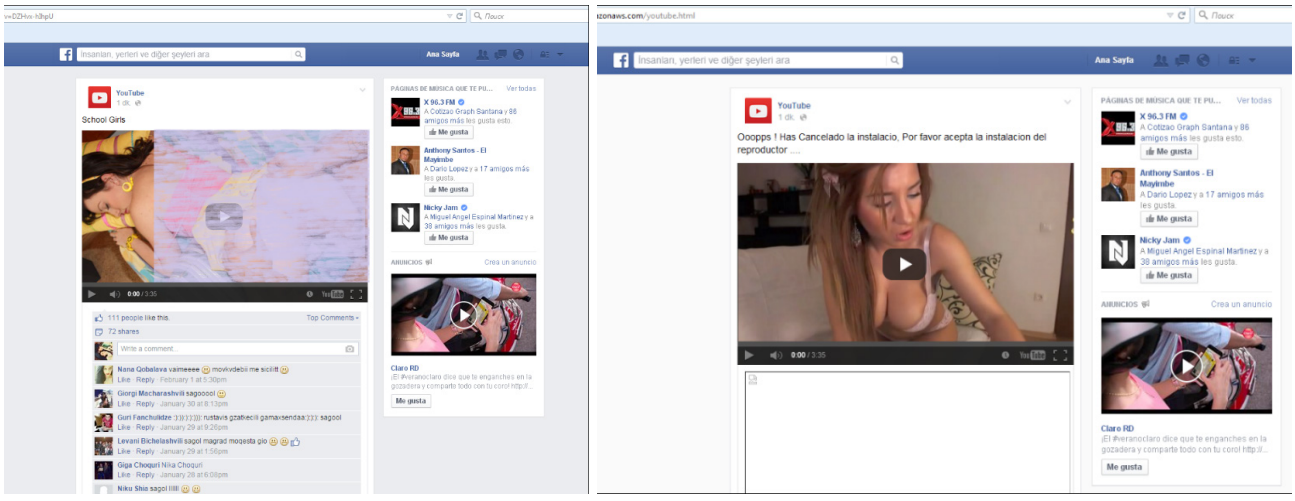
Как мы отмечали в предыдущих отчетах, основная часть нецелевого фишинга направлена на пользователей нескольких наиболее популярных компаний. Такие компании имеют множество клиентов по всему миру, благодаря чему у мошенников больше шансов попасть в цель, организуя очередную фишинговую атаку.

На TOP 3 атакуемых фишерами организаций приходится 45,14% всех детектируемых фишинговых ссылок.

	Организация	% от всех детектируемых фишинговых ссылок
1	Yahoo!	29,03%
2	Facebook	10,44%
3	Google	5,67%

По сравнению с первым кварталом 2015 года состав первой тройки остался без изменений. в нее по-прежнему входят Yahoo! (+23,82 п.п.), Facebook (-0,53 п.п.) и Google (-2,44 п.п.). Значительное увеличение доли срабатываний на фальшивые страницы, маскируемые под Yahoo!, стало возможным благодаря общему снижению количества детектов; в численном выражении количество срабатываний на поддельные страницы Yahoo! выросло незначительно.

Во втором квартале 2015 года мы столкнулись с массой фишинговых страниц, которые имитировали публикацию на странице Facebook, содержащую откровенное YouTube-видео. При попытке запустить видео происходило скачивание вредоносной программы на компьютер жертвы.



Примеры имитирующих Facebook фальшивых страниц, распространяющих вредоносные файлы

ЗАКЛЮЧЕНИЕ

Доля спама в почтовом трафике по итогам второго квартала 2015 года составила 53,4%, что на 5,8 п.п. меньше, чем в предыдущем квартале.

Во втором квартале истории нигерийских писем основывались на реальных событиях: предстоящей Олимпиаде в Рио-де-Жанейро, прошедших в Нигерии выборах президента, а также землетрясении в Непале. Мошенники заманивали получателей не только обещанием вознаграждения или компенсации за нанесенный ущерб, но и упоминанием о выигрыше в лотерею, а также просили сделать безвозмездное пожертвование для пострадавших в Непале.

Информационным поводом к увеличению спама на тему SEO стал выпуск очередного обновления алгоритма поиска Google Search. Целью обновления был подъем сайтов, адаптированных для мобильных телефонов, на более высокие позиции в результатах мобильного поиска.

Тройка лидеров среди стран – источников спама, рассылаемого по всему миру, во втором квартале выглядит следующим образом: США (14,6%), Россия (7,8%), Китай (7,1%).

Рейтинг вредоносных программ, распространенных в почте, по итогам второго квартала возглавляет Trojan-Spy.HTML.Fraud.gen. Среди семейств вредоносных программ лидером стало семейство Upatre. Наиболее часто вредоносным атакам подвергались пользователи Германии – на их долю пришлось 19,6% срабатываний почтового антивируса.

Вредоносные файлы, вложенные в письма, злоумышленники выдавали за факсы и сканы, обновления Flash Player и деловую переписку. Также киберпреступники продолжили рассылать макровирусы в документах Word и Excel, плюс использовали не характерные для спама архивы (.cab и .ace) и файлы .apk.
Во втором квартале 2015 года мы зафиксировали более 30 млн срабатываний системы «Антифишинг» на компьютерах пользователей продуктов «Лаборатории Касперского». Наибольший процент атакованных фишерами пользователей наблюдался в Бразилии, несмотря на то что показатель страны снизился почти в два раза по сравнению с предыдущим кварталом.

О «Лаборатории Касперского»

«Лаборатория Касперского» – крупнейшая в мире частная компания, работающая в сфере информационной безопасности, и один из наиболее быстро развивающихся вендоров защитных решений. Компания входит в четверку ведущих мировых производителей решений для обеспечения IT-безопасности пользователей конечных устройств (IDC, 2014). С 1997 года «Лаборатория Касперского» создает инновационные и эффективные защитные решения и сервисы для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей. «Лаборатория Касперского» – международная компания, работающая почти в 200 странах и территориях мира; ее технологии защищают более 400 миллионов пользователей по всему миру. Более подробная информация доступна на сайте www.kaspersky.ru.

Securelist, ресурс экспертов «Лаборатории Касперского» с актуальной информацией о киберугрозах

Сайт «Лаборатории Касперского»

B2B блог «Лаборатории Касперского»

Блог Евгения Касперского

B2C блог «Лаборатории Касперского»

Новостная служба «Лаборатории Касперского»

Блог Kaspersky Academy

Москва, 125212
Ленинградское шоссе, д.39А, стр.3
БЦ «Олимпия Парк»

Телефон: +7-495-797-8700
+7-495-737-3412
Факс: +7-495-797-8709

KASPERSKY lab