СПАМ И ФИШИНГ В ТРЕТЬЕМ КВАРТАЛЕ 2015

Татьяна Щербакова,
Мария Вергелис,
Надежда Демидова

ОГЛАВЛЕНИЕ

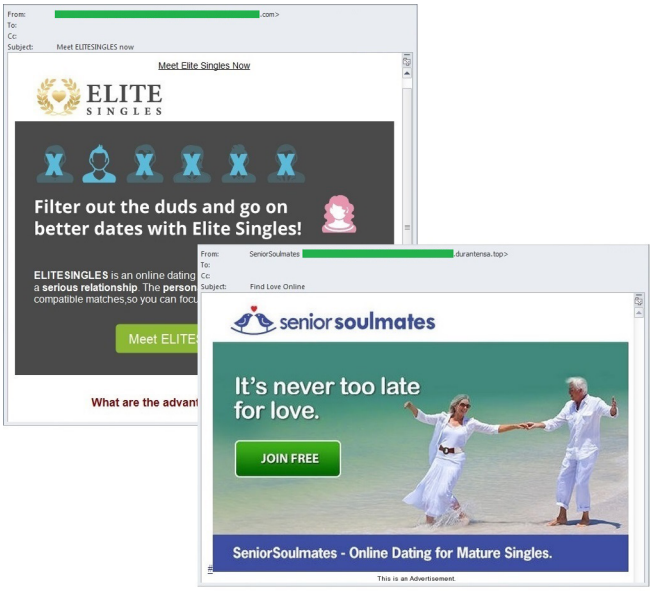
СПАМ: ОСОБЕННОСТИ КВАРТАЛА 3
Онлайн-знакомства 3
Сезонный вредоносный спам 5
Трюки спамеров 7
СТАТИСТИКА 9
Доля спама в почтовом траффике 9
Страны – источники спама 10
Размеры спамовых писем 10
ВРЕДОНОСНЫЕ ВЛОЖЕНИЯ В ПОЧТЕ 11
Семейства вредоносных программ 12
Страны — мишени вредоносных рассылок 12
Особенности вредоносного спама 13
ФИШИНГ 15
Организации - мишени атак 16
TOP 3 атакуемых организаций 19
ЗАКЛЮЧЕНИЕ 20

СПАМ: ОСОБЕННОСТИ КВАРТАЛА

Онлайн-знакомства

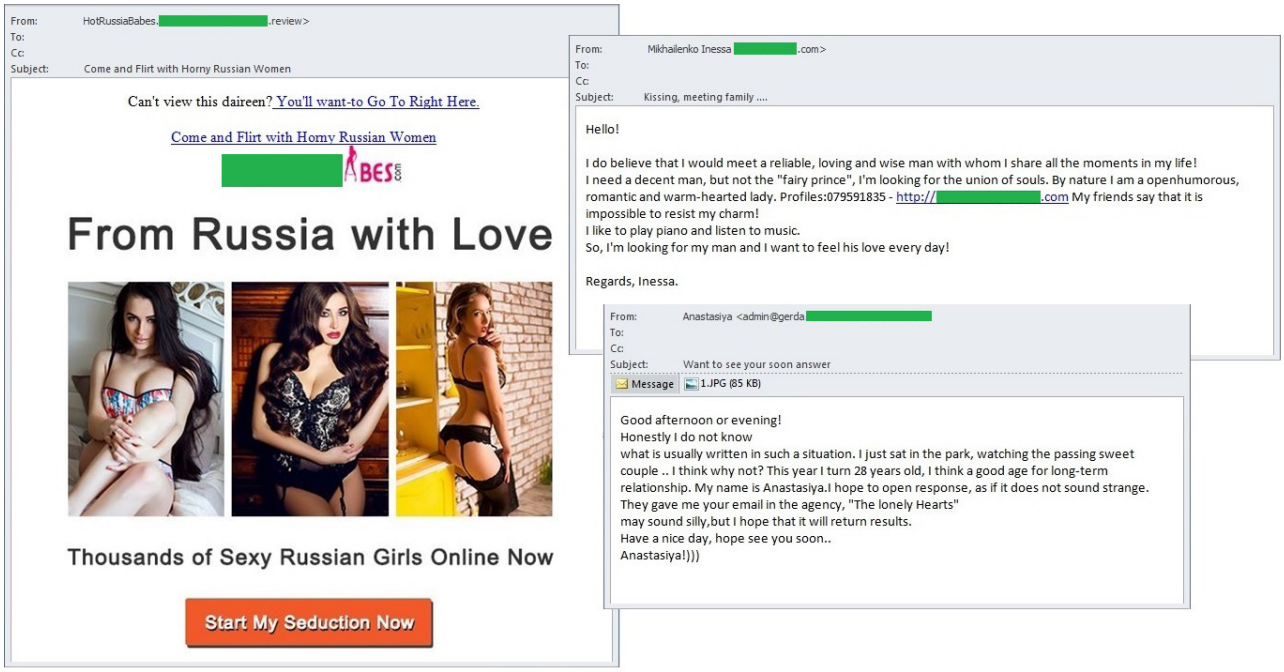
Тематика знакомств и свиданий типична для спама и встречается нам постоянно, однако в третьем квартале 2015 года поток подобных писем стал более разнообразным и этим привлек наше внимание. Мы обнаружили несколько интересных попыток ввести в заблуждение получателя и обойти спам-фильтр, а также зафиксировали новые виды рассылок, по сути близких к мошенничеству.

Обычно главная задача спамеров в рассылках данной тематики – реклама недавно созданных и нераскрученных сайтов знакомств. Владельцы таких сайтов прибегают к спаму, чтобы привлечь как можно большую аудиторию на свой ресурс. Нередко в таких сообщениях встречается тематическое деление: например, сайты знакомств для пожилых, женатых или верующих.



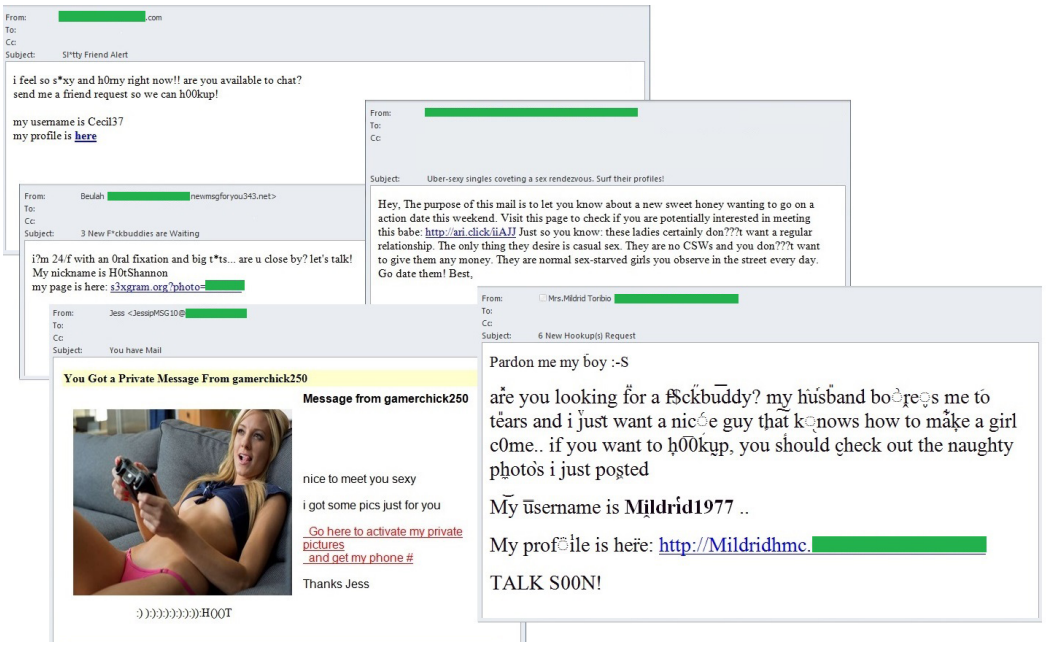
Еще один вид предложений – реклама брачных агентств, занимающихся подбором невест (в основном, из России и Украины) для иностранных женихов. Этот вид спама, как правило, распространяется в англоязычном сегменте интернета. Такие письма содержат приглашение к регистрации на соответствующих ресурсах, обычно небольшое количество текста с обещанием найти идеального спутника жизни и ссылку, ведущую на рекламируемый сайт.

Аналогичные по смыслу письма могут также рассылаться от имени самой «невесты». Этот вид спама уже ближе к мошенничеству, схема которого напоминает «нигерийскую». Письма приходят от имени девушки, которая вкратце рассказывает о себе, своей нелегкой жизни в российской глубинке и мечтах о прекрасном принце. Часто прилагается фотография, на которой не обязательно изображена сама «невеста» – фото могут быть взяты с чужих страниц из социальных сетей и рассылаться для придания сообщению большей убедительности. Поэтому фотографии могут повторяться от письма к письму даже в случае, если они отправлены от имени разных девушек. А вот текст письма меняется: при проведении рассылок спамеры активно используют синонимичные ряды с расчетом на обход фильтра. Обычный вид обратной связи, предполагаемый в таких письмах, – электронная почта. При этом адреса меняются в каждом письме – очевидно, они создаются в большом количестве на бесплатных почтовых сервисах специально под рассылку. Отправив ответное письмо на такой адрес, пользователь в лучшем случае получит уведомление о несуществующем почтовом ящике, в худшем – засветит свой адрес для дальнейших спам-рассылок или станет жертвой мошеннической схемы: девушка попросит выслать ей денег на билет, чтобы добраться до своего избранника, после чего, получив желаемое, пропадет навсегда.



Таким же образом рекламируются и сайты знакомств «для взрослых». Сообщения содержат либо приглашение к регистрации на сайте и обещание интим-знакомств, либо обращение некой девушки, которая ищет партнера для интима, и ссылку на ресурс, где якобы можно перейти к профилю незнакомки. Нередко спам с рекламой таких ресурсов распространяется под видом разнообразных уведомлений о личных сообщениях в социальных сетях, а также о фотографиях

или аудиофайлах, присланных через мессенджеры. В результате реклама ресурса полностью завуалирована, и пользователь не может точно определить, что перед ним, пока не пройдет по предложенным ссылкам. При этом содержимое таких сообщений призвано вызвать у получателя интерес и заставить его пройти по ссылке, нередко за счет «заигрывающего» содержания или прозрачных намеков и откровенных фотографий.

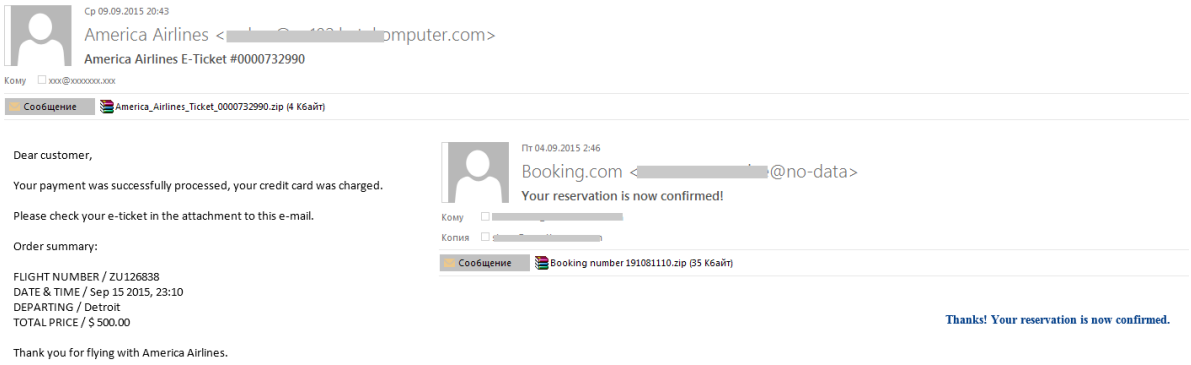


И наконец, еще один вид рассылок, обнаруженный нами в третьем квартале, относится к явному мошенничеству. На протяжении квартала мы наблюдали рассылку, содержание которой имело целью заставить получателя отправить SMS на предложенный телефонный номер; в ответ некая девушка обещала выслать свои откровенные фото. Текст рассылки активно менялся и зашумлялся, как и мобильные номера, указанные в ней. Мы написали сообщения на несколько таких номеров и установили, что они не платные, как могло показаться на первый взгляд, и денег за отправку сообщения с пользователей не взимают. В SMS-переписку с нами вступила девушка, но по ее ответам уже через пару сообщений стало понятно, что это робот, который подводит разговор к необходимости скачать некое приложение для возможности дальнейшего чата и отправки обещанных фотографий. В итоге нам удалось получить от «девушки» несколько SMS с различными короткими ссылками, которые, вели на одну и ту же статью в известной американской газете, рассказывающую о полезных мобильных приложениях. Во время редиректа на данную статью на телефон пользователя загружается архив с мобильным вредоносным ПО.

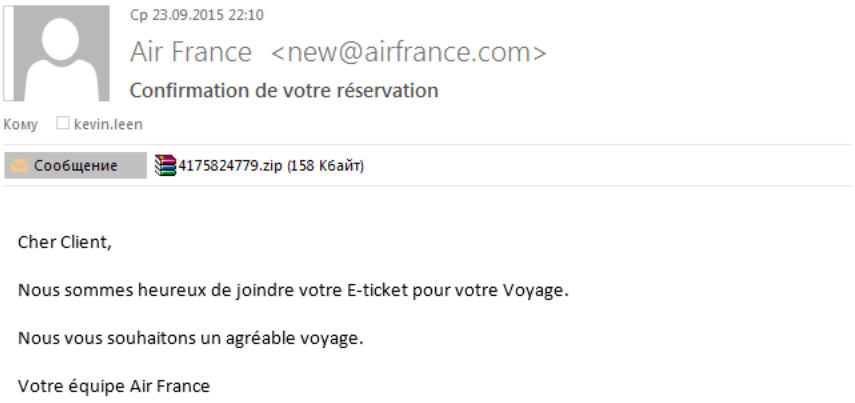
Сезонный вредоносный спам

В летний период традиционно увеличивается количество спама сезонной тематики; это касается не только рекламного спама, но и вредоносного. В прошедший сезон отпусков наиболее актуальным стал туристический спам: поддельные уведомления от имени сервисов бронирования, авиакомпаний и отелей использовались мошенниками для распространения вредоносных программ.

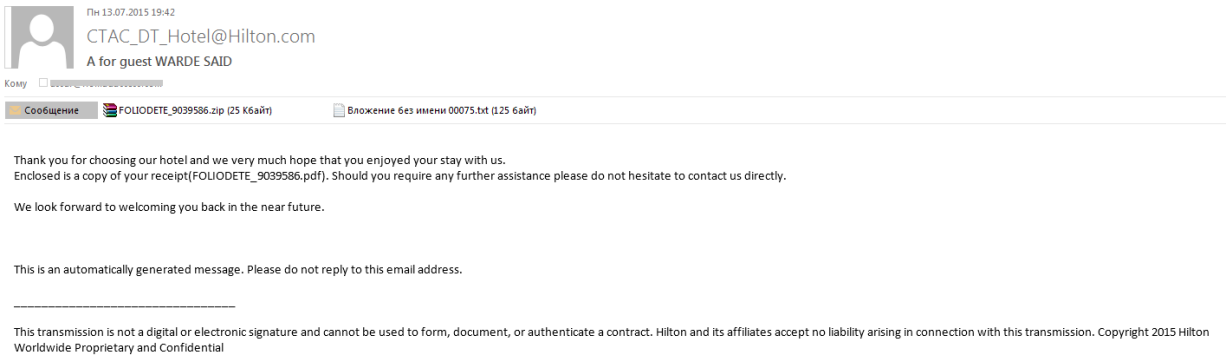
В фальшивых сообщениях от имени крупных международных авиакомпаний и сервисов бронирования мы детектировали троянцев-загрузчиков, а именно Trojan-Downloader.JS.Agent.hhy и Trojan-Downloader.Win32.Upatre.



Подобные письма от имени известных авиакомпаний встречались нам и на французском языке. В тексте письма получателя информировали, что во вложении находится электронный авиабилет. На самом деле ZIP-архив содержал троянца Trojan.Win32.Xtrat и DDoS-бот Nitol (модуль, предназначенный для организации DDoS-атак).



В июле злоумышленники пытались обмануть пользователей, рассылая поддельные уведомления от имени отелей. В сообщении получателя благодарили за пользование отелем и предлагали ознакомиться с копией счета за услуги, приложенной к письму. На деле в архиве находился Trojan-Downloader.Win32.Upatre.dhwi, который в свою очередь скачивал и запускал по ссылкам (вида 98.***.**.39/cv17.rar), прописанным в теле загрузчика, банкер Trojan-Banker.Win32.Dyre.



Кроме фальшивых писем от имени известных компаний мы обнаружили в спам-потоках и письмо на английском языке от частного лица. Письмо содержало просьбу изменить забронированный ранее номер на двухместный в связи с уменьшением количества постояльцев.

Чт 20.08.2015 16:40
Beatrice De Luca <crucial.oberbitschige@xxxxxx-xxxxxx-xxxx.xxx>
room change.
Кому
Сообщение Photo_7314.zip (2 Кбайт)

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

Details of changes in attachment.
Thanks!

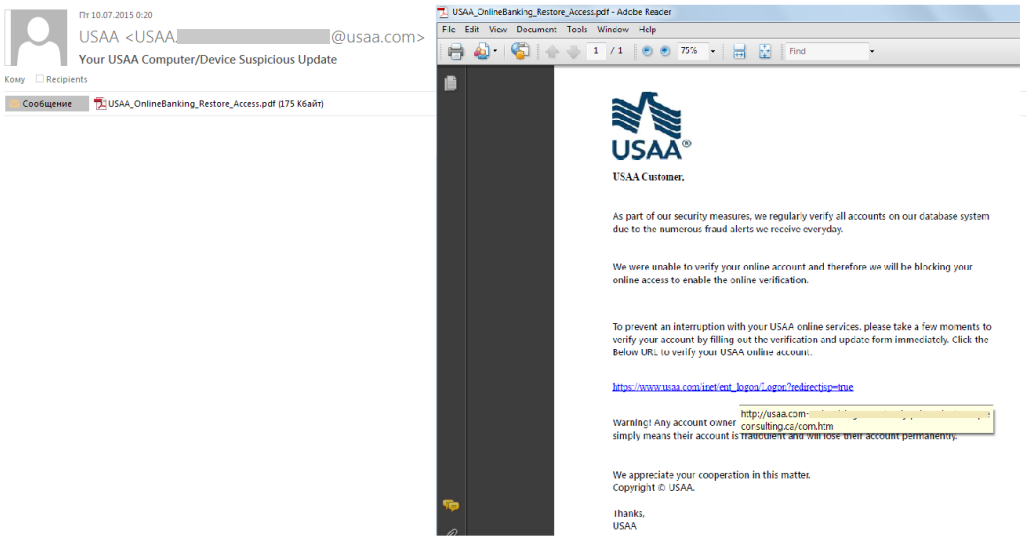
This email has been protected by YAC (Yet Another Cleaner) http://www.yac.mx

Текст данного письма можно принять за легитимное обращение клиента, однако ZIP-вложение содержало загрузчик Trojan-Downloader.JS.Agent.hhi, который закачивал на зараженный компьютер бэкдор Backdoor.Win32.Androm.

Трюки спамеров

В стандартном фишинговом письме текст сообщения находится в теле письма, а персональную информацию необходимо ввести на веб-странице, перейдя по указанной в тексте мошеннической ссылке, или в полях HTML-странички, которая вложена в письмо, или переслать в обратном письме. Последнее наиболее характерно для писем с просьбой подтвердить адрес и пароль от электронной почты.

В третьем квартале злоумышленники придумали новый способ размещения фишингового сообщения и обхода спам-фильтров. Текст фишингового сообщения и поддельная ссылка помещались в PDF-документ, который был вложен в письмо. При переходе по ссылке открывалась обычная фишинговая страничка, на которой пользователю необходимо было ввести персональную информацию. Большинство обнаруженных нами писем, в которых использовался новый прием, имитировали уведомления от банков. В теле таких сообщений обычно приводился максимально короткий текст с описанием проблемы, иногда текст и вовсе отсутствовал.


Пт 10.07.2015 0:20
USAA <USAA.[redacted]@usaa.com>
Your USAA Computer/Device Suspicious Update
Кому Recipients
Сообщение USAA_OnlineBanking_Restore_Access.pdf (175 Кбайт)

USAA_OnlineBanking_Restore_Access.pdf - Adobe Reader
File Edit View Document Tools Window Help

USAA®
USAA Customer,

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

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

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

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

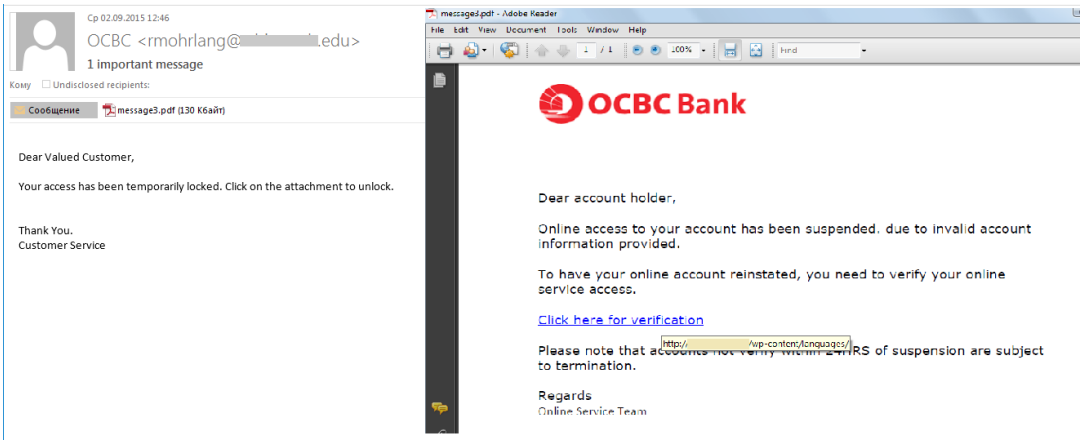
http://usaa.com-[redacted]corsulting.ca/com.htm

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

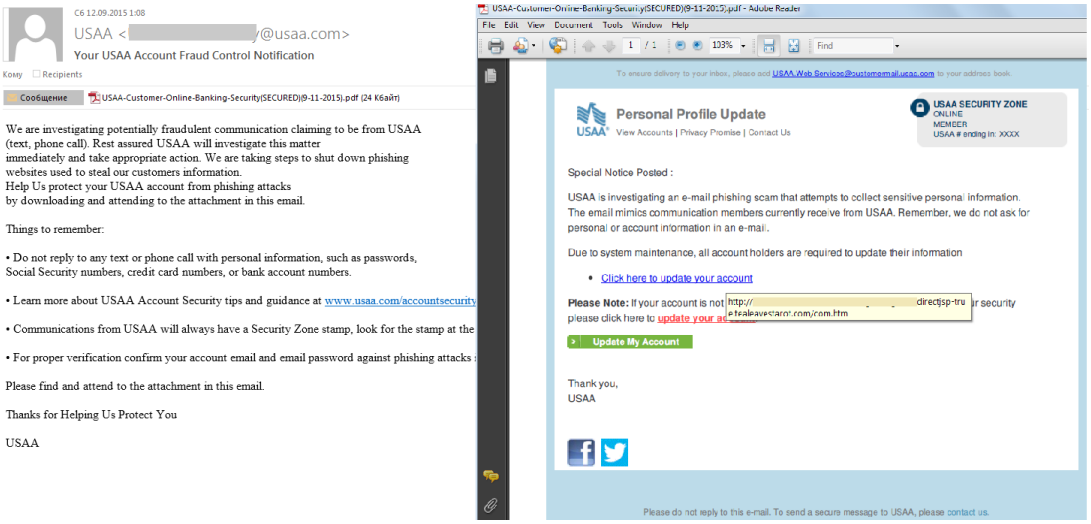
We appreciate your cooperation in this matter.
Copyright © USAA.

Thanks,
USAA

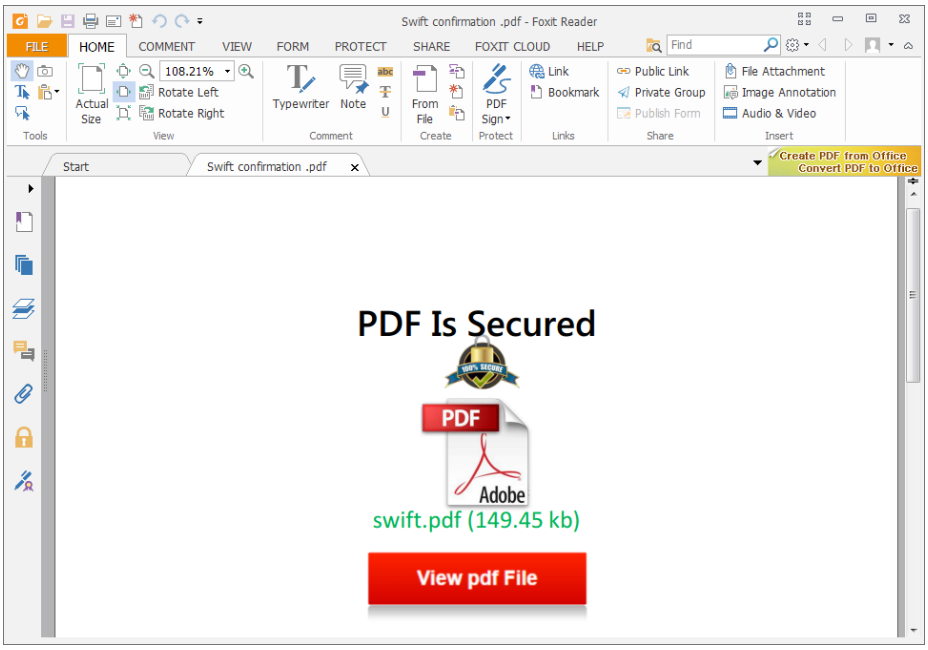
Отметим, что в тексте обнаруженных писем спамеры использовали уже известные фразы и уловки: сообщение о блокировке аккаунта, необходимости пройти верификацию, упоминание о безопасности, расследовании случая фишинга и т.д. Мошеннические ссылки, как и раньше, маскировались легитимными ссылками и текстовыми фрагментами.



Но встречались нам и письма с подробным текстом в теле письма, с указанием настоящих ссылок на официальные ресурсы банка. Фишинговое уведомление так же помещалось в PDF-вложение.



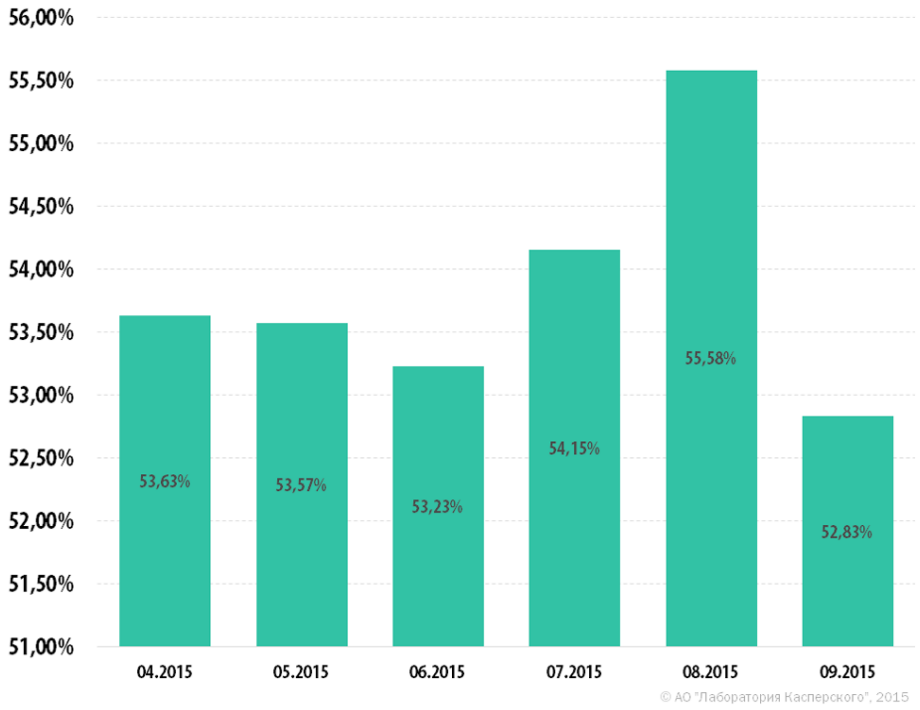
Кроме того, наши коллеги обнаружили немного другой вариант фишинговых писем с использованием объектов Mediabox в PDF-файлах, прикрепленных к письмам.



Объект Mediabox – документ, который открывался щелчком мыши и использовался для переадресации пользователя на фишинговый веб-сайт.

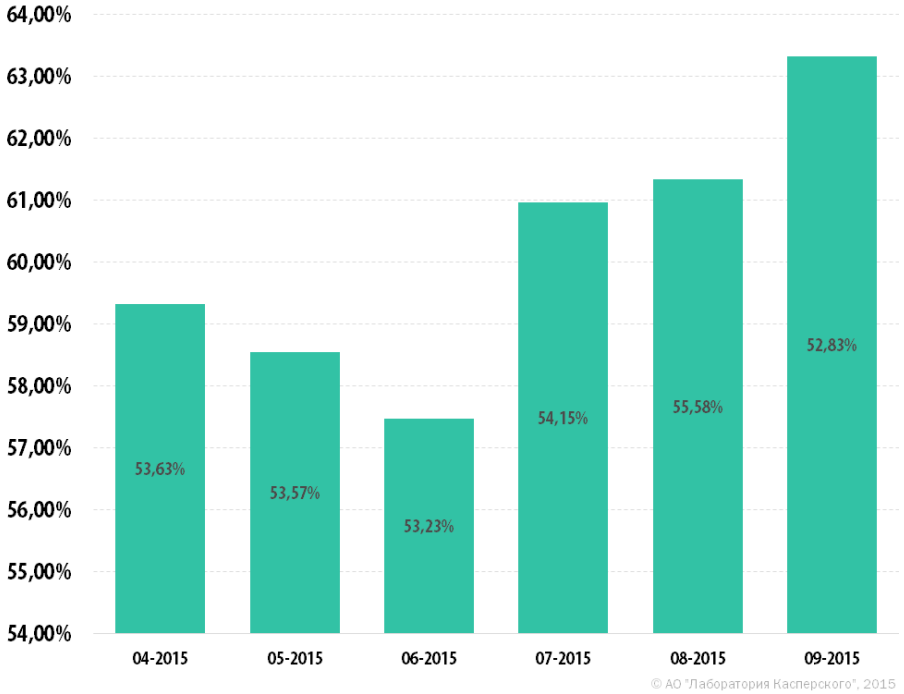
СТАТИСТИКА

Доля спама в почтовом трафике



Доля спама в мировом почтовом трафике, апрель – сентябрь 2015 года

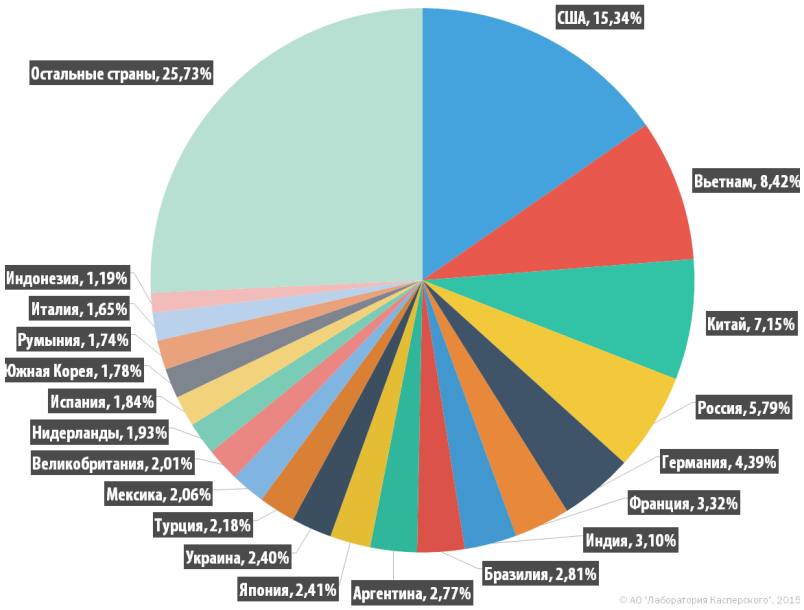
После относительно стабильных месяцев второго квартала доля спама в мировом почтовом трафике снова начала меняться. Небольшой рост в июле и августе 2015 года сменился заметным падением в сентябре. В итоге средний показатель доли спама за третий квартал составил 54,19%, что незначительно выше среднего показателя предыдущего квартала.



Доля спама в российском почтовом трафике, апрель – сентябрь 2015 года

Страны – источники спама

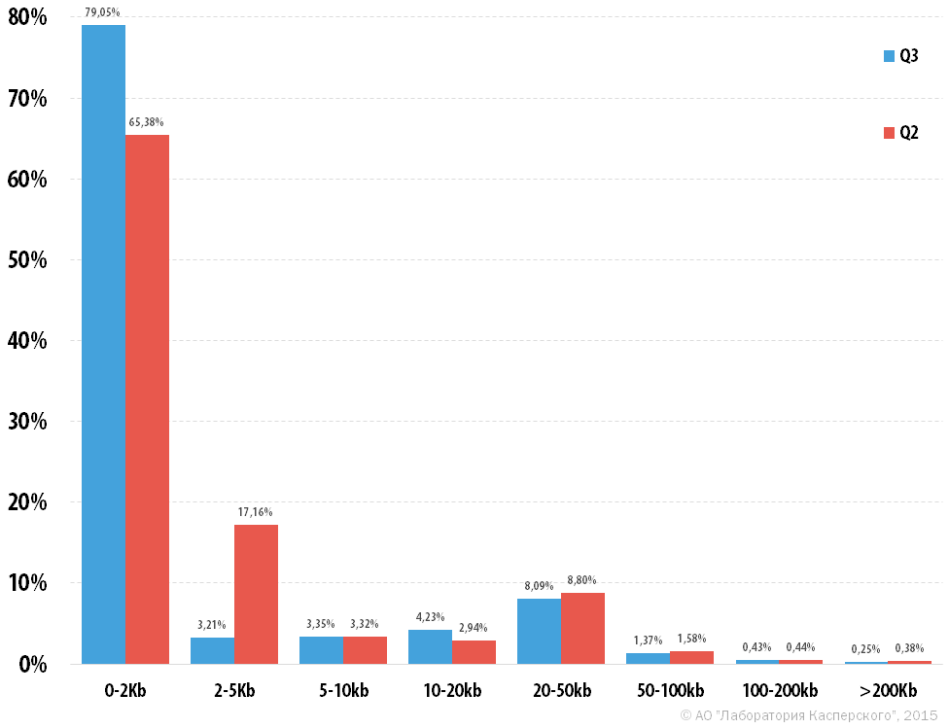
В третьем квартале 2015 года США (15,34%) сохранили за собой первую позицию среди стран – источников спама в мире. На вторую позицию поднялся Вьетнам (8,42%), чей показатель вырос на 3,38 п.п. по сравнению с предыдущим кварталом. Замыкает первую тройку Китай (7,15%), доля этой страны практически не изменилась за прошедшие три месяца.



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

Доля России (5,79%) в третьем квартале снизилась на 2,03 п.п., и страна опустилась со второй позиции на четвертую. За ней следуют Германия (4,39%) и Франция (3,32%), показатели этих стран незначительно изменились по сравнению с предыдущим кварталом.

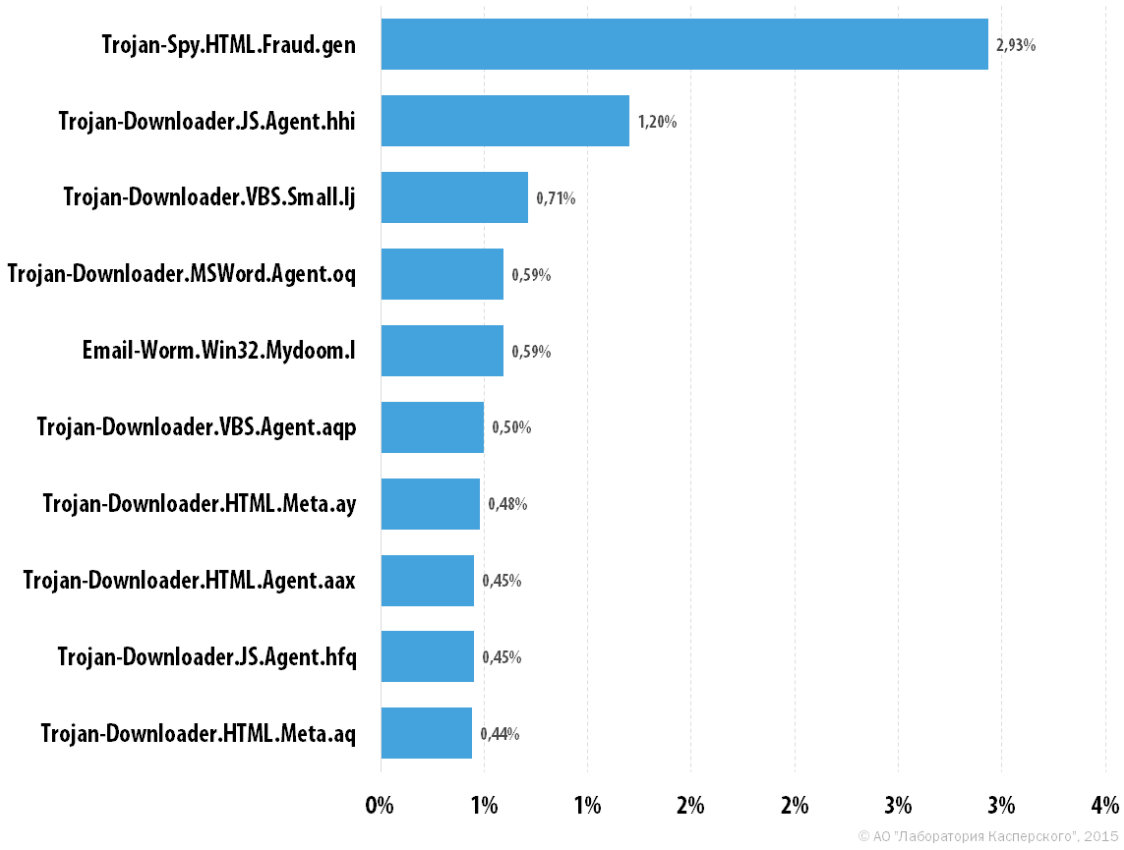
Размеры спамовых писем



Размеры спамовых писем, второй и третий кварталы 2015 г.

Самыми рассылаемыми письмами в третьем квартале стали очень маленькие, от 2 Кб и менее (79,05%), их доля выросла на 13,67 п.п. по сравнению с предыдущим кварталом. Примерно на то же количество процентных пунктов снизилась доля писем объемом от 2 до 5 Кб (3,21%). Доля всех остальных писем незначительно изменилась по сравнению с предыдущим кварталом.

ВРЕДОНОСНЫЕ ВЛОЖЕНИЯ В ПОЧТЕ



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

Самой популярной среди распространяемых в почте вредоносных программ в третьем квартале 2015 года по-прежнему остаётся Trojan-Spy.HTML.Fraud.gen. Этот зловред представляет собой фишинговую HTML-страницу и рассылается под видом важного сообщения от крупных коммерческих банков, интернет-магазинов, компаний-разработчиков ПО и других организаций.

Вторую и девятую строки нашего TOP 10 занимают загрузчики Trojan-Downloader.JS.Agent.hhi и Trojan-Downloader.JS.Agent.hfq. Эти зловреды представляют собой обфусцированный Java-скрипт. Загрузчики используют технологию ADODB.Stream, которая позволяет им скачивать и запускать файлы DLL, EXE и PDF.

На третьей и шестой сточках расположились загрузчики Trojan-Downloader.VBS.Small.lj и Trojan-Downloader.VBS.Agent.aqp. Это VBS-скрипты, которые также использует технологию ADODB.Stream, загружают ZIP-архивы и запускают извлеченное из них вредоносное ПО.

На четвертой позиции разместился Trojan-Downloader.MSWord.Agent.oq. Этот зловред представляет собой DOC-файл со встроенным VBS-макросом, который выполняется при открытии документа. Макрос скачивает с сайта злоумышленников другой VBS-скрипт и запускает его на компьютере пользователя.

Замыкает первую пятерку Email-Worm.Win32.Mydoom.l. Этот червь распространяется в виде вложений в электронные письма, через файлообменные сети и открытые на запись сетевые ресурсы. Адреса для рассылки писем зловред

собирает на уже зараженных компьютерах. Своим владельцам червь предоставляет возможность удаленно управлять инфицированной системой.

На седьмой, восьмой и десятой строчках расположились Trojan-Downloader.HTML.Meta.ay, Trojan-Downloader.HTML.Agent.aax и Trojan-Downloader.HTML.Meta.aq соответственно. Эти зловреды представляют собой HTML-страницы с кодом для переадресации пользователя на сайт злоумышленника. Там жертву обычно ждет фишинговая страничка или предложение скачать программу для работы с сервисом автоматической торговли бинарными опционами. Распространяются зловреды через почтовые вложения и различаются только ссылкой, перенаправляющей пользователя на сайт злоумышленников.

Семейства вредоносных программ

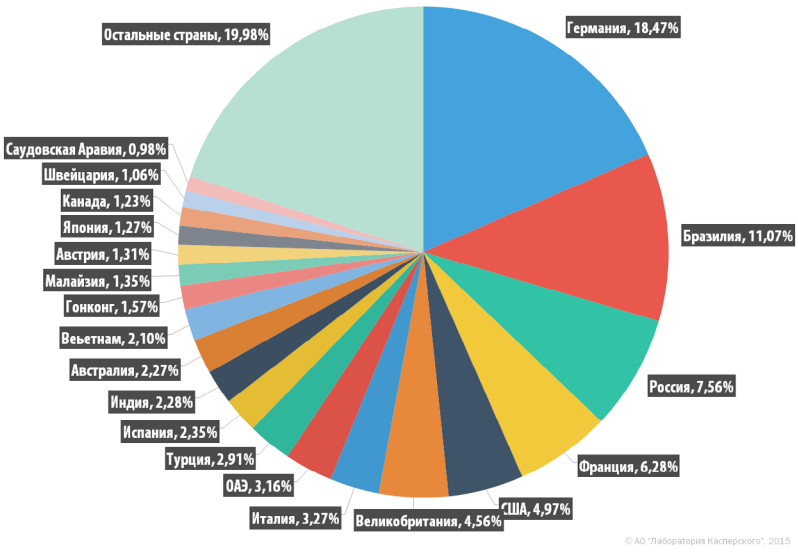
Как и в первых двух кварталах 2015 года список самых распространённых семейств возглавил загрузчик Upatre (9,46%). Чаще всего зловреды этого семейства скачивают на компьютеры жертв троянца-банкера, известного как Dyre/Dyzap/Dyreza.

На второй позиции по-прежнему находится семейство MSWord.Agent (5,55%). Напомним, что зловреды этого семейства представляют собой DOC-файл 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 бэкдоров Andromeda.

Замыкает тройку лидеров семейство VBS.Agent (5,44%). В отличие от MSWord.Agent здесь используется встроенный VBS-скрипт. Для загрузки и запуска различного вредоносного ПО на компьютере пользователя зловреды семейства используют технологию ADODB.Stream.

Страны — мишени вредоносных рассылок

И снова тройка лидеров стран, на территорию которых рассылается наибольшее количество вредоносного спама, претерпела серьёзные изменения. Самым большим из них стало появление на третьей строчке России (7,56%). За квартал ее показатель вырос на 2,82 п.п., и страна поднялась с 5-го места на третье.



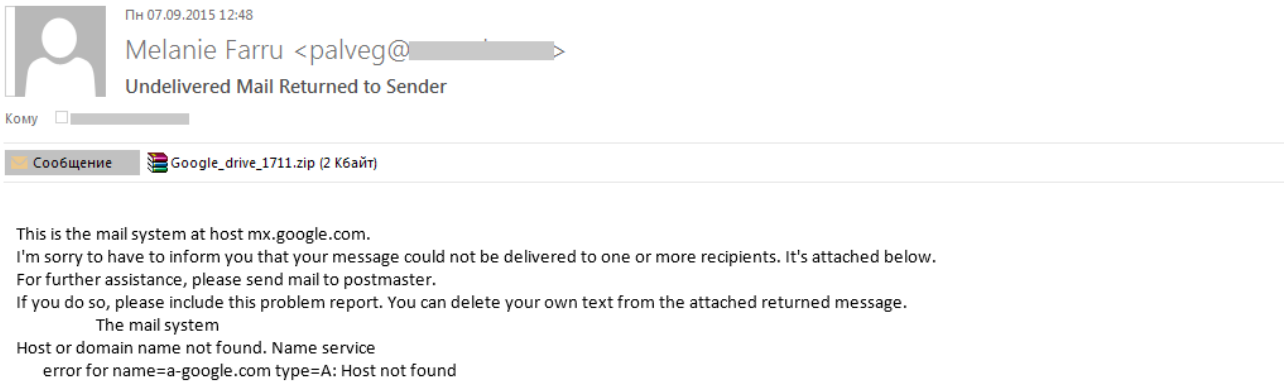
Распределение срабатываний почтового антивируса по странам, третий квартал 2015 г.

Первое место по-прежнему занимает Германия (18,47%), чей показатель уменьшился на 1,12 п.п. На второй строчке Бразилия (11,7%), количество вредоносного спама, разосланного пользователям этой страны, возросло почти вдвое по сравнению со вторым кварталом.

Великобритания (4,56%), занимавшая в предыдущем квартале вторую строчку, оказалась на шестой позиции.

Особенности вредоносного спама

В начале сентября в спам-трафике мы обнаружили масштабную вредоносную рассылку, письма который выглядели как автоответы почтового сервера о недоставке. Текст и тема сообщения были похожи на автоматическое уведомление, однако адрес отправителя принадлежал частному лицу, что вызывало сомнение в легитимности письма. Вложенный архив в формате ZIP с именем «Google_drive_1711» тоже настораживал, поскольку уведомления от почтового сервиса не содержат вложений. Исследование показало, что в архиве находился троянец Trojan-Downloader.JS.Agent.hhi, который в свою очередь скачивал бэкдор Backdoor.Win32.Androm.


Пн 07.09.2015 12:48
Melanie Farru <palveg@
Undelivered Mail Returned to Sender
Кому
Сообщение
Google_drive_1711.zip (2 Кбайт)

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

В начале третьего квартала злоумышленники активно рассылали письма на французском языке, содержащие макровирусы. Обнаруженные нами макровирусы принадлежали к категории троянцев-загрузчиков и использовались для загрузки и установки на компьютеры жертв банковского троянца Dridex. Для обмана получателя мошенники выдавали сообщения за уведомления о получении заказа или счета.

Вт 21.07.2015 13:04
Corrine CABAL <CorrineCABALtnnb@
Notre avis doperation bancaire N503518/29833859
Сообщение
503518_29833859.xls (58 Кбайт)

uf erreur ou omission de votre part, la facture qui vous a été adressée
pas été régularisée au sein de notre service de comptabilité.
ous nous permettons de vous rappeler que léchéance est arrivée à terme le
-07-2015.
erci de faire le nécessaire.
os vous prions dagréer, Madame, Monsieur, nos salutations distinguées.

Ср 22.07.2015 14:18
Nick Becker <Angelita.fed8@
RELANCE FACTURES NF19416/277018
Кому morgane
Сообщение
morgane_F19416_277018.doc (20 Кбайт)

MADAME, MONSIEUR
Je vous remercie de votre commande du 16/07/2015 et vous adresse en pièce jointe le duplicata de la facture.
Je vous rappelle que vous devez la conserver car elle tient lieu de garantie.
Vous en souhaitant bonne réception.
Très cordialement

Вт 21.07.2015 10:22
Gwenaelle DESPRES <
Commande - CD2533
Сообщение
Format A4.docm (24 Кбайт)

adame, Monsieur,
ous vous remercions pour votre nouvelle "Commande - CD2533".
ous revenons vers vous au plus vite pour les de'lais
eilleures salutations,
:DISCOM SECURITE

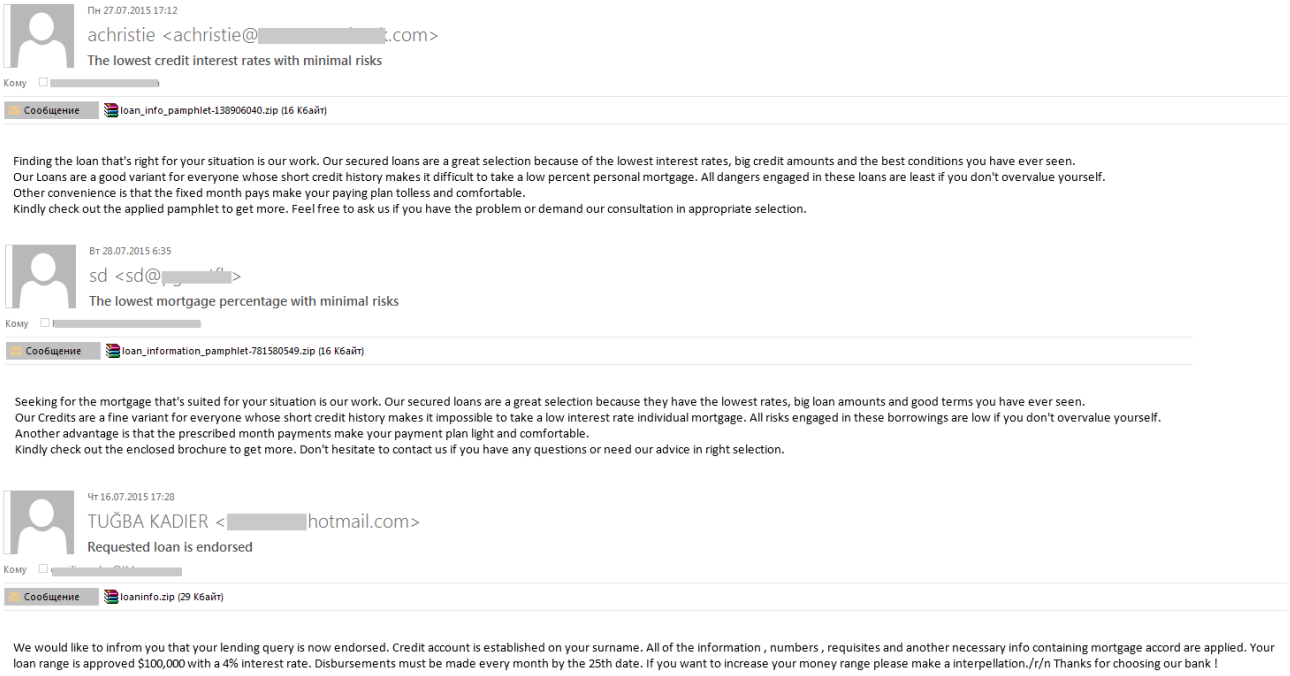
Ср 22.07.2015 14:07
Mervin Norris <Deloris.
Facture N125081/555056
Кому carmemunar
Сообщение
carmemunar 125081 555056.doc (21 Кбайт)

Bonjour,
Ci joint la facturation de juin 2015.

Ср 22.07.2015 14:13
Josh Buck <Kim.83@
RELANCE FACTURES ND62896/595201
Кому
Сообщение
jimar_DG2896_595201.doc (19 Кбайт)

Bonjour ,
Veuillez trouver ci-joint les factures.
- No. D62896/595201
Vous trouverez sur les factures, en bas de la page, nos coordonnées bancair
Bonne réception.
Cordialement,
Josh Buck

Также в июле спамеры использовали для распространения вредоносных файлов традиционную для рекламного спама тему кредитов. В некоторых зафиксированных нами письмах мошенники предлагали взять кредит, привлекая потенциальных клиентов самыми выгодными условиями, низкими процентными ставками и др. В других сообщениях получателя уведомляли, что его заявка на кредит одобрена. Отметим, что подобное содержание может встретиться и в простом рекламном спаме, однако для вредоносного спама характерно вложение, маскирующееся под подробную информацию о кредите.



Пн 27.07.2015 17:12
achristie <achristie@[redacted].com>
The lowest credit interest rates with minimal risks
Кому [redacted]
Сообщение loan_info_pamphlet-138906040.zip (16 Кбайт)

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

Вт 28.07.2015 6:35
sd <sd@[redacted]>
The lowest mortgage percentage with minimal risks
Кому [redacted]
Сообщение loan_information_pamphlet-781580549.zip (16 Кбайт)

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

Чт 16.07.2015 17:28
TUĞBA KADIER <[redacted]hotmail.com>
Requested loan is endorsed
Кому [redacted]
Сообщение loaninfo.zip (29 Кбайт)

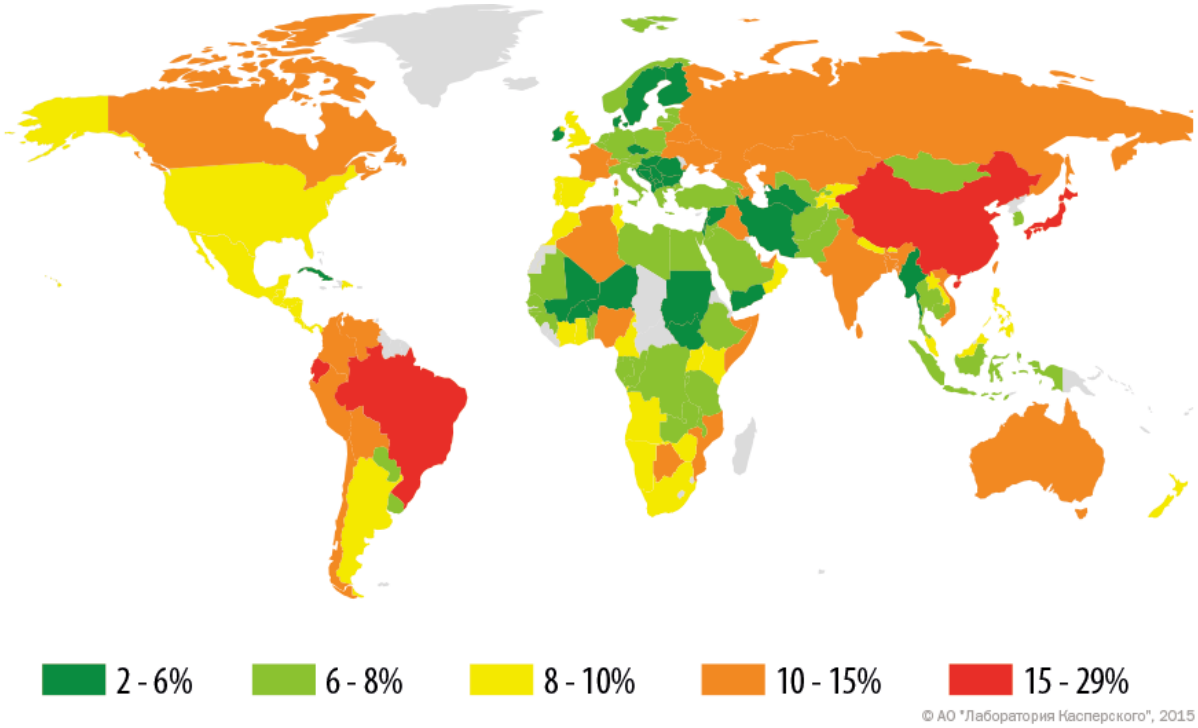
We would like to infrom you that your lending query is now endorsed. Credit account is established on your surname. All of the information , numbers , requisites and another necessary info containing mortgage accord are applied. Your loan range is approved $100,000 with a 4% interest rate. Disbursements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

Интересно, что вредоносные письма, содержащие во вложении троянец Trojan-Downloader.Win32.Upatre, рассылались на адреса сотрудников различных компаний.

ФИШИНГ

В третьем квартале 2015 года с помощью системы «Антифишинг» мы предотвратили **36 300 537** попыток перехода пользователей продуктов «Лаборатории Касперского» на фишинговые сайты. Это на 6 миллионов больше по сравнению с показателями предыдущего квартала. Из них **15 764 588** попыток перехода заблокировано нашими эвристическими компонентами детектирования и **20 535 949** – с помощью детерминистик. За этот же период в базы добавлено **839 672** маски фишинговых URL.

Страной с наибольшей долей атакованных фишерами пользователей по-прежнему остается Бразилия (21,07%). В третьем квартале доля атакованных жителей этой страны увеличилась на 11,33 п.п., т.е. фактически вернулась к показателю первого квартала.



География фишинговых атак, третий квартал 2015 года*

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

Также сильно выросла доля атакованных пользователей в Японии (+10,9 п.п.) и Китае (+7,85 п.п.), эти две страны заняли соответственно второе и третье места в нашем TOP 10.

TOP 10 стран по проценту атакованных пользователей:

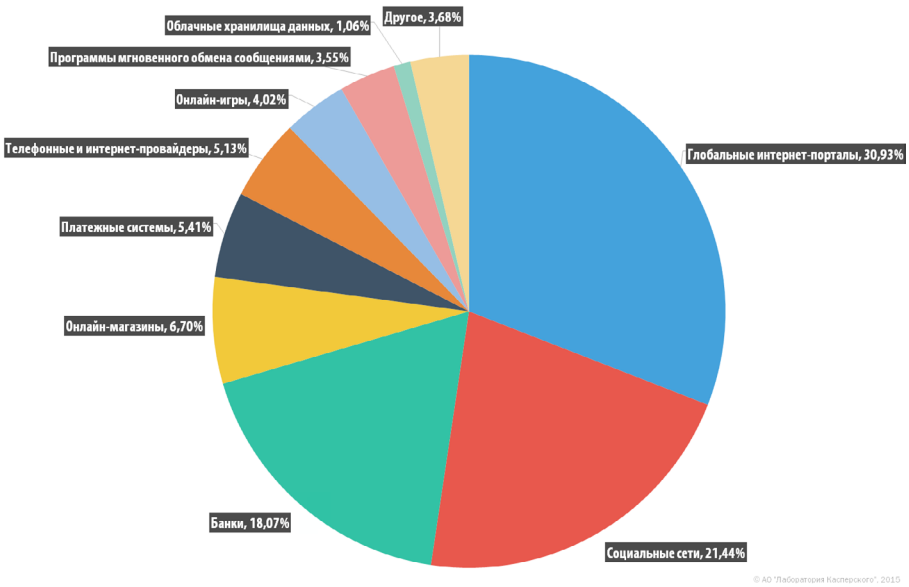
	Страна	% пользователей
1	Бразилия	21,07
2	Япония	16,86

3	Китай	15,08
4	Вьетнам	14,50
5	Бангладеш	13,32
6	Нигерия	13,05
7	Россия	12,91
8	Казахстан	12,85
9	Индия	12,44
10	Колумбия	12,25

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.

В третьем квартале заметно уменьшилась доля категории «Глобальные интернет-порталы» (30,93%), бессменного лидера рейтинга организаций, атакованных фишерами. Падение составило 11,42 п.п. Зато доля категории «Социальные сети и блоги» (21,44%) вновь выросла – на 6,69 п.п. Третью позицию заняла категория «Банки» (18,07%), чья доля выросла на 4,65 п.п. Также в полтора раза увеличилась доля категории «Онлайн-игры» (4,02%).



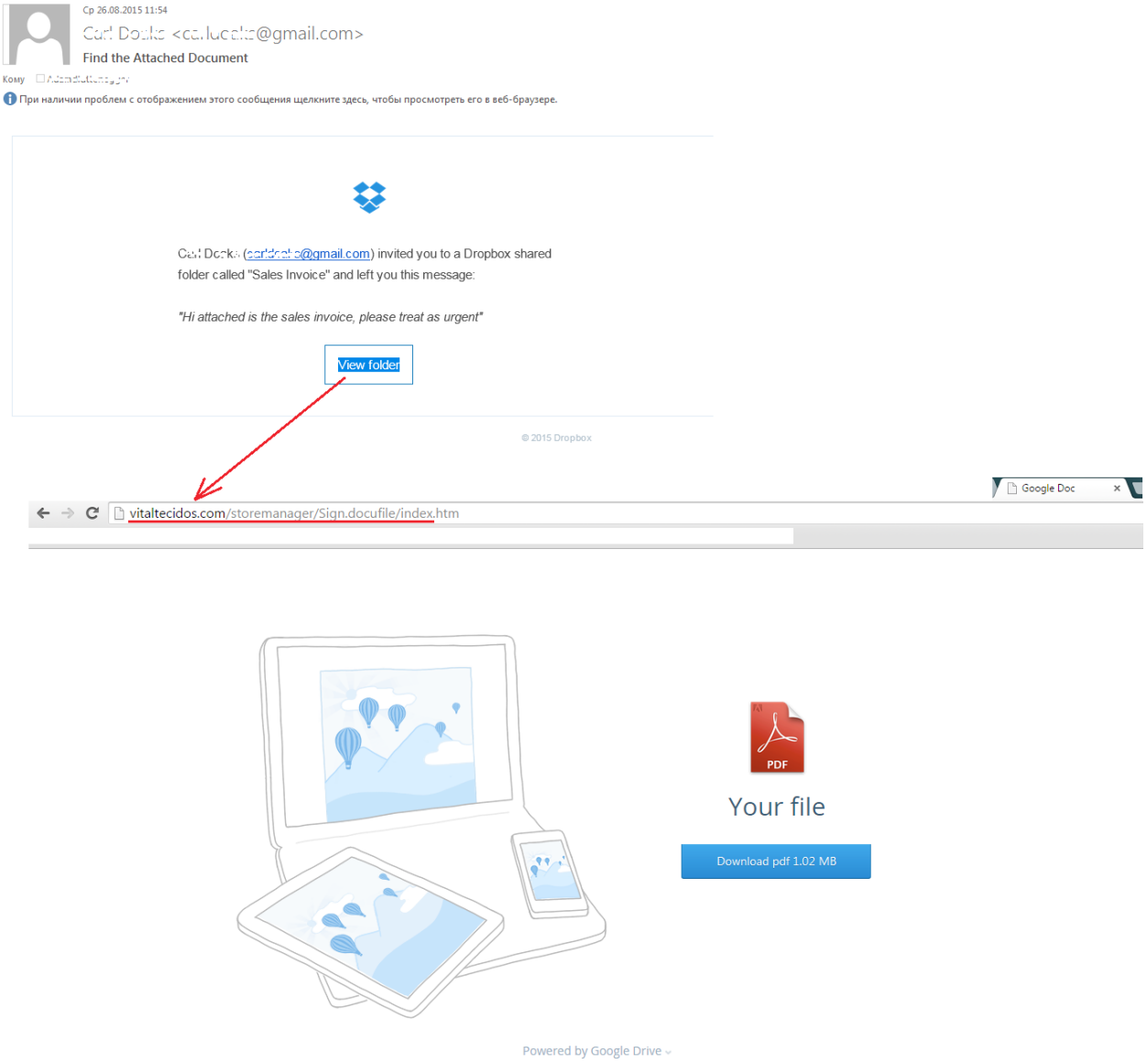
Распределение организаций, атакованных фишерами, по категориям, третий квартал 2015 г.

Доля фишинга на организации категории «Облачные хранилища данных» увеличилась на 0,26 п.п. и составила 1,06%. Пользователи все активней используют технологии облачного хранения данных, и это привлекает внимание мошенников. Украденная информация используется злоумышленниками в целях шантажа, продажи третьим лицам, организации целевых атак.

Часто такой фишинг распространяется по электронной почте или социальным сетям в виде сообщения с призывом скачать тот или иной документ, якобы выложенный на популярном облачном сервисе. Сообщения могут приходить от скомпрометированных аккаунтов из списка друзей или, в случае электронной почты, от имени администрации облачного сервиса.

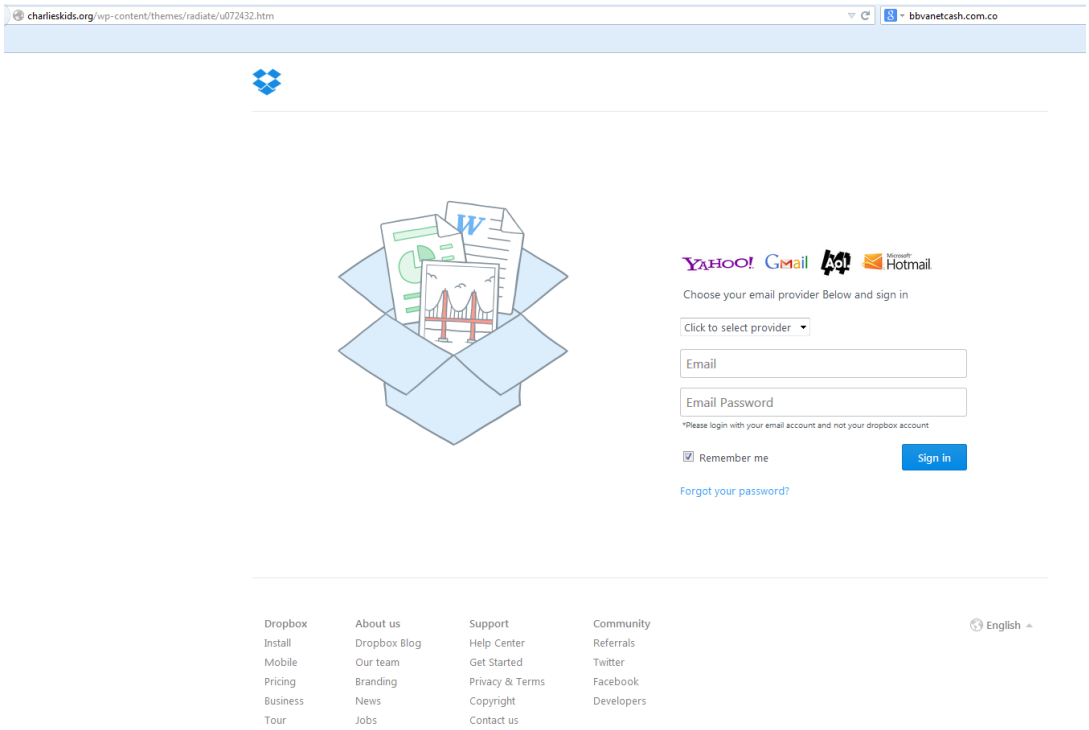
Посредством фишинговых страниц, имитирующих сайты известных облачных хранилищ, могут распространяться и различные вредоносные программы. В таких случаях пользователь, кликнув по ссылке на странице, самостоятельно загружает вредоносную программу на свой компьютер.

Ниже приведен пример атаки, где пользователю предлагается скачать важный PDF-документ. Ссылка из письма ведет на фишинговую страницу, стилизованную под сайт популярного облачного сервиса Dropbox.



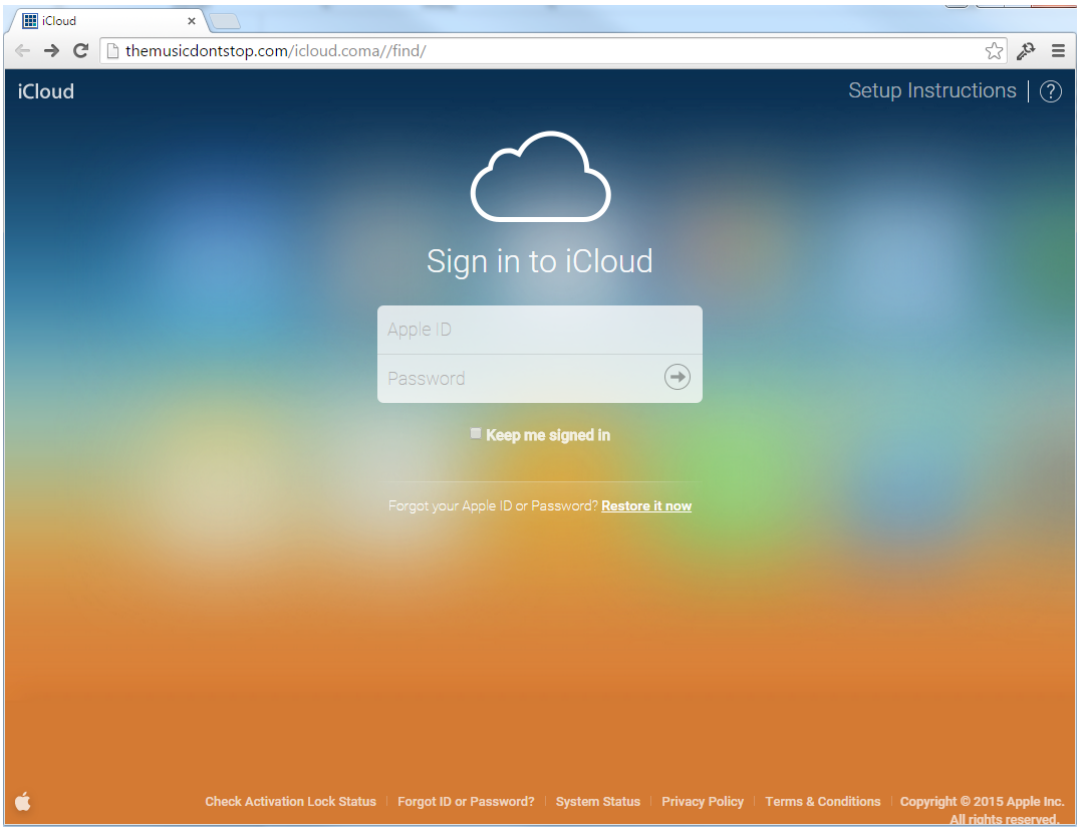
Пример фишинговой атаки на пользователей Dropbox

Помимо кражи хранящихся в облаке данных и распространения вредоносных программ, киберпреступники часто используют имя Dropbox для кражи данных почтового аккаунта жертвы.



Пример фишинговой страницы, использующей бренд Dropbox

А вот другой пример фишинга: мошенники пытаются украсть у пользователя AppleID и пароль к облачному хранилищу данных iCloud.



Пример фишинга на пользователей iCloud

Помимо прочего, в случае успеха злоумышленники получают доступ к приобретенному пользователем контенту и его почтовому ящику.

TOP 3 атакуемых организаций

Мошенники продолжают концентрировать свои силы на самых популярных брендах, направляя на них основную часть нецелевого фишинга. Таким образом они рассчитывают повысить шансы на успех очередной фишинговой атаки. Более половины всех срабатываний эвристической компоненты нашей системы «Антифишинг» приходится на фишинговые страницы, прикрывающиеся именем менее чем 30 известных компаний.

На TOP-3 атакуемых организаций в третьем квартале пришлось 26,39% всех срабатываний эвристической компоненты.

	Организация	% срабатываний
1	Yahoo!	15,38
2	ВКонтакте	9,44
3	Facebook	8,95

В третьем квартале в тройке атакуемых фишерами организаций произошли некоторые изменения. Лидером среди атакуемых организаций по-прежнему является Yahoo! (15,38%), однако ее доля уменьшилась почти в два раза – на 13,65 п.п. На второе место вышла российская социальная сеть ВКонтакте (9,44%), другая социальная сеть – Facebook (8,95%) – потеряла 1,49 п.п. и сместилась со второй позиции на третью.

ЗАКЛЮЧЕНИЕ

Доля спама в почтовом трафике по итогам третьего квартала 2015 года составила 54,2%, что на 0,8 п.п. меньше, чем в предыдущем квартале. Тройка лидеров среди стран – источников спама, рассылаемого по всему миру, в третьем квартале выглядит следующим образом: США (15,3%), Вьетнам (8,4%) и Китай (7,2%).

Сезон отпусков и летних каникул вызвал рост вредоносного спама туристической тематики. Киберпреступники рассылали поддельные уведомления от имени известных сервисов бронирования отелей, авиакомпаний и отелей, а также письма от частных лиц. Как правило, в такие письма были вложены архивы с различными троянцами-загрузчиками.

Первую строчку в рейтинге вредоносных программ, распространенных в почте, по итогам третьего квартала по-прежнему удерживает Trojan-Spy.HTML.Fraud.gen. Среди семейств вредоносных программ лидером на протяжении всего года также остается семейство Upatre. Наиболее часто вредоносным атакам в третьем квартале подвергались пользователи Германии – на их долю пришлось 18,5% срабатываний почтового антивируса.

Особенностью квартала стало использование создателями фишинговых писем нового трюка для обхода спам-фильтра: они помещали текст сообщения и мошенническую ссылку не в тело письма, а во вложенный PDF-документ.

Всего в третьем квартале решения «Лаборатории Касперского» предотвратили более 36 млн. попыток перехода на фишинговые сайты, что на 6 млн. больше показателя предыдущего квартала. Страной с наибольшей долей атакованных фишерами пользователей по-прежнему остается Бразилия (21,07%).

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