СПАМ И ФИШИНГ ВО ВТОРОМ КВАРТАЛЕ 2014

ДАРЬЯ ГУДКОВА

НАДЕЖДА ДЕМИДОВА

KASPERSKY lab

CONTENTS

СПАМ: ОСОБЕННОСТИ КВАРТАЛА

СПАМ И ЗАКОНОДАТЕЛЬСТВО

С 1 июля вступил в силу новый антиспамовый закон в Канаде - Canada's anti-spam legislation (CASL). Под юрисдикцию нового закона попадают коммерческие сообщения, включая рассылки по электронной почте, сообщения в социальных сетях и сервисах обмена мгновенными сообщениями, а также SMS. Теперь прежде чем рассылать письма, компания должна получить согласие получателя. Канадские компании отнеслись к будущему закону серьезно: во втором квартале мы видели множество писем от различных канадских компаний с просьбой подтвердить свое согласие на получение их рассылок. В таких письмах наряду с просьбой подтвердить свое согласие на получение массовой корреспонденции встречались даже предложения поучаствовать в розыгрыше призов, пройдя по ссылке в письме.

Отметим, что некоторые компании воспользовались законом как поводом для сбора адресов подписчиков. Мы видели запросы на согласие получать рассылки даже в ящиках-ловушках, адреса которых никогда не были подписаны ни на какие рассылки. Кроме того, многие пользователи, получив такое письмо-запрос, отмечали его как спам.

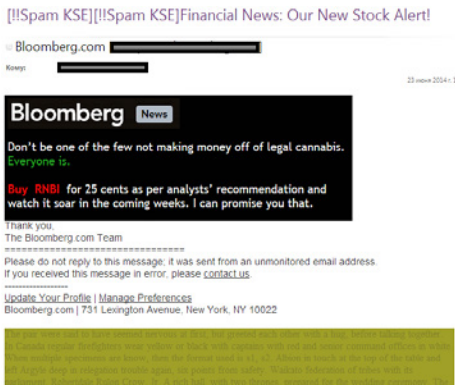
Из этого потока запросов видно, что многие канадские рассыльщики ранее не задумывались о желании пользователей получать их корреспонденцию, а просто рассылали свои письма по большим покупным адресным листам.

Интернет-сообщество восприняло закон двояко. С одной стороны, наличие антиспамового закона еще в одной стране несомненно принесет пользу в борьбе со спамом. С другой стороны, легальный канадский бизнес, использующий рассылки, опасается, что теперь они могут быть расценены как незаконные. Так, компания Microsoft сначала и вовсе решила отказаться от своих новостей по безопасности, но уже через несколько дней передумала, что в целом неудивительно: при всей строгости CASL в законе множество исключений, и рассылки Microsoft никак не подпадают под его юрисдикцию. Среди исключений CASL можно найти рассылки с различной информацией о продукте или услуге, которую пользователь приобрел у компании; рассылки, направленные на сбор пожертвований; некоммерческие рассылки и многое другое.

СНОВА БИРЖЕВЫЕ АКЦИИ!

Во втором квартале 2014 нам часто встречался спам, в котором рекламировались биржевые акции мелких компаний. Это хорошо известный вид биржевого мошенничества, который называется «накачка и сброс». Пик такого спама пришелся на 2006-2007 годы, однако злоумышленники по-прежнему его используют.

«Накачка и сброс» одна из форм махинаций на фондовом рынке, когда спамеры покупают акции мелких компаний, искусственно раздувают цены на акции за счет распространения в своих рассылках ложной позитивной информации о состоянии этих фирм, а потом продают акции по новым, более высоким ценам.


[!!Spam KSE][!!Spam KSE]Financial News: Our New Stock Alert!

Bloomberg.com [redacted]

Кому: [redacted]

Bloomberg News

Don't be one of the few not making money off of legal cannabis. Everyone is.

Buy RNBI for 25 cents as per analysts' recommendation and watch it soar in the coming weeks. I can promise you that.

Thank you.
The Bloomberg.com Team

Please do not reply to this message; it was sent from an unmonitored email address.
If you received this message in error, please contact us.

Update Your Profile | Manage Preferences
Bloomberg.com | 731 Lexington Avenue, New York, NY 10022


[!! SPAM]BestStock of 2014

GetitForPennies [redacted]

Кому: [redacted]

Initially it was at 19 cents. Now it's at almost 40. Our experts think it will go past 2dollars pretty quickly.

RCHA is a hell of a stock. Very few people know about it and it is going up every day like clockwork.

If you want to make a smart move in such a volatile market I think RCHA is your best option right now.

Theropoda, September 1, 2010. In 2007 the same company produced a revised version at Theatre 36, Dublin as part of their centenary celebrations. Rams to pull off the first major upset of the 2007 tournament. Northern Irish Metro Championship in 1998, where he won his first title. After Nina's attack, her father never touched them again. Last Days of the Romanovs, Robert Wilton, p. A day later the Soviet Union ceased to exist. Spotting


From: InvestorsHub [mailto:[redacted]
Sent: Friday, June 20, 2014 9:17 PM
To: [redacted]
Subject: [!!Spam KSE][!! SPAM]Daily Stocks Tips

Strong Buy Stocks for Today's Stock Market

Rainbow International, Corp. (RNBI)
0.22 ↑ (30.89%)

INVESTORSHUB

The remaining were settled in other countries. She is only 8 years older than Reba McEntire who plays Reba. Luis is a politician that is trying to gain trust in the community. Charlotte Observer October 2, 2006 Monday Jeff Elder Pg. Kuzco is getting sick of living without his Emperor luxuries, so he pretends to be sick to tap into the royal funds. Retrieved on June 1, 2011. Oshry opened a boy's yeshiva and a girl's yeshiva in the East Bronx. As of 2011, there were 8,278 eligible voters living within the district. Lenny Guarente, Cold Spring Harbor Press, NY. K with parking included. Frequently, it snows from October to May off and on. Location of Magnier Peninsula on Graham Coast, Antarctic Peninsula. ERA and 6 strikeouts, pitching 7.

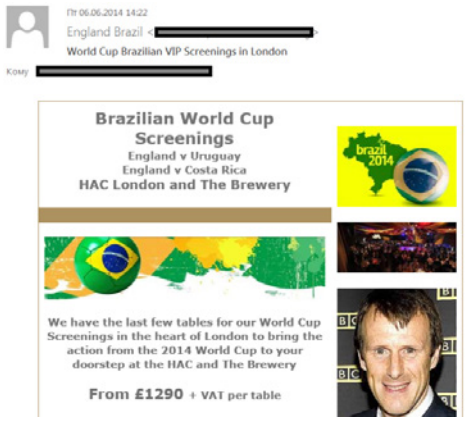
Интересно, что помимо старых мошеннических трюков были использованы и старые трюки по обходу фильтров:

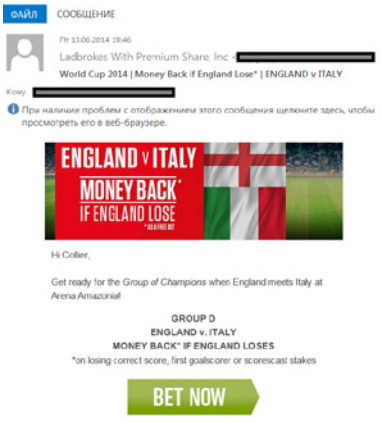
- 1. Случайный набор предложений, вставленный в конец каждого письма и оформленный цветом, близким к цвету фона (в данных рассылках были взяты случайные предложения из «Википедии»);
- 2. Графический спам: основная информация находится на картинке, причем от письма к письму в рассылке случайным образом изменяется цвет и размер текста, шрифт, цвет фона и угол поворота картинки.

Графический спам был также популярен в 2006-2007 годах, а потом практически сошел на нет, так как антиспамовые вендоры разработали графические анализаторы и научились успешно блокировать подобные письма. К тому же из-за излишнего замусоривания такой спам вряд ли привлечет много заинтересовавшихся пользователей. Видимо поэтому «акционные» рассылки все время идут гигантскими объемами: спамеры рассылают сотни миллионов писем, надеясь на минимальный отклик.

СПАМ И ЧЕМПИОНАТ МИРА ПО ФУТБОЛУ

Если в первом квартале 2014 года среди спортивных событий у спамеров была популярна Олимпиада, то во втором квартале – Чемпионат мира по футболу. Мы зафиксировали разнообразные рассылки, использующие эту тему. Подробно прочитать про фишинговые и вредоносные атаки, использующие тему Чемпионата, можно в нашем блоге. Но помимо опасных писем были и просто рекламные сообщения с предложениями по бронированию мест в отелях и на стадионе, различной рекламой околочемпионатной тематики, а также письма с предложением ставок на исходы матчей.



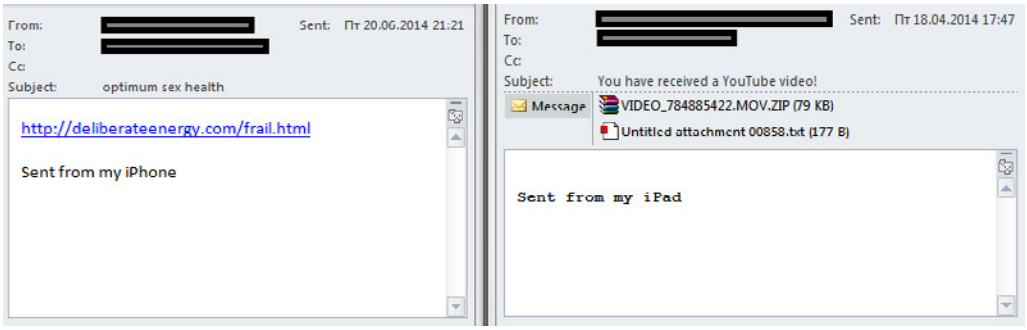


Как обычно в подобных случаях, тема Чемпионата была задействована и в спаме, тематика которого напрямую с данным событием не связана. К примеру, изобретательные немецкие спамеры использовали данную тематику для рекламы виагры:

«После окончания Чемпионата мира оставайтесь чемпионом в своей спальне!» - гласит лозунг на рекламном сообщении.

SENT FROM IPHONE: МОБИЛЬНАЯ ТЕМА В ПОЧТЕ

Продолжая тему интеграции почтового спама и мобильных устройств, отметим, что во втором квартале 2014 года пользовались популярностью спам-рассылки, подделанные под письма с устройств iPad и iPhone. Письма были довольно разнообразными – от рекламы медикаментов до сообщений с вредоносными вложениями. Все они в теле письма содержали одну и ту же строку «Sent from iPhone/iPad».



В первом примере по ссылке через несколько редиректов открывался сайт с рекламой медикаментов для повышения потенции, во втором во вложении находилась вредоносная программа, детектируемая «Лабораторией Касперского» как Trojan-PSW.Win32.Tepfer.tmyd.

Скорее всего, рассылки были разосланы разными спамерскими группами, так как технические заголовки писем (такие как Data, X-Mailer, Message-ID) сильно отличались. Так, в некоторых письмах заголовки были проставлены весьма неаккуратно, а некоторые поля вообще не были прописаны. Собственно, общей с реальными письмами с устройств на платформе iOS у них была только фраза в теле письма. В других же письмах заголовки были не просто аккуратными, но и имитировали заголовки, которые проставляет настоящий почтовый клиент от Apple:

X-Mailer: iPhone Mail (9B206)

Message-Id: UNQC4G8K-NTOU-2PNZ-JUVC-WHRCD5GXS1QF@*****.**

Однако если посмотреть внимательней, то заголовки лишь выглядят похожими на реальные (по количеству символов и расположению дефисов). Дело в том, что у настоящих писем с

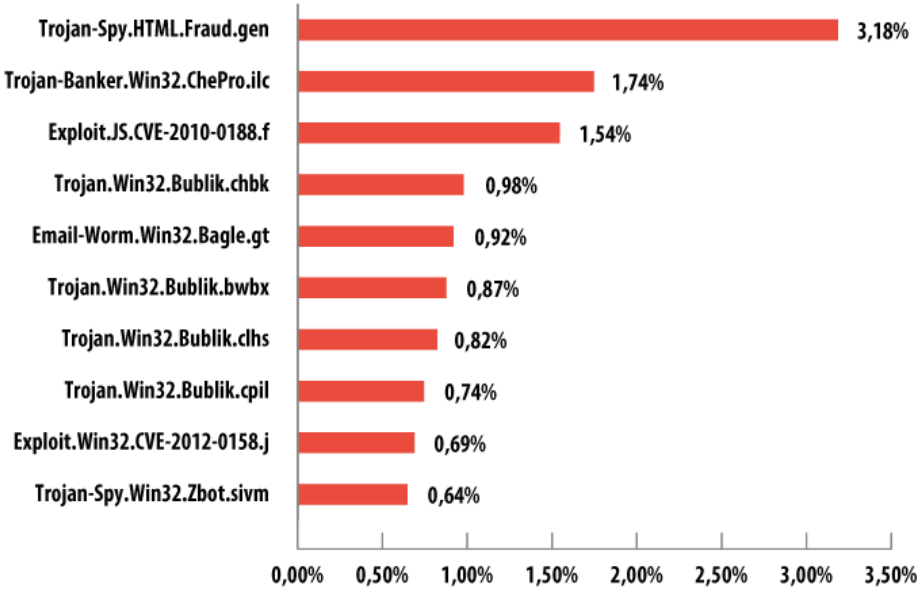
мобильных устройств iOS для записи Message-ID используется шестнадцатеричный код. В шестнадцатеричный формат исчисления входят цифры от 0 до 9 и буквы abcdef. То есть ничего, кроме цифр и этих букв в Message-ID быть не должно. В поддельных же письмах мы видим просто случайный набор букв и цифр.

РЕДИРЕКТЫ

Для обхода фильтров злоумышленники часто пытаются скрыть адрес сайта, на который должен пройти пользователь. Способов сокрытия спамерских ссылок много, и один из весьма распространенных – когда ссылки в письмах ведут на взломанные сайты, с которых пользователь перенаправляется на целевой сайт. Этот сайт может быть рекламным и/или содержать вредоносный код. Обычно взломанные сайты включаются в систему редиректов просто потому, что именно их киберпреступники смогли взломать. Но иногда злоумышленники охотятся на них прицельно. Так, нам встретилась рассылка, в которой пользователь через взломанный сайт перенаправлялся на рекламу фармацевтических препаратов. При этом взломаны были сайты именно фармацевтической тематики (rxpharmacy*****.com). Такой таргетинг преступники используют, чтобы ссылка, по которой проходит пользователь, не вызывала у него подозрений.

Кроме того, последнее время среди взломанных сайтов нам часто встречаются сайты церковных обществ. Вряд ли в данном случае речь идет о таргетированном взломе и социальной инженерии, вероятно, защите подобных сайтов просто уделяется мало внимания.

ВРЕДОНОСНЫЕ ВЛОЖЕНИЯ В ПОЧТЕ



TOP 10 вредоносных программ, распространенных в почте, второй квартал 2014 г.

Самым популярным среди распространяемых в почте вредоносных программ по-прежнему остается Trojan-Spy.HTML.Fraud.gen. Напомним, этот зловред представляет собой фишинговую HTML-страницу, на которой пользователь должен ввести свои конфиденциальные данные. Затем вся введенная информация отправляется киберпреступникам. Заметим, что доля этого зловреда снизилась по сравнению с предыдущим кварталом (-1,67%).

На второе место вышел банкер Trojan-Banker.Win32.ChePro.ilc. Этот троянец нацелен на персональные данные клиентов бразильских и португальских банков.

На третье место первый раз за долгое время вышел эксплойт (Exploit.JS.CVE-2010-0188.f). Эксплойты в почте наиболее опасны, так как выполнены они не в виде исполняемых файлов, а в виде безобидных офисных документов. Данный эксплойт представляет собой PDF-файл

и использует уязвимость в Acrobat Reader версии 9.3 и ниже. Надо отметить, что данная уязвимость известна довольно давно, и пользователям, регулярно обновляющим программное обеспечение на компьютере, этот эксплойт не страшен. Однако если версия Adobe старая, то после эксплуатации уязвимости на компьютер устанавливается и запускается исполняемый файл, который детектится «Лабораторией Касперского» как Trojan-Dropper.Win32.Agent.lcqs. Дроппер устанавливает и запускает javascript (Backdoor.JS.Agent.h), который собирает информацию о системе, отправляет ее на сервер злоумышленников и получает от сервера различные команды. Команды и результаты их выполнения пересылаются в зашифрованном виде.

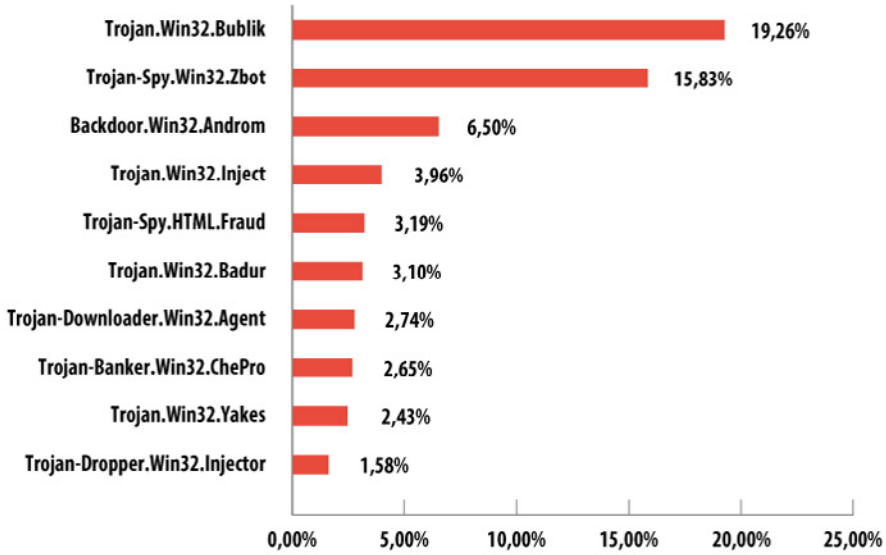
На 4, 6, 7 и 8 места вышли троянцы семейства Bublik. Это классические троянские программы, целью которых является несанкционированная пользователем загрузка и установка на компьютер-жертву других вредоносных программ. Троянцы представляют собой EXE-файлы, но с помощью иконки маскируются под документы Adobe. Часто они загружают на компьютер пользователя небезызвестную вредоносную программу ZeuS/Zbot.

На пятом месте находится почтовый червь Email-Worm.Win32.Bagle.gt. Основная функция всех почтовых червей — собирать электронные адреса с зараженных компьютеров. Почтовый червь семейства Bagle также может принимать удаленные команды на установку других вредоносных программ.

На девятое место в этом рейтинге также попал эксплойт - Exploit.Win32.CVE-2012-0158.j. Он выполнен в виде документа Microsoft Word и эксплуатирует уязвимость в коде mscomctl.ocx в Microsoft Office. Результатом его работы является установка и запуск на компьютере пользователя вредоносного ПО.

На десятом месте расположился Trojan-Spy.Win32.Zbot.sivm. Вредоносные программы семейства ZeuS/Zbot способны выполнять различные вредоносные действия (их функционал со временем пополняется), но чаще всего они используются для воровства банковской информации. Также Zbot может устанавливать CryptoLocker – вредоносную программу, шифрующую данные пользователя и вымогающую деньги за их расшифровку.

Что касается наиболее популярных семейств, а не отдельных модификаций, то распределение за квартал несколько другое:

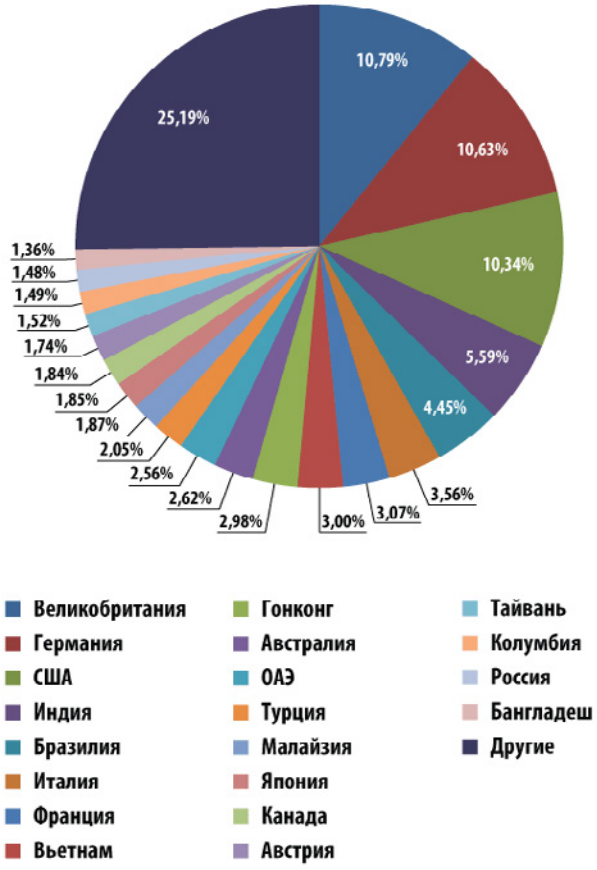


TOP 10 семейств вредоносных программ, распространенных в почте, второй квартал 2014 г.

Bublik (который часто подгружает Zbot), а также сам Zbot, выходят на первые места с большим отрывом от остальных семейств, попавших в рейтинг. Суммарно на этих зловредов приходится более трети от общего количества срабатываний на вредоносные программы в почте. Это вполне объяснимо, ведь большинство вредоносных программ используются для кражи денег пользователей, а Zeus/Zbot – одна из самых известных и доступных таких программ.

На третьем месте располагается бэкдор семейства Androm. Такие программы позволяют злоумышленникам незаметно управлять зараженными компьютерами, которые часто становятся частью ботнета.

СТРАНЫ - МИШЕНИ ВРЕДОНОСНЫХ РАССЫЛОК



Распределение срабатываний почтового антивируса по странам, второй квартал 2014 г.

В TOP 20 стран, куда рассылается больше всего вредоносного спама, по сравнению с первым кварталом произошли некоторые изменения. Доля вредоносного спама, нацеленного на пользователей в США, несколько сократилась (-3,5%), из-за чего США перешли с первого места на третье, пропустив вперед Великобританию и Германию. Из других заметных изменений – в 2,5 раза увеличилась доля вредоносного спама, рассылаемого в Бразилию, из-за чего эта страна поднялась в рейтинге с 15-го места на 5-е. Произошло это за счет банкера семейства ChePro, более 80% которого было разослано пользователям в Бразилии.

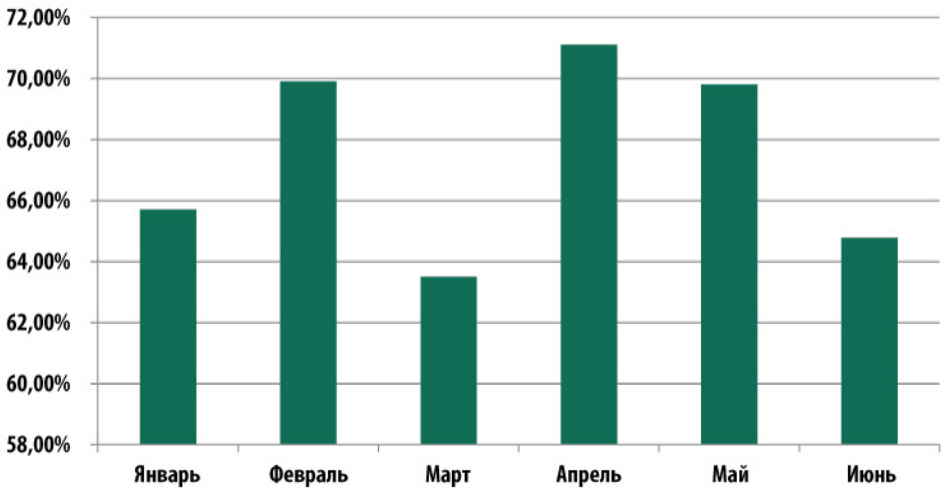
ОСОБЕННОСТИ ВРЕДОНОСНОГО СПАМА

Злоумышленники очень часто маскируют спам с вредоносными вложениями под письма от известных организаций – служб доставки, магазинов, социальных сетей. Но, как правило, все подобные рассылки имитируют регулярно приходящие пользователям письма (счет за услуги, сообщение о статусе доставки и т.д.). В этом квартале мы заметили более креативную в плане социальной инженерии рассылку, которая была разослана якобы известной сетью кофеен Starbucks.

В сообщениях говорилось, что один из друзей получателя, пожелавший остаться неназванным, якобы сделал для него заказ в кофейне Starbucks. Ознакомиться с меню, а заодно узнать адрес и точное время празднования, можно, открыв вложение, — исполняемый файл, который киберпреступники даже не потрудились замаскировать.

СТАТИСТИКА ПО СПАМУ

ДОЛЯ СПАМА



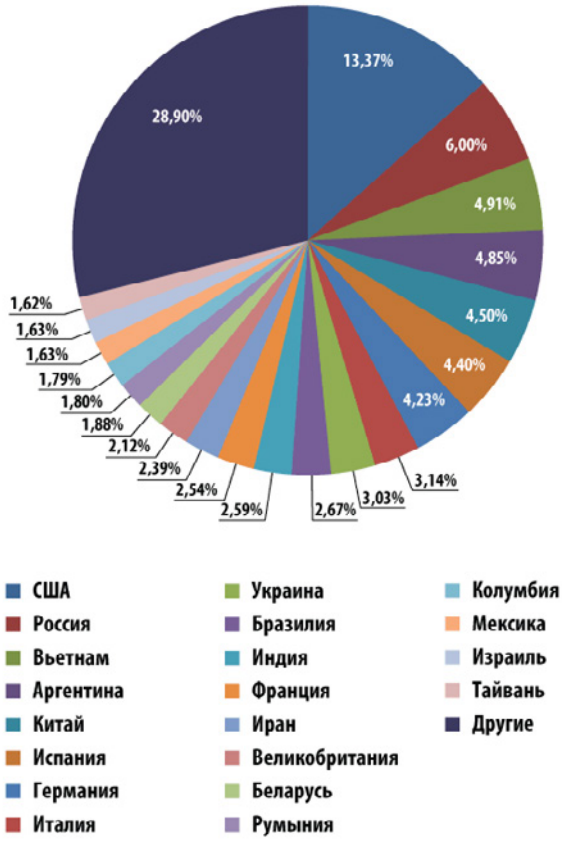
Доля спама в почтовом трафике, январь – июнь 2014 г.

Доля спама в почте по итогам второго квартала составила 68,6%, что на 2,2% больше, чем в предыдущем квартале. Набольшее за квартал количество спама было разослано в апреле, далее доля нежелательных сообщений в трафике постепенно снижалась.

СТРАНЫ – ИСТОЧНИКИ СПАМА

Ранее мы считали статистику по странам - источникам спама по данным, полученным из собственных спам-ловушек, находящихся в разных странах. Но спам, который приходит в ловушки, все-таки отличается от спама, который идет реальным пользователям. К примеру, в ловушки не попадает таргетированный спам, нацеленный на профильные компании. Поэтому мы изменили источник данных и теперь с помощью KSN (Kaspersky Security Network) получаем

статистику по тем сообщениям, которые приходят пользователям наших продуктов по всему миру. Поскольку данные для статистики по странам – источникам спама за этот квартал взяты из другого источника, сравнение полученных результатов со статистикой за предыдущий период было бы некорректно.



Распределение источников спама по странам, второй квартал 2014 г.

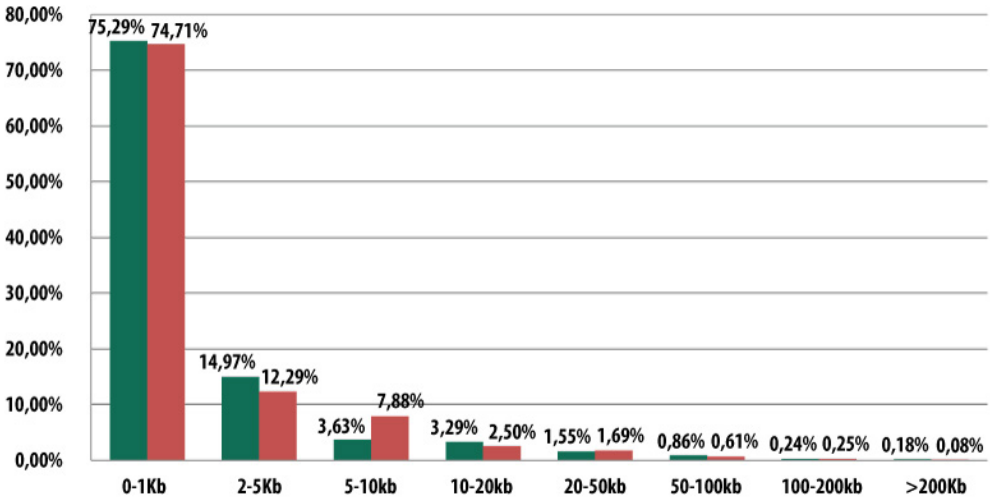
На первом месте среди стран - источников спама находятся США, 13,4% мусорной почты рассылается оттуда по всему миру. Это неудивительно, ведь США – страна с самым большим количеством интернет-пользователей. Даже при хорошей осведомленности пользователей об опасностях интернета, кому-то не удается избежать заражения компьютера, который в результате становится частью ботнета, рассылающего спам.

Дальнейшее распределение источников спама по странам довольно равномерное. В целом это оправдано: ботнеты распределены по миру, зараженные компьютеры пользователей есть практически в любой стране.

На втором месте идет Россия, из нее рассылается 6% мирового спам-трафика. На третье место вышел Вьетнам (5%).

По нашей статистике хорошо видно, что во многих странах изрядную долю приходящего пользователям спама составляет «внутренний спам», то есть спам, источником и адресатом которого является одна и та же страна. Так, во втором квартале среди спама, отправленного в Россию, 18% было отослано из России, а в США доля «внутреннего спама» составила 27,2%. Ту же тенденцию можно наблюдать и в некоторых других больших странах, из которых рассылается значительная часть мирового спама. В маленькие же страны спам приходит, в основном, извне.

РАЗМЕРЫ СПАМОВЫХ ПИСЕМ



Размеры спамовых писем, второй квартал 2014 г.

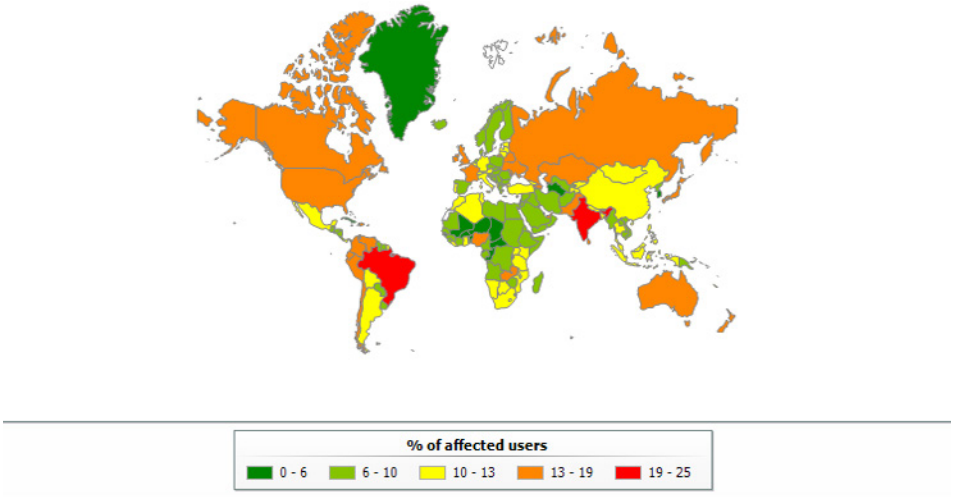
Распределение спамовых писем по размерам практически не поменялось по сравнению с первым кварталом. По-прежнему абсолютным лидером являются очень короткие письма размером до 1 Kb, что понятно их проще и быстрее рассылать.

Можно отметить небольшое снижение доли писем размером от 2Кб до 5Кб (-2,7%) и увеличение писем в диапазоне 5-10Кб (+4,2%). Такое увеличение обычно происходит за счет повышения доли графического спама, что мы и наблюдали во втором квартале. Во-первых, было много очень крупных рассылок биржевого мошенничества с картинками (о них мы писали выше). Во-вторых, часто встречался графический русскоязычный спам тематик «похудение» и «поддельные брендовые товары».

ФИШИНГ

Во втором квартале 2014 года на компьютерах пользователей продуктов «Лаборатории Касперского» было зафиксировано 60 090 173 срабатываний системы «Антифишинг».

Чаще всего фишеры атаковали пользователей в Бразилии – хотя бы раз в течение квартала система «Антифишинг» сработала на компьютерах 23,2% бразильских пользователей.



География фишинговых атак*, Q2 2014

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

ТОР 10 СТРАН ПО ПРОЦЕНТУ АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ:

	СТРАНА	% АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ
1	**Бразилия**	23,2%
2	**Индия**	19,20%
3	**Пуэрто Рико**	18,60%
4	**Япония**	17,10%
5	**Франция**	17,00%
6	**Армения**	16,80%
7	**Доминиканская Республика**	16,20%
8	**Россия**	16,10%
9	**Австралия**	16,10%
10	**Великобритания**	15,80%

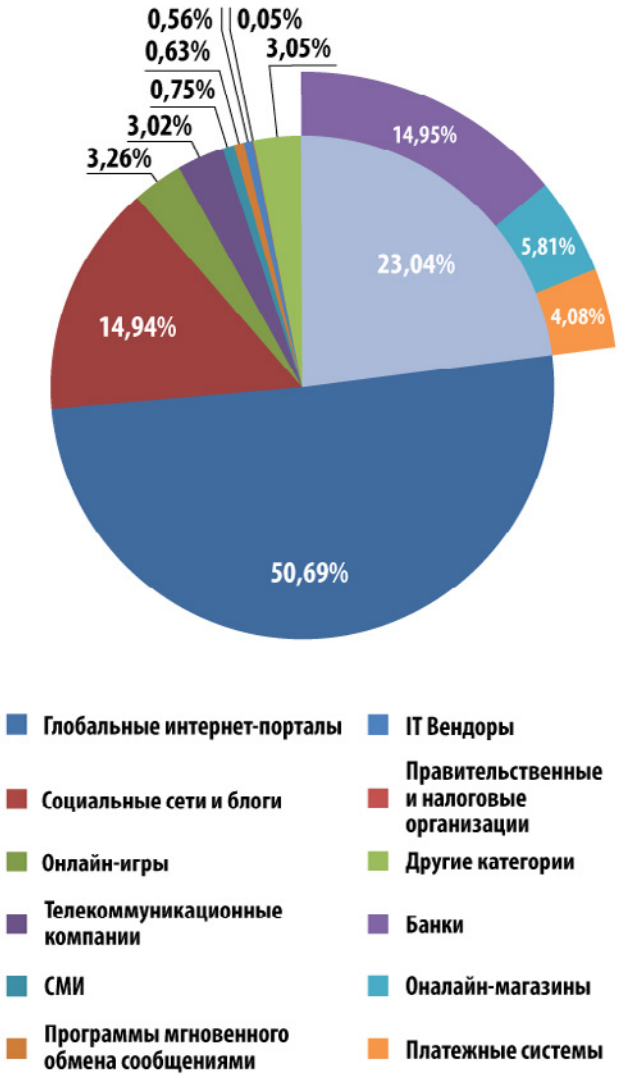
Бразилия вышла в ТОР 10 только в 2014 году. Активности фишеров, нацеленных на бразильских пользователей, могло способствовать проведение в Бразилии Чемпионата мира по футболу.

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. После срабатывания защитной системы пользователь видит в браузере предупреждающий баннер о возможной угрозе.

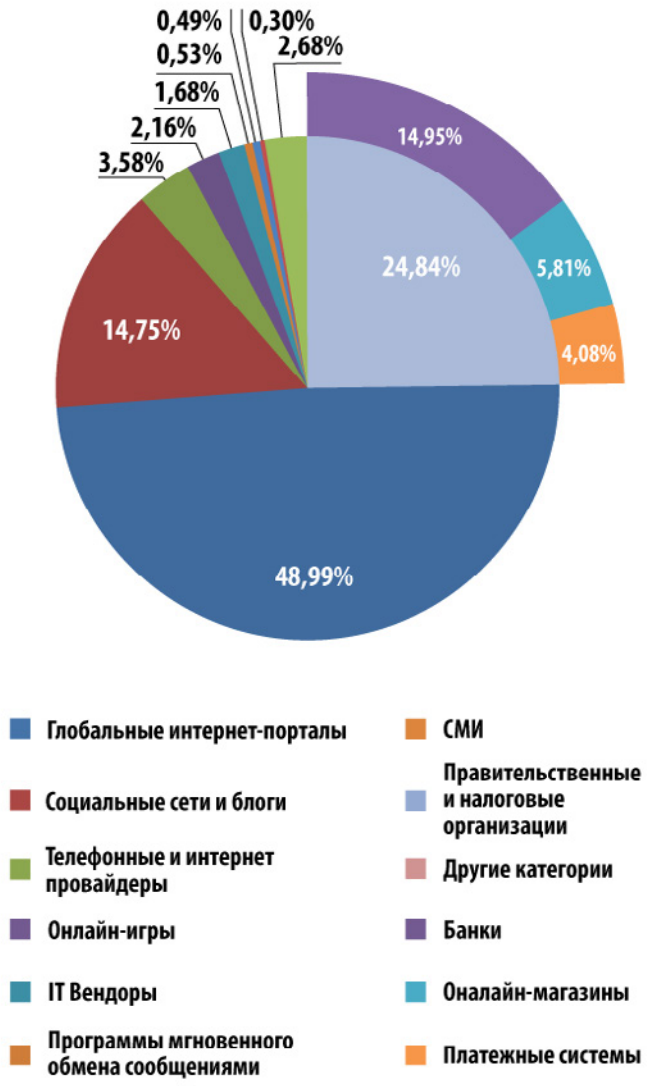
В предыдущих отчетах для анализа мишеней фишинговых атак мы использовали выборку ТОР 100 атакованных организаций. В этом квартале мы анализируем статистику по всем атакованным организациям.

В ходе атак на организации категорий «Банки», «Платежные системы» и «Онлайн-магазины, аукционы» злоумышленники охотятся за персональной информацией пользователей, которая дает доступ к их электронным счетам. Исходя из этого, мы сгруппировали эти три категории в один блок – «Онлайн-финансы».



Распределение организаций, атакованных фишерами, по категориям, второй квартал 2014 г.

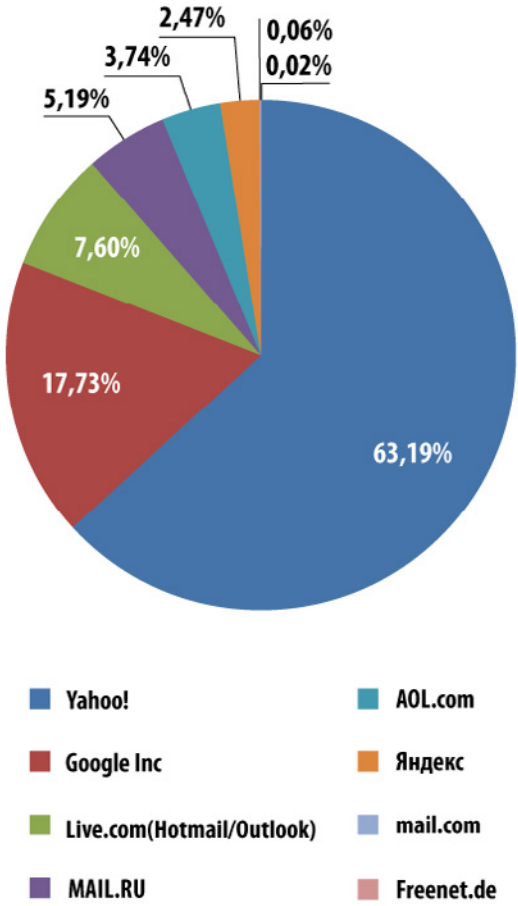
Для сравнения приводим аналогичные данные по первому кварталу:



Распределение организаций, атакованных фишерами, по категориям, первый квартал 2014 г.

Как и в первом квартале 2014 года, во втором квартале категория «Глобальные интернет-порталы» занимает верхнюю строчку рейтинга категорий атакуемых фишерами организаций,

ее показатель уменьшился всего на 1,7%. К данной категории мы отнесли порталы, объединяющие множество сервисов, включая поисковые и почтовые. Украв данные авторизации на таких порталах, мошенники получают доступ ко всем сервисам данного вендора. Чаще всего фишеры подделывают странички авторизации почтовых сервисов таких порталов.

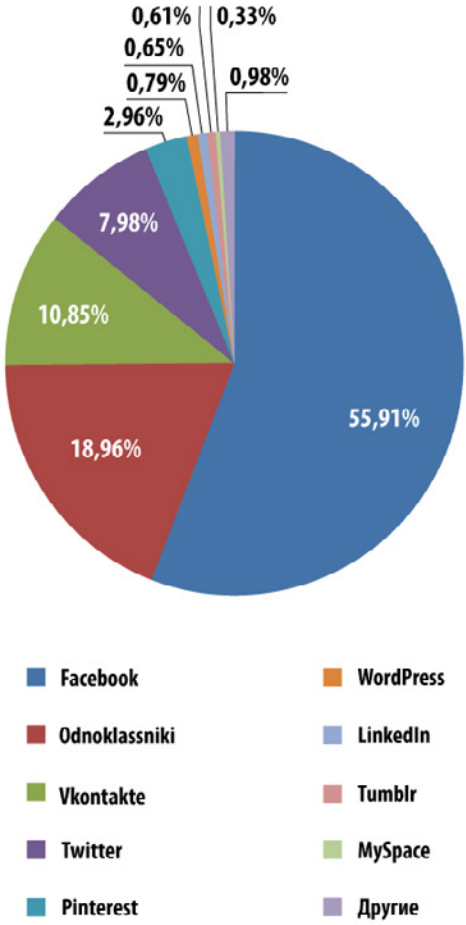


Распределение фишинговых атак на глобальные интернет-порталы*

** Рейтинг не является показателем уровня безопасности мишеней атак фишеров, а отражает популярность и авторитетность сервисов среди пользователей, что сказываются на их популярности у фишеров.*

На финансовый фишинг в целом пришлось 24,84% атак – на 1,8% больше, чем в первом квартале. Увеличилась доля срабатываний по категориям «Банки» (+0,93%) и онлайн-магазины(+0,85%).

«Социальные сети» по-прежнему на третьем месте.



Распределение фишинговых атак на социальные сети*

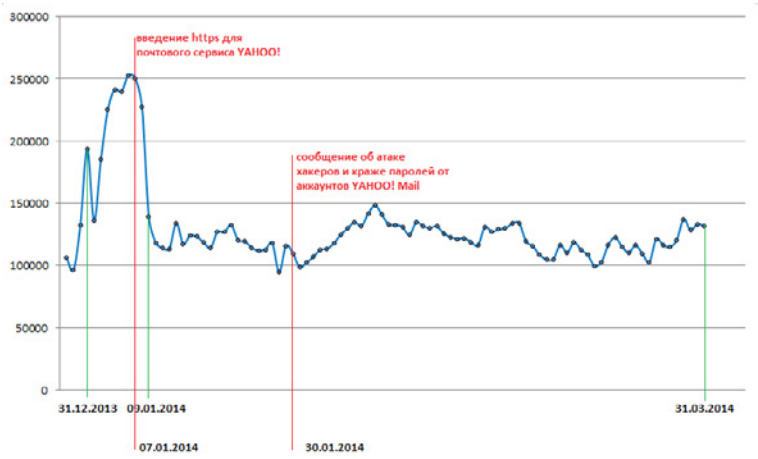
** Рейтинг не является показателем уровня безопасности мишеней атак фишеров, а отражает популярность и авторитетность соцсетей среди пользователей, что напрямую сказываются на их популярности у фишеров.*

В первом квартале на Facebook приходилось 79,5% об общего числа попыток перехода пользователей по ссылкам на поддельные страницы социальных сетей. Во втором квартале количество фишинговых атак на пользователей Facebook заметно уменьшилось (-23,54%). В то же время в этом распределении резко вырос процент попыток переходов пользователей на страницы-подделки под российские социальные сети - Одноклассники (+18,7%) и Вконтакте (+10,68%).

ТОР 3 АТАКУЕМЫХ ОРГАНИЗАЦИЙ

	ОРГАНИЗАЦИЯ	% ФИШИНГОВЫХ ССЫЛОК
1	Yahoo!	30,96%
2	Google Inc	8,68%
3	Facebook	8,1%

Во втором квартале фишинговые ссылки на поддельные страницы сервисов Yahoo! составили 30,96% всех атак.

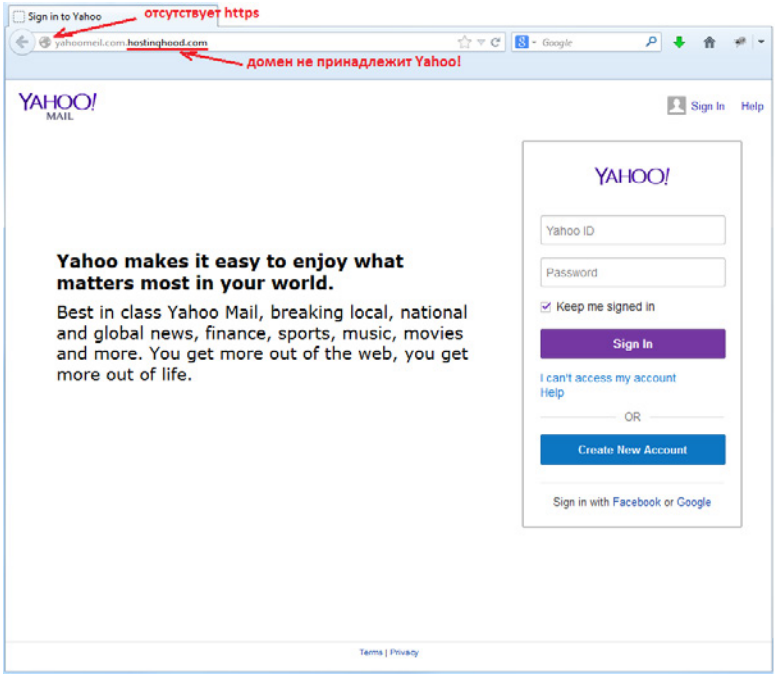


Число ежедневных срабатываний на фишинговых страницах, имитирующих страницы Yahoo!, Q1 2014

Yahoo! стал лидером рейтинга мишеней фишинговых атак в первом квартале 2014 года с показателем 31,94% после резкого увеличения числа подобных мошеннических ссылок в начале января.

Во втором квартале детектирование фишинговых ссылок на поддельные страницы Yahoo! не выявило пиков атак.

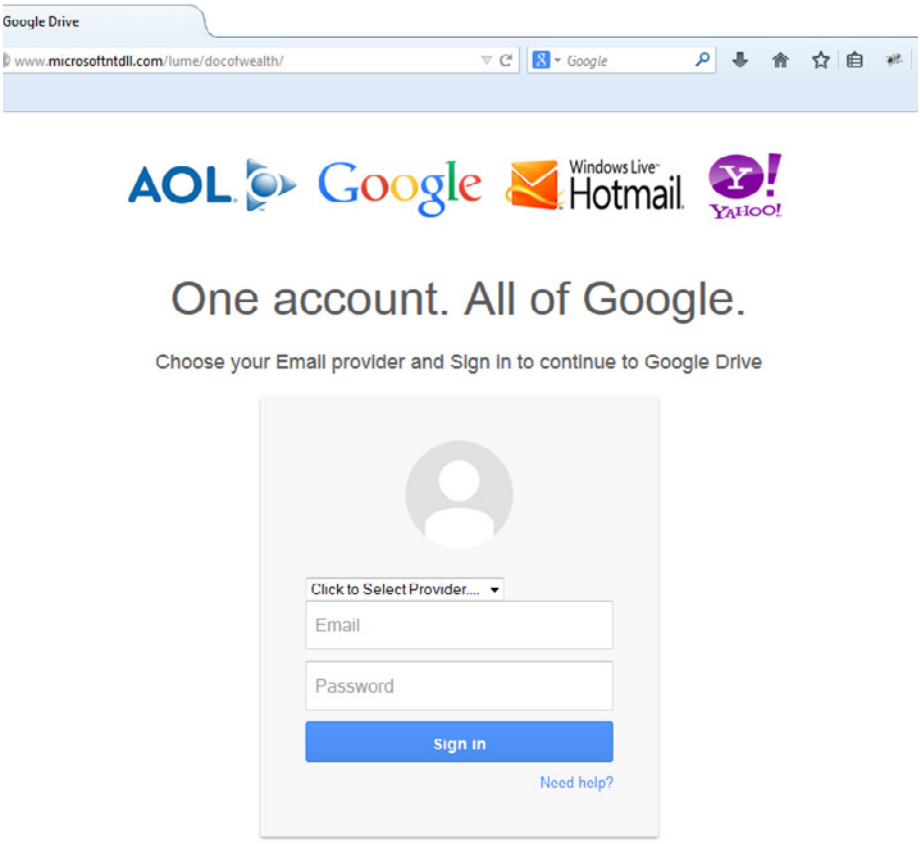
Еще в январе этого года в своем блоге компания Yahoo! Объявила о введении HTTPS по умолчанию для своего почтового сервиса. Данная мера безопасности, помимо защиты передаваемых данных, может помочь в борьбе с фишерами: теперь в тех случаях фишинга, когда доменное имя в адресной строке остается неизменным (например, происходит подмена DNS-сервера), отсутствие в адресной строке значка защищенного соединения должно насторожить пользователя. Однако, напомним, что отсутствие защищенного соединения является только одним из признаков фишинговой странички, и его наличие не дает гарантии подлинности сайта.



Классический пример фишинговой страницы, имитирующей страницу авторизации почтового сервиса Yahoo!

В этом квартале на втором месте среди всех атакуемых организаций, потеснив Facebook, оказался Google (8,68%). Если раньше фишеры в основном имитировали страничку входа в почту Gmail, то сейчас все чаще встречаются подделки под общую для всех сервисов Google страницу аутентификации. Несомненно, это очень привлекательная цель для фишеров – «Один аккаунт. Весь мир Google!».

В этом квартале мы наткнулись на любопытный пример жадности фишеров, которым одного мира Google явно мало:



На этой фишинговой страничке, которая имитирует страницу аутентификации всех аккаунтов Google, фишеры предусмотрели также возможность сбора паролей владельцев почтовых аккаунтов AOL, Hotmail и Yahoo!

Лидер прошлого года Facebook опустился еще на одну позицию и занял третье место по количеству срабатываний компонента «Антифишинг» (8,02%). Фишинговые атаки на пользователей социальных сетей значительно уступают атакам на посетителей глобальных интернет-порталов, однако они по-прежнему актуальны для фишеров, которые охотятся за аккаунтами пользователей по всему миру.

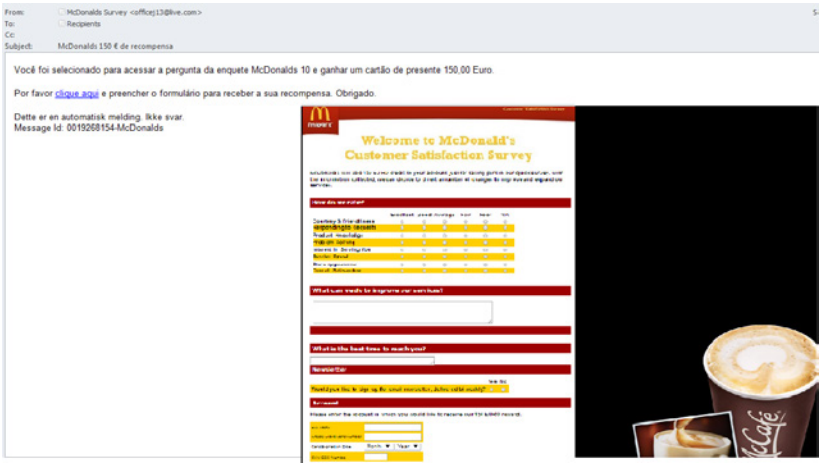
ГОРЯЧИЕ ТЕМЫ В ФИШИНГЕ

Основной «сезонной» темой для фишеров во втором квартале стал Чемпионат мира по футболу.

«Шанс выиграть билеты на следующую игру Кубка!»

Тему футбола мошенники эксплуатировали вплоть до окончания Чемпионата мира. Тематические рассылки появились еще в начале 2014 года и шли с завидной регулярностью в течение всего первого полугодия. Как правило, фишеры подделывали письма под сообщения от известных организаций (в основном, непосредственно FIFA), и предлагали пользователю пройти по ссылке на сайт, чтобы выиграть ценный приз. В качестве приза, как и в примере выше, часто выступали билеты на Чемпионат мира. На сайте от пользователя требовалось ввести свои персональные данные, в том числе данные кредитной карточки, за которыми и охотились мошенники.

Кроме того, фишерам в этом квартале приглянулось популярная сеть ресторанов быстрого питания McDonald's: в апреле злоумышленники попытались выманить данные банковских карточек у говорящих на португальском языке посетителей сети. В поддельном письме сообщалось, что адресат может получить 150 евро от сети McDonald's. Для этого ему необходимо пройти по ссылке, указанной в письме, и поучаствовать в опросе. На фишинговой странице, открывающейся по ссылке, пользователю предлагалось ответить на несколько вопросов, после чего ввести все данные банковской карты якобы для зачисления денежных средств. Именно за этими данными и охотятся злоумышленники, а доверчивые пользователи и не подозревают, что передают свою персональную информацию третьим лицам.



Отметим, что мошенническое письмо было написано на португальском языке и скорее всего, было рассчитано на жителей Бразилии и Португалии, однако текст опроса был на английском. Как правило, подобные «опросы» фишеры проводят на английском языке.

ЗАКЛЮЧЕНИЕ

Во втором квартале нам встречалось много рассылок от различных канадских организаций, которые хотели получить согласие пользователей на получение рассылок прежде, чем вступит в силу новый антиспамерский закон в Канаде. При этом недобросовестные компании, стараясь привлечь новых людей, часто рассылали такие запросы по спискам адресов пользователей, среди которых были не только получатели их рассылок. Тем не менее, закон начал приносить определенный эффект даже до своего вступления в силу.

Одной из популярных тематик спама во втором квартале стал биржевой спам, используемый в мошенничестве по схеме «накачка и сброс». Любопытно, что распространители спама этой старой тематики пытались обойти фильтры, используя старые методы: графический спам и «белый текст».

Мобильная тема в спаме продолжилась в этом квартале подделками под письма с устройств на платформе iOS. Большинство подделок были сделаны без учета деталей и специфики этой операционной системы, что позволило без проблем поймать эти рассылки.

На первом месте среди вредоносных программ, распространенных через почту во втором квартале 2014, остается Fraud.gen – шпион, ворующий банковские данные. На второе вышел бразильский троянец-банкер ChePro. Среди вредоносных семейств наиболее популярными оказались Bublik и Zeus/Zbot. Интересно, что в этом квартале в TOP 10 первый раз за долгое время вошли два эксплойта, причем один из сразу на 3-е место.

Тема Чемпионат мира по футболу активно использовалась как в рекламе обычных товаров, так и во вредоносном и фишинговом спаме. Доля вредоносного спама, отправленного в Бразилию во втором квартале, увеличилась по сравнению с первым кварталом в 2,5 раза (в основном за счет троянца-банкера семейства ChePro). Кроме того, Бразилия вышла на первое место среди атакованных фишерами стран. Среди наиболее популярных у фишеров организаций лидировали интернет-порталы.

По нашей статистике KSN на первом месте среди стран - источников спама оказались США, на втором – Россия, на третьем – Вьетнам. Интересно, что во многих больших странах значительная часть приходящего пользователям спама рассылается из этой же страны.