Спам в третьем квартале 2012

Цифры квартала

- Доля спама в третьем квартале уменьшилась на 2,8% и составила 71,5%.
- Доля писем с вредоносными вложениями увеличилась на 0,9% и составила 3,9%.
- 27% фишинговых атак приходится на социальные сети.
- 26,7% всего спама было отправлено из США.

Особенности периода: политика и религия в спаме

Самой популярной личностью в спаме третьего квартала 2012 вновь стал американский президент Барак Обама. Его имя упоминалось в письмах на самые разные темы: от банальной рекламы «часов как у президента» до разоблачения президентской администрации и призываов к американским гражданам бороться с политикой действующего президента (как правило, в таких призывах содержались также просьбы пожертвовать деньги на эту борьбу). Были замечены также мошеннические и вредоносные рассылки, использующие имя президента США.

К концу сентября количество англоязычных рассылок, призывающих американских граждан сменить политиче

ский курс страны, увеличилось. Видимо, сказалось начало предвыборной гонки: выборы президента США пройдут 6 ноября 2012 г. В сообщениях встречалась и критика деятельности Барака Обамы, и призывы голосовать за другого кандидата — Митта Ромни.

Стоит отметить, что в США под юрисдикцию закона против спама (CAN-SPAM Act 2003) подпадают только коммерческие рассылки (рекламного характера), политические же массовые письма законодательно спамом не считаются.

Мошенники также использовали популярность Барака Обамы в своих целях. Причем в мошеннических письмах можно было увидеть не только имя президента США, но и имя его жены, Мишель Обамы. Рассылая письма от имени первой леди, нигерийские мошенники пытались втереться в доверие к пользователям: в письме «Мишель Обама» обещает миллионы долларов тем, кто пришлет «ей» свои адреса, номера телефонов и 240 долларов.

В этом квартале кроме политического спама мы наблюдали и религиозный. Именно в спаме распространялись ссылки на размещенный на сайте YouTube ролик со скандально известным фильмом «Невинность мусульман». Интересно, что обычно злоумышленники просто эксплуатируют интерес пользователя к горячим темам и ссылки в подобных письмах ведут на вредоносные ресурсы, и однако в данном случае ссылки в письмах действительно вели на

ролик на YouTube, никакие вредоносные программы с помощью этой рассылки не распространялись.

Тем не менее некоторые злоумышленники все-таки воспользовались скандалом вокруг фильма в своих целях, разослав вредоносные письма в стиле горячих новостей:

Ссылки в письмах вели на взломанный сайт с дальнейшей переадресацией на вредоносный ресурс pillsearnings.nl. На этот же ресурс вела и ссылка в другой части той же рассылки использующей имя американского президента и тему выборов:

Новые рекламные площадки: плюсы и минусы

Уменьшение доли спама

В прошлом квартале мы уже отмечали, что реклама мигрирует из спама на другие площадки: баннеры, социальные сети, контекстную рекламу, купонные сервисы. В третьем квартале эта тенденция сохранилась, и доля спама в почтовом трафике сократилась еще на 2,8%.

На графике заметно характерное для лета уменьшение доли спама и небольшой рост этого показателя в сентябре. Осенью такой рост наблюдается почти каждый год: заканчиваются отпуска, люди больше времени проводят в интернете, и рекламодатели пытаются дать больше рекламы, в том числе в спаме. И все же отчетливо видна общая тенденция к уменьшению доли спама.

«Серые зоны» рассылок

В последнее время в Сети появилось много разнообразных купонных (скидочных) сервисов — интернет-проектов, которые предоставляют пользователям так называемые коллективные скидки. Такие сервисы пользуются спросом во всем мире и оттягивают рекламодателей из спама. С одной стороны, это положительный процесс. С другой — не все такие сервисы рассылают собственную рекламу корректно с точки зрения закона. В результате возникают так называемые «серые зоны» рассылок.

Некоторые купонные сервисы рассылают спам, чтобы раскручивать себя и привлекать новых клиентов, для чего часть рассылок идет и подписчикам, и по гораздо более широкой базе адресов. А ведь если получатель не подписывался на рассылку, она является спамом, даже если помимо прямой рекламы товара она содержит новости, статьи по теме и любую другую релевантную информацию. Более того, любой человек может подать в суд на такого рассыльщика. В России существует Статья 18 ФЗ «О Рекламе», в которой, в частности, говорится:

«Распространение рекламы по сетям электросвязи, в том числе посредством использования телефонной, факсимильной, подвижной радиотелефонной связи, допускается только при условии предварительного согласия абонента или адресата на получение рекламы. При этом реклама признается распространенной без предварительного согласия абонента или адресата, если рекламораспространитель не докажет, что такое согласие было получено».

Практически во всех странах существуют аналогичные статьи, а иногда даже специальные законы о спаме.

То есть любой человек может подать в суд на нечестного рекламодателя, приславшего ему спам. И если в случае классического спама, где отправитель анонимен, найти и привлечь к ответственности нарушителя закона действительно сложно, то в случае с подобными «серыми зонами» найти ответчика гораздо проще.

Вредоносные подделки под сообщения купонных сервисов

Возрастающую популярность новых легальных рекламных площадок спамеры используют в своих целях. В первую очередь, рассылая вредоносные письма, подделанные под различные официальные уведомления. Все больше становится вредоносного спама — подделок под уведомления купонных сервисов.

Мы уже поднимали тему использования купонов в спаме в отчете за второй квартал 2012 г. Вернуться к купонному спаму нас заставило появление в спам-потоках вредоносных рассылок — подделок под сообщения от крупнейшего купонного сервиса Groupon.

Мы ожидали появления такого спама, поскольку купоны очень популярны у пользователей, а купонные сервисы пользуются их доверием. Письма от купонных сервисов — идеальная маскировка для рассылки зловредов.

Первая зафиксированная нами подобная рассылка прошла в июле. Тогда к сообщению, имитирующему уведомление о новой акции крупнейшего купонного сервиса, был приложен zip-архив, содержащий исполняемый файл Gift coupon.exe. На деле файл был вредоносной программой Trojan.Win32.Yakes.aigd. Все ссылки в письмах с вредоносными вложениями вели на сайт Groupon, на котором никаких опасных объектов не было. Очевидно, это был трюк, использованный злоумышленниками, чтобы вызвать доверие пользователя.

Совсем иная ситуация с вредоносными сообщениями, зафиксированными нами в сентябре. В новой рассылке якобы от Groupon не было вложений, однако все ссылки через несколько переадресаций вели на вредоносный ресурс с эксплойтами.

Как мы уже отмечали выше, появление вредоносного спама, использующего тему купонов, было вполне ожидаемо, поскольку такие сервисы пользуются большой популярностью. В связи с этим хотелось бы предупредить пользователей:

во-первых, купонные сервисы никогда не вкладывают файлы-вложения в свои письма, особенно в виде zip-архивов или исполняемых файлов.

во-вторых, пользователь, прежде чем перейти по ссылке в письме, всегда может и должен убедиться в том, что письмо, выдаваемое за рассылку известного сервиса, хотя бы имеет соответствующего отправителя в поле from, и все ссылки ведут именно туда, куда заявлено (проверить это можно, наведя курсор на ссылку).

Практические советы на эту тему можно прочитать на нашем сайте.

Вредоносные рассылки: разнообразие

Надо отметить, что в этом квартале мы наблюдали огромное разнообразие вредоносных рассылок. Практически все они маскировались под официальные уведомления: в наших спам-потоках мы встречали поддельные письма от хостингов, банковских систем, социальных сетей, онлайн-магазинов и других сервисов.

Интересно, что если в прошлом квартале наибольшей популярностью у злоумышленников пользовались уведомления о приобретении авиабилетов, то в этом чаще встречались поддельные уведомления о бронировании гостиниц.

В некоторых случаях злоумышленники объединяли два приема социальной инженерии: чтобы заставить пользователя пройти по ссылке, в поддельных уведомлениях популярного ресурса упоминался некий приз:

При таком количестве и качестве подделок с вредоносными ссылками пользователям следует быть еще более внимательными: любое письмо может оказаться опасным!

Статистика

Вредоносные вложения в почте

Хотя в течение всего третьего квартала доля вредоносных вложений в почтовом трафике уменьшалась, по итогам квартала средний процент писем, содержавших вредоносные вложения, увеличился на 0,9 пункта по сравнению с предыдущим кварталом и составил 3,9%. На диаграмме ниже представлено распределение этого показателя по месяцам.

**Доля вредоносных вложений в почтовом трафике,
третий квартал 2012 г.**

Распределение срабатываний почтового антивируса по странам

Самым заметным изменением в рейтинге стран по срабатыванию почтового антивируса по итогам Q3, бесспорно, является выход на первое место Германии (+3,8%).

Распределение срабатываний почтового антивируса по странам в третьем квартале 2012 г.

США, лидировавшие в этом рейтинге восемь месяцев подряд, в сентябре неожиданно сместились сразу на восьмую строчку, что повлияло и на итоги квартала. В результате по сравнению с прошлым кварталом доля США уменьшилась на 5,2 пункта, и они заняли вторую строчку, незначительно отстав от лидера.

На 1,7 пунктов снизилась доля Великобритании (пятая строка рейтинга), и на 1,6 пунктов — Италии, не вошедшей в TOP 10. Изменения долей остальных стран рейтинга не превышают 1,5%.

Любопытно выглядит динамика рассылки вредоносного кода на территории Вьетнама и Австралии: на протяжении всего квартала показатели этих стран практически совпадали.

Доля вредоносного спама в Австралии и во Вьетнаме
июнь - сентябрь 2012 г.

TOP 10 вредоносных программ, распространенных в почте

Несмотря на то что по итогам сентября доля детектирований почтовым антивирусом традиционного лидера нашего рейтинга Trojan-Spy.HTML.Fraud.gen резко сократилась, по результатам квартала этот зловред занял первую строчку, с большим отрывом обогнав другие программы. Более пятой части всех детектирований почтового антивируса в третьем квартале 2012 года пришлось на эту программу. Напомним, что Trojan-Spy.HTML.Fraud.gen — это вредоносная программа, выполненная в виде html-странички с регистрационной формой финансовой организации или какого-либо онлайн-сервиса. Регистрационные данные, введенные на такой страничке, отправляются злоумышленникам. Использование этого зловреда является одним из приемов фишеров.

TOP 10 вредоносных программ, распространенных в почте,
третий квартал 2012 г.

Почтовые черви Bagle.gt, Mydoom.m и Mydoom.l занимают в рейтинге второе, третье и четвертое места соответственно, поотстал от своих соратников червь Netsky.q — он занимает шестую строчку рейтинга. Напомним, что стандартный функционал почтовых червей заключается в сборе электронных адресов на зараженном компьютере и рассылке по ним самих себя. Bagle.gt — единственный из четырех зловредов, который снабжен дополнительным функционалом: он может обращаться к интернету и загружать на компьютер пользователя другие вредоносные программы.

Появившиеся в рейтинге в июне программы семейства Androm сохраняли свои позиции все лето, а в сентябре один из представителей этого семейства — Androm.kv — занял первую строчку рейтинга. По итогам третьего квартала эта модификация оказалась на пятой строчке рейтинга. Еще один представитель этого семейства расположился на последнем месте в рейтинге. Эти зловреды, установившись в систему пользователя, загружают из интернета другие вредоносные программы, в том числе спам-боты.

На седьмом месте расположился зловред Trojan-Ransom.Win32.PornoAsset.aauh — это программа-вымогатель, блокирующая операционную систему и требующая у пользователя заплатить за разблокирование. Такие программы были в числе наиболее заметных в сентябре: четыре программы из TOP 10 за первый осенний месяц были представителями именно этого семейства.

Размер спамовых писем

Размер спамовых писем, третий квартал 2012 г.

В третьем квартале 2012 г., как обычно, в спаме преобладали очень короткие письма (1 КБ и меньше). Как правило, в теле таких писем находится одна короткая фраза и ссылка на сайт, куда, по замыслу спамеров, должен попасть пользователь. В сентябре мы отметили увеличение количества чуть более объемных писем (2-5 КБ). Это связано с тем, что осенью увеличивается количество заказного спама малого и среднего бизнеса: такой спам, как правило, содержит больше информации в теле письма. Партнерский же спам непременно должен содержать ссылку, так как доход спамера зависит от количества пользователей, прошедших по разосланной им ссылке.

Распределение источников спама по странам и регионам

В третьем квартале существенно выросла доля спам-писем, разосланных из Китая(+6,7%) и США (+15%). Суммарно эти две страны ответственны более чем за половину мирового спама.

Доля остальных стран уменьшилась относительно пропорционально.

Страны — источники спама, третий квартал 2012 г.

Спам из Китая рассылался в основном в страны APAC и в Западную Европу, спам из США активно распространялся по Американскому континенту и также по странам APAC. Что касается Восточной Европы, то наибольшее количество спама приходило туда из Индии и Вьетнама. Из Индии спам активно рассылался и в Западную Европу, где эта страна заняла второе место в рейтинге стран — источников спама.

Что касается регионов — источников спама, то за счет США значительно выросла доля региона Северная Америка (+15%), при этом доля Азии по-прежнему высока: почти половина спама рассылается с компьютеров, находящихся в этом регионе. Западная Европа обогнала Восточную и вышла на четвертое место, приблизившись по показателям к Латинской Америке.

Распределение источников спама по регионам,
третий квартал 2012 г.

Фишинг

Распределение TOP 100 организаций, атакованных фишерами, по категориям, третий квартал 2012 г.

Рейтинг категорий атакованных фишерами организаций основывается на срабатываниях нашего компонента антифишинга на компьютерах пользователей. Антифишинг детектирует все фишинговые ссылки, по которым пытался пройти пользователь, — будь то ссылка в спамовом письме или в интернете.

По итогам квартала в распределении фишинговых атак по категориям лидируют социальные сети, на которые пришлось 26,5% атак, что на 0,6 пункта больше, чем в предыдущем квартале. На втором месте расположились финансовые организации — на них пришлось 22% всех фишинговых атак, что на 1,6 пунктов меньше, чем в прошлом квартале.

Интересно отметить, что, несмотря на небольшую долю фишинговых атак на онлайн-игры, на протяжении всего квартала мы регистрировали рассылки, целью которых была кража регистрационных данных пользователей battle.net. Можно предположить, что недавний выход WoW: Mists of Pandaria подогреет интерес фишеров к аккаунтам в играх компании Blizzards.

Заключение и прогнозы

В третьем квартале 2012 мы наблюдали множество рассылок политической направленности. Очевидно, вплоть до выборов американского президента 6 ноября их количество будет расти. Вероятно, вырастет и количество вредоносных рассылок, эксплуатирующих интерес пользователей к теме выборов.

Миграция рекламодателей из спама на другие площадки способствует тому, что спам становится более криминализированным, с бОльшим количеством рекламы запрещенных товаров, мошенничества и вредоносных писем. В течение последнего года мы наблюдаем две параллельные тенденции: снижение доли спама и небольшое увеличение доли вредоносных рассылок. Скорее всего, обе тенденции продолжатся, так как доля спама снижается за счет ухода из спама рекламодателей, предлагающих честные товары и услуги.

Что касается стран — источников спама, то значительно возросшая доля США, скорее всего, не продержится на таком высоком уровне и в следующем квартале несколько снизится. Азия же останется регионом, из которого рассылается наибольшее количество спама.

Источник: SecureList.