Kaspersky Security Bulletin. Спам в 2011 году

В антиспам-лаборатории компании «Лаборатория Касперского» ежедневно обрабатывается более миллиона писем, попадающих в наши ловушки. Для защиты пользователей используется контентная фильтрация, анализ технических заголовков, уникальные графические сигнатуры, а также облачные технологии. Наши аналитики создают новые сигнатуры круглосуточно 7 дней в неделю.

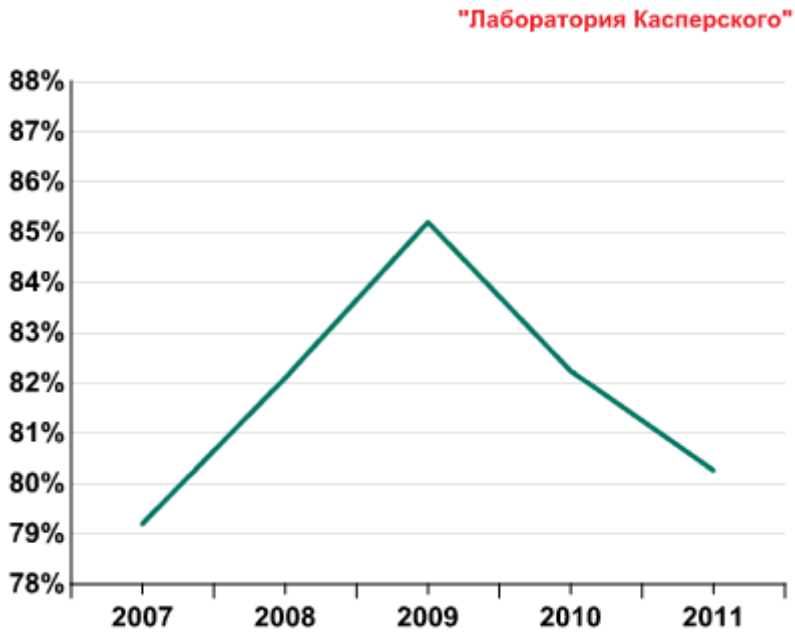
Цифры года

- Доля спама в почте в среднем составила 80,26%.
- Доля фишинговых писем уменьшилась в 15 раз и в среднем составила 0,02% от всего почтового трафика.
- Доля спама с вредоносными вложениями увеличилась в 1,7 раз и составила 3,8% почтового трафика.

Тенденции 2011

Спама становится меньше

После активной борьбы с ботнетами в 2010 году количество спама в почтовом трафике заметно сократилось. В 2011 году доля спама в среднем составила 80,26%. Это меньше показателя 2010 года, не говоря уже о «пиковом» 2009-м.



Доля спама в почтовом трафике 2007—2011 гг.

На графике хорошо видно, что последние 2 года доля спама в почте уменьшается. Этому есть несколько объяснений. Во-первых, инициативные группы продолжают закрывать командные центры ботнетов: в 2011 году были закрыты Rustock и Hlux/Kelihos. Во-вторых, спамеры все чаще делают ставку на целевые рассылки. Например, участники партнерских программ по распространению фармацевтического спама стараются использовать для своих рассылок базы адресов, украденные с веб-ресурсов традиционно мужских направлений. При этом объем целевых спам-рассылок значительно меньше, чем обычных веерных, а отклик на них потенциально больше. В-третьих, уже несколько лет спамеры учитывают различия в спросе на предлагаемые в спаме товары в разных странах и регионах. Так, например, в США и странах Западной Европы на протяжении последних лет спама, содержащего рекламу «Медикаментов» и «Реплик элитных товаров», было заметно больше, чем в России и странах СНГ, хотя и в зоне Рунета он был представлен в немалых количествах. 2011

год с этой точки зрения был переломным: из-за ограниченности ресурсов спамерам, включенным в фармацевтические партнерки, пришлось исключить из своих баз адреса Рунета, благодаря чему партнерского спама в российском сегменте интернета стало значительно меньше.

Целевые фишинг-атаки

Яркая тенденция 2011 года — spear phishing. Направленный, или целевой, фишинг. Этот вид фишинговых атак отличается тем, что злоумышленники распространяют свои сообщения не по случайным адресам, а заранее выбирают группу лиц или пользователя, на которых будет проведена атака.

Под целевым фишингом понимают не один определенный прием, а несколько, отличающихся друг от друга сложностью исполнения и поставленной задачей.

Он выполняет ту же задачу, что и традиционный фишинг, а именно — сподвигнуть пользователей передать ихрегистрационные данные в руки мошенников для получения доступа к аккаунтам. Например, одна из разновидностей целевых фишинговых атак — это атака на группу пользователей, которые являются клиентами какого-либо сервиса. Письма фишеров до мельчайших деталей воспроизводят официальные уведомления атакуемого сервиса и имеют в теле ссылку на регистрационную форму — точную копию настоящей регистрационной формы сервиса. Считается, что именно эта нехитрая схема атаки была применена китайскими преступниками, которые в результате получили доступ к аккаунтам Google, принадлежащим высокопоставленным чиновникам США. Основное отличие такой схемы от традиционного фишинга — меньший охват аудитории при более точном выборе цели.

Последнее время фишеры стали использовать и другой, еще более хитрый прием — рассылку персонализированных писем. Мы привыкли к тому, что фишинговые письма содержат обезличенные обращения, такие как «Дорогой пользователь нашей сети!» или «Уважаемый клиент!». Более сложная схема целевого фишинга подразумевает, что злоумышленник знает не только то, клиентом или работником какой компании является его потенциальная жертва, но также имя и фамилию человека. В настоящее время получить такую информацию для фишеров не составляет большого труда: пользователи социальных сетей часто не скрывают информацию о себе, чем и пользуются злоумышленники. Используя нехитрый набор данных, которые пользователь сам выложил на всеобщее обозрение, преступники с большой вероятностью могут добиться доверия жертвы.

Другая разновидность целевых атак — атака с целью получения доступа к ресурсам какой-либо компании. Именно эту цель преследовали злоумышленники, которые провели атаку на RSA — подразделение безопасности крупной IT-корпорации EMC, в марте 2011 года. Атаковав несколько групп сотрудников компании, злоумышленники добились того, что один сотрудник RSA точно открыл разосланный ими файл "2011 Recruitment plan.xls." В файл Microsoft Excel был внедрен эксплойт, использующий уязвимость нулевого дня, благодаря которому фишеры получили доступ к системам компании. В результате атаки фишерами были украдены данные компании RSA.

Целевые фишинговые атаки опасны еще и тем, что сообщения, рассылаемые в ходе таких атак, немногочисленны или вовсе уникальны. Такие письма зачастую не распознаются как спам защитным ПО. Для организаций, подвергшихся целевой фишинговой атаке, защитой может послужить система DLP, предохраняющая от утечки данных. Для индивидуальных пользователей последним рубежом на пути фишера к финансовым, персональным или иным данным становится тот самый человеческий фактор, на использовании которого и построена вся эта схема. Будучи внимательным и настроеннным критично, пользователь может избежать опасности и не попасть в ловушки фишеров.

Пользователям нужно помнить, что как бы умело фишер ни подделывал внешний вид сообщения и регистрационной формы, он все равно вынужден использовать домен, никак не связанный с организацией, под уведомление от которой замаскировано письмо. Если вам предлагается ввести свои регистрационные данные на сайте банка или иного онлайн-сервиса — зайдите на сайт

организации, не используя ссылку в письме, а введя нужный адрес в адресную строку браузера. Также важно помнить, что ни один онлайн-сервис не попросит вас переслать ваши регистрационные данные в электронном письме.

Мы предполагаем, что в ближайшем будущем нас ждет рост количества целевых фишинговых атак и в связи с этим напоминаем пользователям о необходимости быть осторожными.

Год вредоносного спама

Несмотря на общее снижение количества спама, можно с уверенностью сказать, что спам стал опасней. В 2011 году доля писем с вредоносными вложениями увеличилась в 1,7 раза по сравнению с предыдущим годом и составила 3,8% почтового трафика. Кроме писем, содержащих вложенные вредоносные файлы, рассылался и спам со ссылками на вредоносные ресурсы.

Количество писем с вредоносными вложениями было стабильно высоким в течение всего года.

Доля писем с вредоносными вложениями в почтовом трафике, 2011 год

Как видно на графике ниже, последние два года наблюдается отчетливая тенденция: в почтовом трафике — одновременно с уменьшением доли спама — увеличивается доля писем с вредоносными вложениями.

Доля писем с вредоносными вложениями в почтовом трафике, 2009-2011 гг.

Вредоносный спам и социальная инженерия

Для вредоносного спама характерно использование социальной инженерии — злоумышленникам нужно убедить пользователя открыть вложение или перейти по ссылке в письме. В этом году киберпреступники не страдали отсутствием фантазии и для достижения своих целей применяли разнообразные приемы.

1. Маскировка под авторитетный источник.
   Вредоносные письма маскировались под уведомления от служб поддержки социальных сетей, международных служб доставки, федеральных налоговых и кредитных организаций.

2. Запугивание.
   В письмах сообщалось про заблокированные аккаунты, зараженные компьютеры, рассылку спама с аккаунта пользователя. Во избежание неприятностей, пользователя призывали немедленно совершить одно из двух действий: открыть вложение или пройти по ссылке.

3. Заманивание.
   В письмах пользователю обещались бесплатные купоны, ключи активации для различных продуктов и прочие подарки. Для того чтобы эти «подарки» получить, надо было всего лишь открыть вложение или пройти по ссылке.

4. Прочие случаи.
   Чаще всего злоумышленники эксплуатировали любопытство пользователя или делали ставку на отсутствие бдительности у получателя. Вложение маскировалось под отсканированный документ, электронные билеты, инструкции по восстановлению почтового пароля и многое другое. Иногда пользователя просто просили открыть вложение.

Мошенничество в спаме

Надо особо отметить, что многие громкие события этого года использовались не только для того, чтобы заинтересовать пользователя и заставить его пройти по ссылке, но и в мошеннических целях.

Землетрясение в Японии мошенники использовали, чтобы выманить у пользователей деньги якобы на помощь пострадавшим.

Имена Муаммара Каддафи и Ким Чен Ира использовались в «нигерийском» спаме. Мошенники, пытаясь выманить у пользователя деньги, представлялись всевозможными родственниками, друзьями или врагами покойных.

Спам-статистика

Доля спама в почтовом трафике

Как было сказано выше, по сравнению с 2010 годом количество спама в почтовом трафике заметно сократилось: если в прошлом году на спам пришлось 82,2%, то в 2011 году доля спама в почтовом трафике в среднем составила 80,26%.

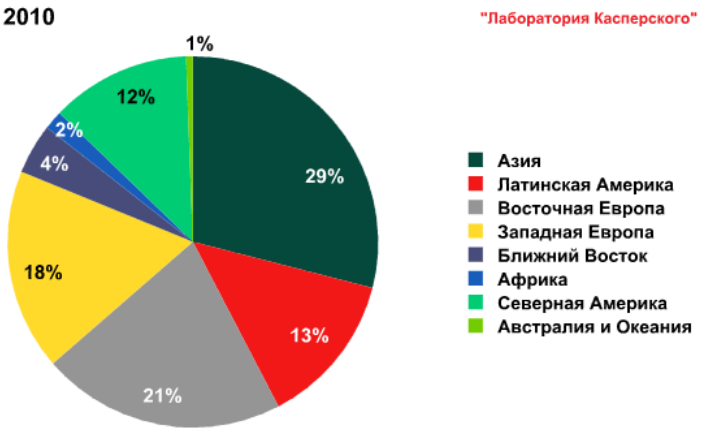
Доля спама в почтовом трафике в 2011 году

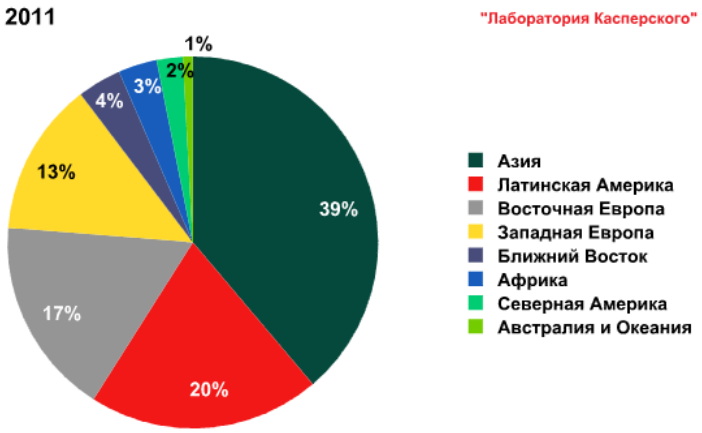
В первом полугодии доля спама стабильно росла. Однако во второй половине 2011 ситуация изменилась. В результате итоговый показатель 2011 года не достиг даже уровня 2010, не говоря уже о «пиковом» 2009-м.

Регионы — источники спама

В 2011 году заметно выросло количество спама, разосланного из стран Азии и Латинской Америки. На долю двух этих регионов приходится более половины — 59,02% — всего исходящего спама. Показатели Северной Америки после резкого падения в конце 2010 года так и остались на низком уровне.

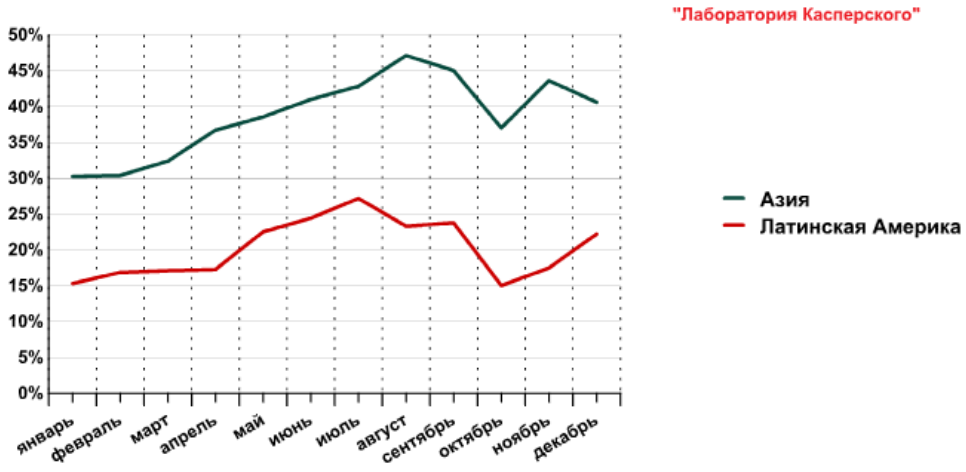
Распределение источников спама по регионам, 2010 и 2011 гг.





Отметим, что для регионов Азия и Латинская Америка динамика рассылки спама во многом схожа:

Динамика рассылки спама из Азии и Латинской Америки в 2011 г.



Этот факт косвенно подтверждает, что зараженные компьютеры в Азии и Латинской Америке входят в одни и те же ботнеты. Увеличение доли этих регионов в мировом спам-трафике говорит о том, что

размеры этих ботнетов за год увеличились. О причинах, обуславливающих такое положение вещей, мы уже писали: высокое качество интернет-доступа, низкая компьютерная грамотность пользователей и отсутствие антиспамовых законов в большинстве стран Азии и Латинской Америки делают эти регионы наиболее привлекательными для организаторов ботнетов.

Несколько увеличилась и доля Африки: в этом регионе, пока еще мало вовлеченном в рассылку спама, количество незапрошенной почты постепенно растет, в целом — по тем же причинам, что и в Азии и Латинской Америке.

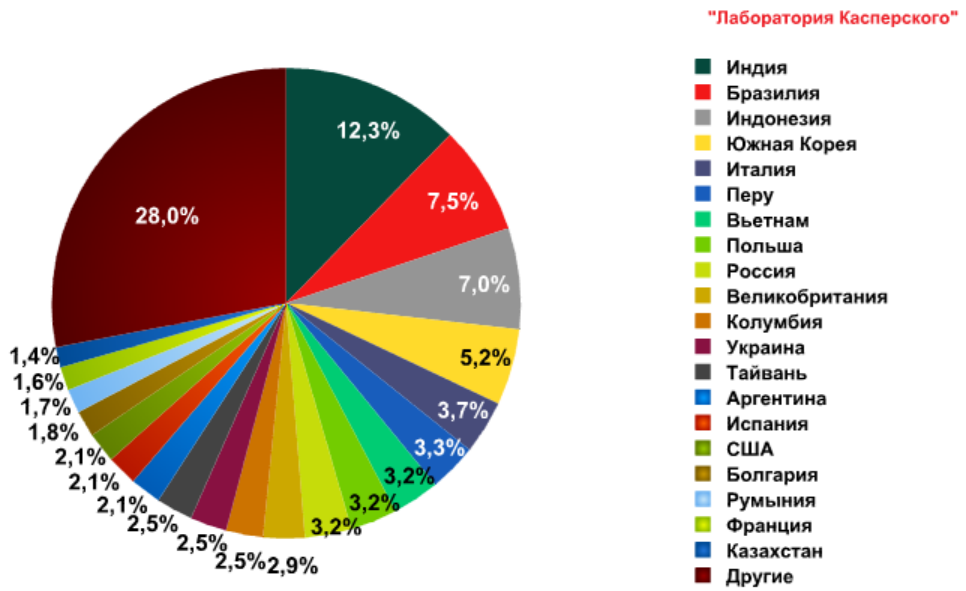
Доля Западной Европы сократилась на 4%. Интересно, что из такого большого и хорошо компьютеризированного региона с каждым годом рассылается все меньше спама. Благодаря высокой компьютерной грамотности пользователей и успешной борьбе с пиратством, в этом регионе на компьютерах, как правило, стоит регулярно обновляемое программное обеспечение и лицензионные антивирусные программы. Злоумышленникам непросто заразить такие компьютеры вредоносными программами и подключить их к спамерскому ботнету.

Страны — источники спама

Увеличение долевых показателей регионов, лидирующих в рассылке мусорной почты отразилось и на составе TOP 20 стран — источников спама.

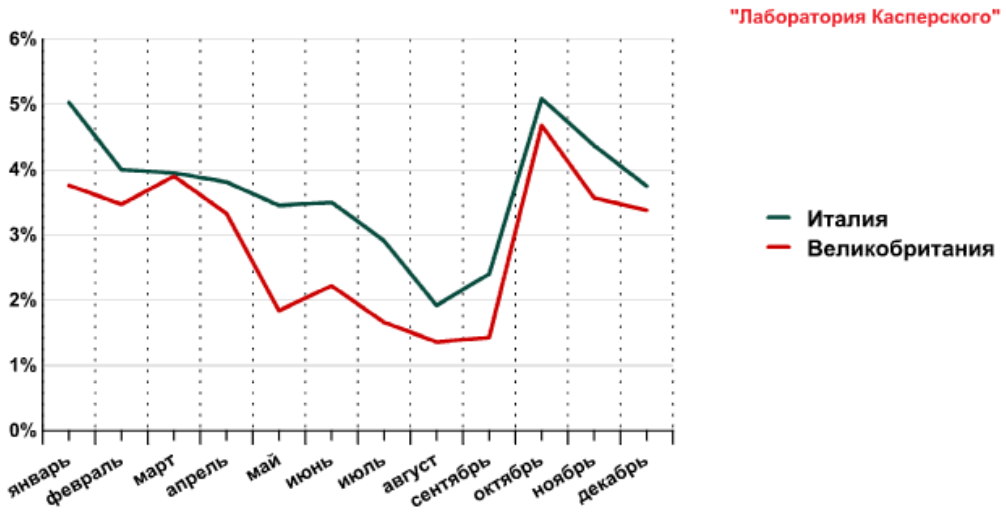
Лидер прошлого года — США (-9,24%) — не попал даже в TOP 10, заняв 16-е место в рейтинге. Сдала свои позиции и Россия (-2,8%), сместившаяся с 3-го на 9-е место. В первую тройку, помимо Индии (+4%) и Бразилии (+3,4%), вошла Индонезия (+5,15%), ранее занимавшая лишь 16-е место среди стран — распространителей спама.

Распределение источников спама по странам в 2011 г.



В TOP 10 по-прежнему входят две страны Западной Европы: Италия и Великобритания. Динамика рассылки спама из них схожа. Вероятно, компьютеры пользователей этих стран входят в одни и те же ботнеты.

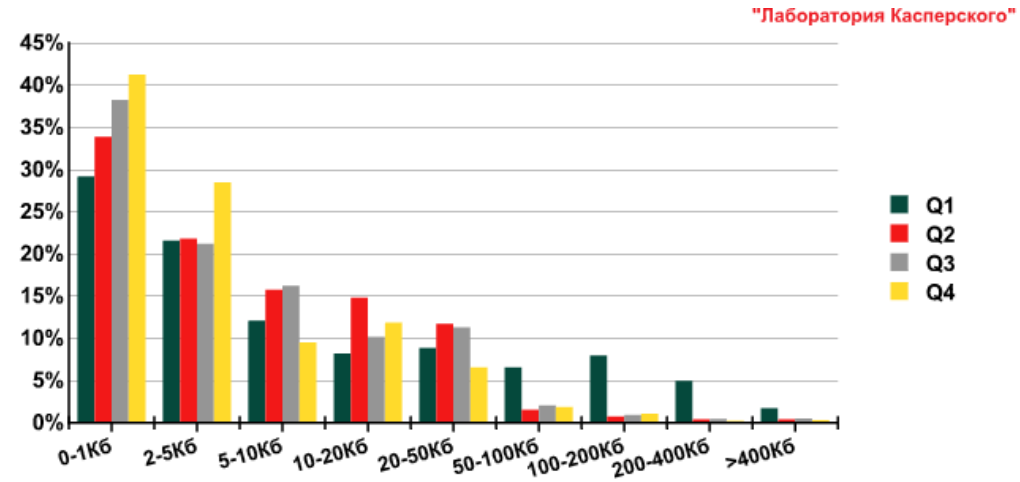
Динамика рассылки спама из Италии и Великобритании в 2011 г.



Размеры спамовых писем

В течение года наблюдалась тенденция к уменьшению размера спамовых писем. В первом квартале увеличилось количество писем, объем которых превышал 100КБ, но уже ко второму кварталу число таких писем сильно сократилось. К концу года на письма объемом более 50КБ приходилось менее 3%, в то время как письма, размер которых не превышал 5КБ, составили 69,46% всего спама.

Распределение размеров спамовых писем в 2011 г.



Тематический состав спама

В 2011 году в рейтинге тематических категорий спама Рунета первое место с большим отрывом заняла тематика «Образование» — предложение семинаров и тренингов. В течение года доля этой рубрики сильно колебалась: в разные месяцы она составляла от 13% до 60% всего спама в Рунете.

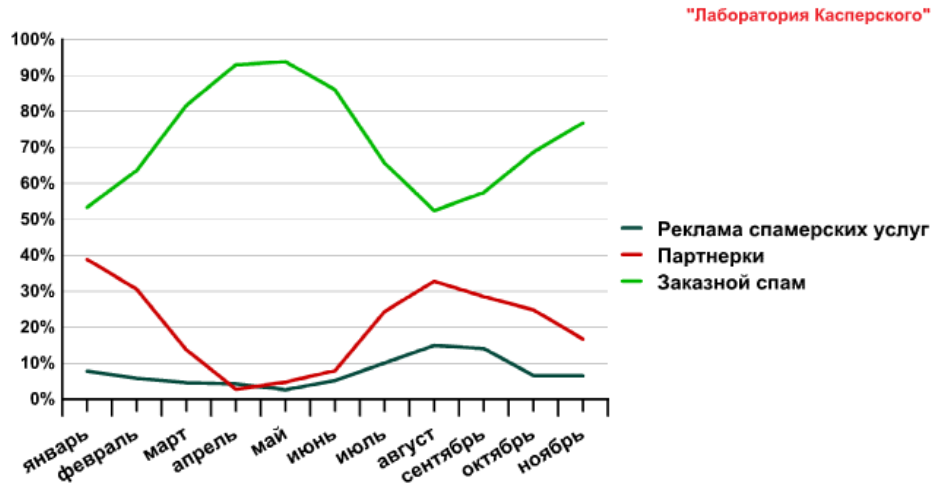
Пятерка лидеров выглядит так:

1. Образование — 35,75%
2. Другие товары и услуги — 15,53%
3. Недвижимость — 9,92%
4. Медикаменты; товары/услуги для здоровья — 9,58%
5. Реклама спамерских услуг — 7,50%

Напомним, что все тематические категории спама (за исключением саморекламы спамеров) можно объединить в две большие группы: заказной и партнерский спам. К заказному спаму относятся преимущественно рекламные объявления, за распространение которых, т.е. за рассылку спам-сообщений, платит заказчик. Распространение партнерского спама заказывается через партнерские программы. Такой спам является преимущественно рекламой нелицензионных товаров или используется для распространения вредоносных программ. При этом спамер получает деньги за количество приобретенного товара/зараженных компьютеров пользователей.

В 2011 году в Рунете значительно выросло количество заказного спама. Процент такого спама ни разу за год не опустился ниже 50. Самые низкие показатели были зафиксированы в январе и августе — это месяцы традиционного сезонного затишья рекламы. В периоды такого затишья растет не только количество партнерского спама, но и количество саморекламы спамеров, поскольку спамеры пытаются вновь привлечь клиентов, как приостановивших свои заказы, так и новых.

Доля партнерского и заказного спама в 2011 году



Напомним, что в прошлом году ситуация была иной — процент партнерского и заказного спама был примерно одинаковым (46,6% и 47,7% соответственно). Скорее всего, после закрытия ботнетов в конце 2010 года владельцы ботнетов стали более экономно использовать имеющиеся мощности, а также не слишком привлекать к себе внимание. Теперь они стремятся не увеличивать, а уменьшать размеры своих рассылок. Для этого они делают рассылки более целенаправленными и, в частности, не рассылают партнерский спам в регионы, где он не пользуется спросом. Так, в России основная «партнерская» тематика — «Медикаменты» — никогда не была популярна, потому что в России, в отличие от США, на большинство лекарств не требуются рецепты. К тому же, в России еще не так много людей пользуются кредитными картами для оплаты покупок в интернете, а именно этот способ оплаты и предлагается в партнерском спаме. С другой стороны, в России отсутствуют антиспамовые законы (спама в какой-то мере касается только ФЗ «О рекламе»), поэтому малый бизнес достаточно широко пользуется таким способом рекламы, и количество заказного спама в России выше, чем в США и Европейских странах.

Спам и политика

Не обошли спамеры вниманием и выборы в Государственную думу РФ. Заметим, что 4 года назад перед думскими выборами тоже рассылался политический спам. Однако в 2011 году содержание такого спама заметно изменилось. Если 4 года назад в роли заказчика рассылок очевидно выступала та или иная партия с призывами голосовать за нее, то в 2011 году никакая отдельная партия не пыталась рекламировать себя с помощью спама. Рассылки были направлены против партии власти, их содержание варьировало от призывов к бойкоту выборов до призывов к свержению действующей власти.

Спам на тему политики распространялся и после выборов. Не пропустили спамеры и митинги, прошедшие в конце 2011 года. Но в данном случае политика послужила лишь поводом для самых банальных вещей:

Фишинг

В среднем доля фишинговых писем в 2011 году уменьшилась в 15 раз и составила 0,02% от всего почтового трафика.

Процент фишинговых писем в почте в 2011 г.

Однако по итогам года чуть менее 10% всех срабатываний почтового антивируса пришлось на программы, которые используются в ходе фишинговых атак, — на Trojan-Spy.HTML.gen и Trojan.HTML.Fraud.fc. Обе эти программы выполнены в виде html-страниц, копирующих регистрационные формы онлайновых сервисов. Данные, вводимые в этих формах, перенаправляются злоумышленникам. Доля сообщений, содержащих во вложении такие вредоносные программы, составляет около 0,35% всей электронной почты.

ТОР 3 организаций, атакованных фишерами в 2011 г*.

1. PayPal 43,14%
2. eBay 9,90%
3. Facebook 7,04%

* Рейтинг составляется на основании доли фишинговых URL, распространенных в сети с целью получения регистрационных данных пользователей того или иного сервиса. Рейтинг не является показателем уровня безопасности упомянутых организаций. Рейтинг отражает популярность и авторитетность сервисов среди пользователей, которые напрямую сказываются на популярности сервисов у фишеров.

По сравнению с прошлым годом тройка лидеров среди организаций, которые чаще всего атаковали фишеры, не изменилась. Более того, доля интернет-аукциона eBay (9,9%) и социальной сети Facebook (7%), занимающих второе и третье места соответственно, изменилась по сравнению с 2010 годом менее чем на 0,1%. Доля бессменного лидера нашего рейтинга — платежной системы PayPal (43,1%) — уменьшилась по итогам года на 10,2%.

Кроме Facebook в течение года внимание фишеров привлекли социальные сети Habbo и Orkut, доля атак на пользователей которых по итогам года составила 6,9% и 2,6% соответственно.

Популярными у фишеров мишенями остаются и пользователи онлайн-игр. Так, доля атак на World of Warcraft увеличилась по сравнению с прошлым годом примерно на 0,5% и составила 2,2%. Почти столько же атак было проведено в 2011 и на RuneScape (2%).

Таким образом, в фокусе внимания фишеров по итогам 2011 года остаются виртуальные деньги и виртуальная собственность: учетные записи социальных сетей и персонажи и деньги в онлайн-играх.

Вредоносные вложения в письмах

Доля вредоносных вложений в почте по итогам года составила 3,8%. Это в 1,7 раза больше, чем аналогичный показатель 2010 года. Отметим, что в 2010 году сравнительно высокая доля вредоносных вложений была обусловлена летним всплеском вредоносных рассылок. В этом году ситуация иная: процент вредоносных вложений в почте в течение всего года не опускался ниже 2,5.

Доля писем с вредоносными вложениями в почте в 2011 г.

Пиковыми месяцами второй год подряд становятся июль, август и сентябрь, и именно в эти месяцы спамеры применяли наибольшее количество трюков для распространения вредоносного кода.

Распределение срабатываний почтового антивируса по странам

Наибольшее количество срабатываний почтового антивируса пришлось на Россию (12,3%), при этом в предыдущем, 2010 году, она не вошла даже в TOP 10 стран по срабатываниям почтового антивируса. Доля срабатываний почтового антивируса на территории США увеличилась на 1,5% по сравнению с 2010 годом и составила 10,9%. Штаты заняли вторую строчку по итогам 2011 года. Не изменилась позиция Великобритании. По итогам 2011 года она заняла 3-е место, ее доля сократилась лишь на 0,9%.

Из заметных изменений стоит отметить увеличение доли срабатываний почтового антивируса на территории Вьетнама (+2,7%) и уменьшение доли срабатываний на территории Германии (-2,6%).

Интересно отметить, что в течение всего года сохранялась обратная зависимость между динамикой рассылки вредоносного кода на территории США и Индии: когда больше вредоносного спама детектировалось в США, в Индии доля таких детектирований заметно сокращалась, и наоборот.

Вероятно, это связано с тем, что в эти страны рассылаются вредоносные программы совершенно разного характера. В Индию злоумышленники предпочитают отправлять программы для построения там ботсети, а в США — для кражи персональных и финансовых данных. Если учесть, что ресурсы злоумышленников ограничены, то картина становится ясна: одни и те же ботнеты работают то на расширение зомби-сети в Индии, то на зарабатывание денег путем кражи данных американских пользователей.

Второй год подряд первое место в рейтинге вредоносных программ, задетектированных в почте, занимает Trojan-Spy.HTML.Fraud.gen. Доля этого зловреда уменьшилась по сравнению с прошлым годом на 3,5%. Эта вредоносная программа по сути является фишинговой: зловред выполнен в виде html-страницы, копирующей регистрационную форму онлайн-банкингов или других интернет-сервисов. Регистрационные данные, введенные в такую «форму», будут отправлены злоумышленникам.

Вредоносная программа Trojan.HTML.Fraud.fc впервые появилась в нашем рейтинге в апреле 2011 года и во втором квартале заняла третью строчку. По итогам 2011 года этот троянец, представляющий собой фишинговую HTML-страничку и нацеленный на кражу финансовых данных у бразильских пользователей, занял шестое место.

Занявший во втором квартале 2011 четвертую строчку рейтинга упаковщик Packed.Win32.Katusha.n по итогам года занял восьмое место. Он используется для обхода детектирования антивирусными средствами других вредоносных программ.

Семь из десяти вредоносных программ нашего рейтинга — это почтовые черви. Некоторые из них не покидали рейтинг практически в течение всего 2011 года.

На второй и четвертой строчках расположились Email-Worm.Win32.Mydoom.m, Email-Worm.Win32.NetSky.q — почтовые черви, выполняющие только две функции: сбор электронных адресов на зараженных машинах и рассылка по ним самих себя. Эти вредоносные программы входили в рейтинг и в 2010 году. При этом доля сообщений, содержавших Email-Worm.Win32.Mydoom.m, увеличилась по сравнению с 2010 годом вдвое. Доля сообщений с вредоносной программой Email-Worm.Win32.NetSky.q увеличилась по сравнению с прошлым годом незначительно.

Еще два представителя тех же семейств — Email-Worm.Win32.Mydoom.l и Email-Worm.Win32.NetSky.ghc — расположились на седьмой и девятой строчках соответственно. Их функционал не отличается от описанного выше.

Еще один почтовый червь, завсегдатай нашего рейтинга Email-Worm.Win32.Bagle.gt, занял четвертое место. В дополнение к обычному функционалу почтовых червей этот зловред обращается к интернет-ресурсам для загрузки оттуда вредоносных программ.

Заключение

Давление мирового IT-сообщества и правоохранительных органов разных стран на спам-бизнес приносит свои плоды. Спама в почте пользователей стало меньше. Однако в целом непрошеная

корреспонденция стала опаснее — вырос процент писем с вредоносными вложениями. Увеличивается и число целевых фишинговых рассылок.

Мы ожидаем, что в дальнейшем фишеры чаще будут атаковать конкретные группы пользователей, а в спаме будет больше писем, подделанных под уведомления от популярных ресурсов. В обоих случаях — и при адресной фишинговой атаке, и при попадании в ящик очередного «уведомления» от известного ресурса — фальшивые письма сложно отличить от настоящих. В результате компьютеры пользователей будут подвергаться большей опасности заражения, а конфиденциальные данные пользователей и компаний — большему риску кражи.

Экономя ресурсы и стремясь обойти средства антиспам-защиты, владельцы ботнетов сегментируют свою аудиторию, уменьшая тем самым объем рассылок и делая их более эффективными. Эта тенденция сохранится.

В некоторых регионах, например в Западной Европе, борьба со спамом привела к сокращению исходящих из них спам-потоков. Пальму первенства теперь держат Азия и Латинская Америка. Такое положение дел будет сохраняться до тех пор, пока в странах этих регионов не появится должное антиспамовое законодательство. Вероятно, увеличится вклад в мировой спам-трафик африканского региона. На этом континенте с каждым годом растет количество компьютеров и улучшается качество интернета, чего нельзя сказать о компьютерной грамотности пользователей.

Борьба со спамом и фишингом должна строиться с учетом этих тенденций и новых стратегий фишеров и владельцев ботнетов. Ну а пользователь — в условиях новой реальности — должен быть еще более внимательным и критичным.

Источник: Securelist.com