Спам в декабре 2011 года

Декабрь в цифрах

- Доля спама в почтовом трафике по сравнению с ноябрем уменьшилась на 4,4% и составила в среднем 76,2%.
- Доля фишинговых писем в почтовом потоке по сравнению с ноябрем не изменилась и составила 0,02%.
- В декабре вредоносные файлы содержались в 4% всех электронных сообщений, что на 1% больше, чем в прошлом месяце.

Обзор главных событий месяца

Купоны на спам

Купонные сервисы пользуются огромным спросом как в России, так и в других странах мира. Поясню, что купонные сервисы — это интернет-проекты, предоставляющие пользователям коллективные скидки. Покупая купон, пользователь покупает право получить определенный товар или услугу с большой скидкой, — как правило, при условии, что такой купон приобретет еще определенное количество человек.

Постепенно такие сервисы становятся для предприятий малого и среднего бизнеса в России альтернативой спам-рекламе. На то есть несколько причин: во-первых, они, в отличие от спама, абсолютно законны; во-вторых, путь распространения рекламы в целом схож — купонные сервисы проводят регулярные рассылки новостей среди своих клиентов. Однако в отличие от спама, новостные рассылки купонных сервисов не блокируются спам-фильтрами. К тому же, помимо почтового оповещения информация о товаре или услуге рекламодателя размещается и в интернете, что потенциально увеличивает охват аудитории. В-третьих, вероятность привлечения клиентов через купонный сервис значительно выше — купонные сервисы не вызывают такой негативной реакции, какую вызывает спам, а рассылки проходят по целевой аудитории, заинтересованной в покупке купонов.

В данный момент около 5% всех предложений на купонных сервисах — это предложения от фирм, занимающихся проведением семинаров. Напомним, что часто такие предложения распространяются через спам. Еще около 5% - предложения, которые мы бы отнесли к тематике «Отдых и путешествия». Среди предлагаемых на сервисах купонов примерно 0,5% составляют предложения о покупке электронных сигарет, ранее довольно часто встречавшиеся в спаме. Одновременно и в спаме, и на купонных сервисах сейчас предлагаются перчатки для телефонов с сенсорным экраном. Все это говорит о том, что многие фирмы, ранее использовавшие спам, сейчас если не полностью переключились на рекламу через купонные сервисы, то по крайней мере не пренебрегают ни той, ни другой площадкой.

Влияние купонных сервисов на почтовый трафик и интернет-рекламу не могло остаться не замеченным спамерами. Они поняли, что слово «купон» для пользователя еще привлекательнее, чем «скидка». Ведь «купон» — это своего рода скидка для избранных.

Так, распространители немецкоязычного фармацевтического спама решили, что предложение «условного купона» повысит спрос на продаваемые ими препараты:

Даже те, кто не знает немецкого языка, легко распознают слово «купон» на приведенном скриншоте. Видно также, что скидку спамеры предлагают не такую уж и большую — всего 10%.

И это не единственный случай, когда внимание пользователей к товарам, которые широко рекламируются в спаме (например, фармацевтических средств или копий элитных товаров), привлекается с помощью обещания купона.

До сих пор мы не фиксировали вредоносных вложений, подделанных под купоны. И тем не менее мы призываем пользователей быть осторожными, поскольку предполагаем скорое появление таковых в спам-потоках: обычно на популярные новшества первыми реагируют спамеры, участвующие в партнерских программах, а вторыми — распространители вредоносного кода.

Нужно также иметь в виду, что кража регистрационных данных купонного сервиса грозит потерей денег, которые пользователь, возможно, держит на своем счету. В этой связи стоит напомнить о том, что ни один крупный сервис не запросит у пользователя пересылки логина и пароля при помощи электронного письма. Прежде чем вводить какие-либо регистрационные данные, необходимо удостовериться, что адрес страницы, на которой вы их вводите, верный.

Затишье перед Рождеством

В конце года в спаме наступает традиционное затишье — приходит сезон каникул и зимних отпусков. В эти дни множество компьютеров, включенных в ботнеты, неактивны. Деловая активность также заметно снижается. Пользователи тратят деньги в основном на новогодние и рождественские подарки и воздерживаются от иных трат. Рекламодатели, зная особенности этого периода, не распыляются на бесполезные рекламные кампании. Кроме того, спамерам тоже не чуждо желание отдохнуть.

2011 год не стал исключением. Доля спама в почтовом трафике в последнем месяце года уменьшилась на 4,4%.

Доля спама в почтовом трафике в ноябре-декабре 2011 г.

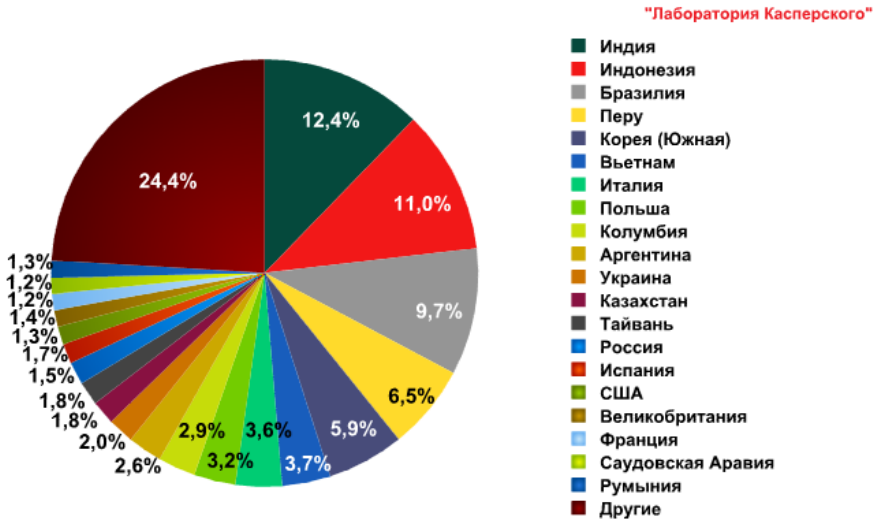
В то же время, доля спама, в котором так или иначе обыгрывалась тема Нового года и Рождества, напротив, увеличивалась, начиная с ноября. На предпоследней неделе декабря она составила более 10%.

По итогам месяца доля «новогоднего» и «рождественского» спама вкупе составила 6,8%.

Доля спама, эксплуатирующего тему Рождества и Нового года в почтовом трафике в декабре 2011 г.

Статистический обзор

Страны — источники спама



Страны — источники спама в декабре 2011 г. (TOP 20)

В декабре лидером среди стран — источников спама оставалась Индия. С территории этой страны было распространено на 0,34% спама больше, чем в прошлом месяце.

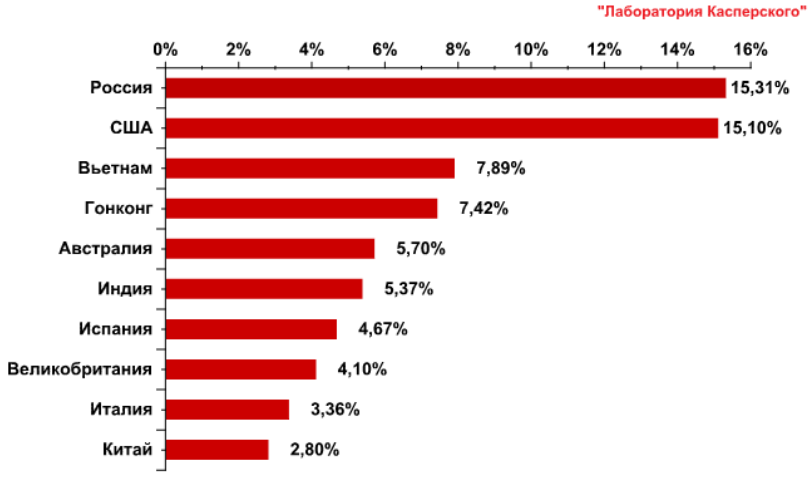
За Индией в нашем рейтинге следуют три страны, чья доля в распространении мирового мусорного трафика по сравнению с ноябрем увеличилась более чем на 3%: Индонезия (+3,55%), Бразилия (+3,5%) и Перу (+3,5%). Одновременно, вклад Южной Кореи, занимавшей в прошлом месяце вторую строчку, уменьшился на 2,85%, что привело к тому, что эта страна оказалась на пятом месте.

Еще одно заметное изменение в рейтинге — смещение Великобритании с седьмой на семнадцатую строчку. Доля спама, распространенного с территории этого государства, уменьшилась на 2,31%. Интересно отметить, что на первой неделе декабря эта страна занимала восьмую позицию, а на последней неделе — лишь 53-ю. Такое перемещение Великобритании в рейтинге в декабре связано в первую очередь с сезоном отпусков — многие служащие в Великобритании отправились отдыхать на время рождественских праздников, оставив выключенными свои рабочие и домашние компьютеры.

Доля остальных стран рейтинга изменилась незначительно — в пределах 1%.

Вредоносные вложения в почте

В декабре вредоносные файлы содержались в 4% всех электронных сообщений, что на 1% больше, чем в прошлом месяце.



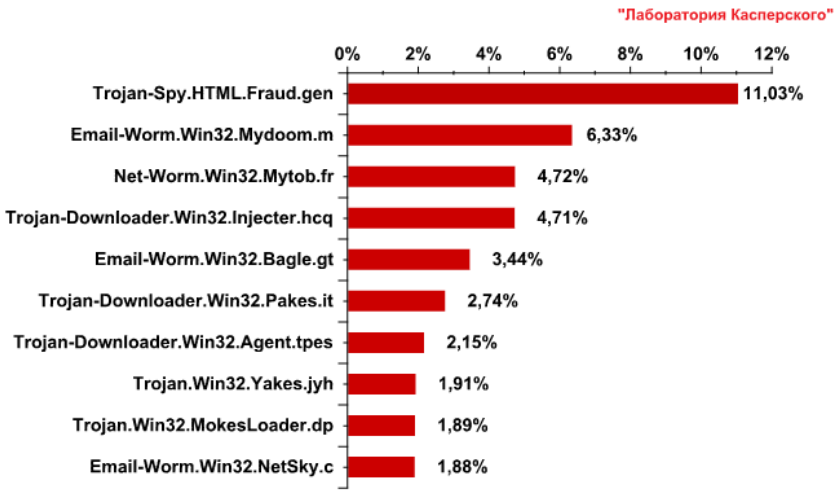
Распределение срабатываний почтового антивируса по странам в декабре 2011 г.

Соединенные Штаты Америки остались на второй строчке рейтинга стран по срабатыванию почтового антивируса. Однако по этому показателю они почти догнали лидера — Россию. Доля детектирований почтового антивируса, пришедшаяся на США, составила в декабре 15,1%, что на 0,9% больше, чем в прошлом месяце. При этом доля срабатываний почтового антивируса на территории России уменьшилась на 4,9% и составила 15,3%.

Австралия поднялась в декабре с десятой строчки рейтинга на пятую. Доля этой страны по сравнению с ноябрем увеличилась на 2,6%.

Хотелось бы отметить появление на четвертой строчке рейтинга Гонконга, а на десятой — Китая. Доля срабатываний почтового антивируса на территории специального административного района КНР составила 7,4%, в то время как на остальной

территории Китая почтовый антивирус Касперского срабатывал почти в два с половиной раза реже — сюда пришлось лишь 2,8% всех срабатываний.



TOP 10 вредоносных программ, распространенных в почте в декабре 2011 г.

Среди программ, наиболее часто детектировавшихся нашим почтовым антивирусом, по-прежнему лидирует Trojan-Spy.HTML.Fraud.gen. Доля срабатываний, связанных с ним, снизилась еще на 1% и составила 11%. Напомним, что Trojan-Spy.HTML.Fraud.gen — вредоносная программа, выполненная в виде html-странички, подделанной под регистрационную форму финансовой организации или какого-либо онлайн-сервиса.

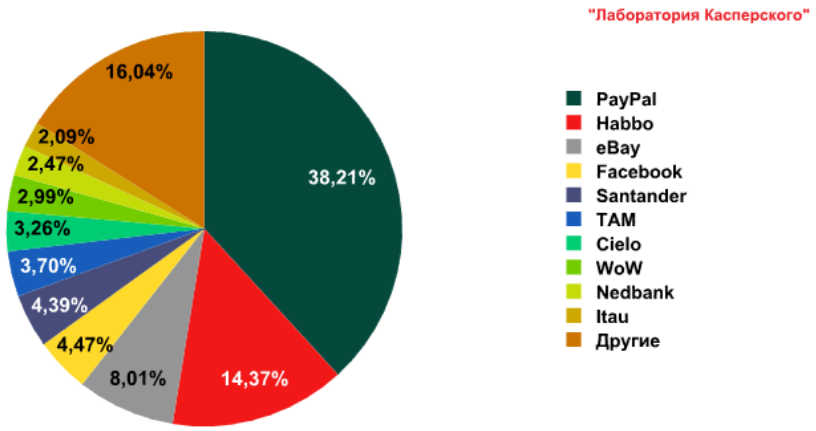
На втором месте вновь Email-Worm.Win32.Mydoom.m — почтовый червь, выполняющий только две функции: сбор электронных адресов на зараженных машинах и рассылку по ним самого себя. Тем же функционалом обладает и занявший десятое место Email-Worm.Win32.NetSky.c. Другой почтовый червь — Email-Worm.Win32.Bagle.gt — расположился на пятом месте. В дополнение к уже обозначенному выше функционалу традиционных почтовых червей этот зловред еще и обращается к интернет-ресурсам для загрузки оттуда вредоносных программ.

В декабре в TOP 10 программ, которые наш антивирус чаще всего детектировал в почте, места с седьмого по девятое занимают программы, являющиеся классическими троянцами-загрузчиками — это Trojan-Downloader.Win32.Agent.tpes, Trojan.Win32.Yakes.jyh и Trojan.Win32.MokesLoader.dp. Эти зловреды после установки на компьютер пользователя обращаются к определенному сетевому ресурсу и получают ссылки для скачивания других вредоносных программ.

Занимающий шестую строчку троянец семейства Trojan.Win32.Pakes является программой-упаковщиком, которая используется для обхода детектирования антивирусными средствами других вредоносных программ.

Фишинг

Доля фишинговых писем в почтовом потоке по сравнению с ноябрем не изменилась и составила 0,02%.



TOP 10 организаций, атакованных фишерами*

* Рейтинг составляется на основе доли фишинговых URL, распространенных в Сети. Рейтинг не является показателем уровня безопасности упомянутых организаций, а отображает популярность различных сервисов у фишеров. Отметим, что фишеры предпочитают атаковать сервисы, наиболее популярные и авторитетные среди пользователей.

В декабре TOP 5 организаций рейтинга осталась неизменной: это PayPal (+5%), Habbo (+1%), eBay (-2,7%), Facebook (-3,6%) и Santander (+0,2%).

Как видно, доля атак на Facebook уменьшилась почти вдвое по сравнению с ноябрем.

В остальном TOP 10 также претерпел мало изменений по сравнению с прошлым месяцем. Интересно, однако, отметить появление на шестой строчки бразильской авиакомпании TAM (3,7%) и исчезновение из рейтинга организации по налоговым сборам США IRS. Эти изменения легко объяснимы: срок подачи налоговых деклараций в США истек, что охладило интерес

злоумышленников к налоговым органам Соединенных Штатов. Одновременно в сезон отпусков множество туристов заказывают билеты на самолет в Сети, чем пользуются злоумышленники, подделывая свои мошеннические сайты под формы авиакомпаний.

Тематические направления в спаме

Тематические категории спама в декабре 2011 г.

Лидером среди популярных спамерских тематик в декабре стал спам, рекламирующий фармацевтические препараты. Больше всего его процент вырос на последней неделе декабря, благодаря чему эта категория попала на первую строчку. Увеличение доли этой категории, как и в целом увеличение доли сообщений, разосланных с целью участия в партнерских программах (+13,5%), связаны в первую очередь со снижением активности среди мелких и средних фирм – клиентов спамеров.

На втором месте среди популярных спамерских тематик оказалась тематика «Образование», его доля по сравнению с прошлым месяцем уменьшилась почти вдвое.

На четвертом месте в декабре категория «Другие товары и услуги». Рост доли сообщений этой тематики связан с большим объемом спама, предлагающего новогодние подарки и иные товары, связанные с новогодним торжеством.

Пятерка лидирующих тематических категорий в спаме:

- Медикаменты; товары/услуги для здоровья 15,2%; +6,3%
- Образование 13,9%; -11,0%
- Недвижимость 13,7%; -2,8%
- Другие товары и услуги 13,2%; +5,3%
- Отдых и путешествия 10,0%; -1,1%

Спам, предлагающий отдых и путешествия, сдал свои позиции (-1,1%) и сместился со второй строчки на пятую. В самом начале декабря, с 5 по 11 число, процент таких сообщений не достиг даже 3%. К концу месяца доля таких сообщений заметно увеличилась.

Интересно отметить, что в четыре раза увеличилась доля спама «для взрослых». Вероятно, такому росту способствовали две причины. Во-первых, перед праздниками многие пользователи более расслаблены и не прочь потратить время на просмотр пикантного видео. Во-вторых, в преддверии Рождества и Нового года одинокие люди еще острее ощущают свое одиночество и стремятся скрасить его хоть чем-то. Спамеры знают о таких особенностях предновогоднего периода и стараются ими воспользоваться.

Заключение

В целом, в отношении спама декабрь был спокойным месяцем. Доля спамерских сообщений в почтовом потоке уменьшилась, что связано как с сезоном отпусков, во время которого многие включенные в ботнеты компьютеры отключены, так и с общим снижением бизнес-активности.

Большое количество писем рекламировало Рождественские товары и услуги, что также было вполне предсказуемо. Заметим, что подавляющее большинство такого рода сообщений — плоды деятельности сезонных партнерских программ.

Неприятной тенденцией всего этого года, сохранившейся и в декабре, является увеличение доли вредоносного спама. В декабре многие вредоносные сообщения эксплуатировали тему Рождества. Кроме того, многие из них были подделаны под уведомления от онлайн-магазинов о регистрации заказа.

В новом году процент вредоносного спама в почте не уменьшится, просто злоумышленники начнут использовать другие приемы для распространения зловредов.

Начало января традиционно является сезоном затишья в спаме. Можно полагать, что начало 2012 года не станет исключением из этого доброго новогоднего правила.

Источник: Securelist.com