пять козырных трюков спаммеров и меры борьбы с ними

крис касперски ака мыщъх, a.k.a. nezumi, a.k.a. souriz, a.k.a. elraton, no-email

мало того, что спамеры вредоносны, так они еще дьявольски хитры и нереально изворотливы. у них все тузы и козыря. чтобы нас не развели как лохов, приходится предпринимать кучу мер предосторожности и держать ухо востро. как говориться, кто предупрежден — тот вооружен!!! рассмотрим основные трюки спаммеров и покажем как им противостоять

трюк первый — как спаммеры добывают адреса

База адресов — основное топливо спаммера, без которого он никуда не уедет. А как создаются такие базы? Самое простое и чрезвычайно эффективное — атака по словарю. Выбирается какой-нибудь популярный почтовый сервер (типа mail.ru) и начинают последовательно перебираются все имена и клички в стиле Alex@mai.ru, Sveta@mai.ru, SuperMan@mail.ru, включая в том числе и инициалы, типа kk@mail.ru. Отсюда — обладатели коротких (или словарных) адресов рискуют попасть в спаммерские базы даже если вообще нигде не будут публиковать свои контакты.

Кстати, о публикации. Оставляя свою мыльницу на форумах, гостевых книгах и прочих отхожих местах типа заборов, многие прибегают к обфускации или, говоря простым языком, маскировке, скрывая их от "пауков", которые как харвестры бродят по сети, отыскивая все, что содержит в себе символ "@" (он же "собака"). Ну это раньше они тупо искали "@"… Теперь же стратегия добычи адресов изменилась. Харвестр, просматривая одну web-страничку за другой, ищет имена известных почтовых серверов, а потом берет все, что расположено слева от них. То есть, "Invisible-Joe гав-гав mai.ru" будет захавано за милую душу. И даже "Invisible-Joe_antismap_at_mai.ru /* remove "_antismap_" */ не спасет, поскольку подобные шаблонные примы уже давно распознаются автоматами. Единственное, что пока более или менее стабильно работает так это — имя после адреса сервера: "пишите мне на mail.ru на Invisible-Joe", хрен какой харвестр его добудет.

Еще круче — написать свое мыло в paint'e, вставляя его как рисунок, желательно на пятнистом неоднородном фоне, затрудняющим "механическое" распознавание, хотя харвестры, распознающие картинки, мне пока не встречались. С другой стороны, далеко не всякий форум и доска объявлений позволяют вставлять картинки, плюс ко всему прочему, пока перепишешь текст с картинки — ошибешься сто раз подряд и вообще писать всякое желание пропадет.

А вот еще один источник угрозы — вирусы, трояны и черви, сканирующие адресные книги и почтовые базы входящих и отправленных писем, добывая из них адреса, вместе с именами получателей. Поэтому, если ты следишь за своей безопасностью, а твой друг — нет, то, во-первых, он тебе не друг, а, во-вторых, писать ему лучше с отдельного ящика, чтобы потом не выгребать мегабайты спама со своей основной мыльницы (что особенно актуально для служебных ящиков, не снабженных мощными антиспаммерскими фильтрами). Впрочем, защита корпоративных ящиков — тема совсем другого разговора и за этим должен следить админ.

Рисунок 1 SPAM – это не ругательство. это торговая марка фирмы, выпускающей низкосортные мясные консервы и рекламирующая их путем разбрасывания рекламных буклетов по почтовым ящикам мирных жителей, которые затрахавшись выгребать горы макулатуры, назвали спамом непрошеную электронную рассылку

трюк второй — из реанимации в морг

Собрать базу почтовых адресов — это только половина дела. Еще, как минимум, предстоит отделить действующие мыльницы от давно заброшенных. Естественно, если обозначенный адрес не существует, то почтовый сервер вернет ругательный ответ и с этим будет все предельно ясно — просто вычерчиваем адрес из списков живых и капец. Если же письмо ушло и не вернулось, то вовсе не факт, что оно действительно доставлено реально существующему получателю. Возможно, он давно забросил этот ящик и уже год как его не посещает. Когда ящик переполнится, сервер начнет возвращать письма, но, учитывая, что многие современные службы предоставляют ящики неограниченного объема (ну, или, _практически_ неограниченного) то переполнение случится нескоро.

Анти-спаммерские фильтры сплошь и рядом режут почту без каких бы то ни было уведомлений, от чего страдают не только спаммеры, но и честные пользователи и прибегать к такой политике борцам со спамом категорически не рекомендуется, поскольку, отправитель _всегда_ должен иметь возможность узнать, что его письмо не дошло до получателя (особенно, если речь идет о корпоративной переписке). Но, увы, политикой поведения фильтров заведуют злобные администраторы у которых свое видение проблемы. Мы не понимаем их, они не понимают нас… Но оставим в покое администраторов и вернемся к нашим баранам, то есть спаммерам.

Даже если спам достиг ящика пользователя, получатель мог удалить его даже не открывая, просто прочитав название темы и отправив непрошеную корреспонденцию в корзину (что особенно удобно делать через web-интерфейс, локальные же почтовые клиенты обычно автоматически загружают письмо в окне предварительного просмотра — стоит только поднести к нему курсор, а если не подносить — то как, черт возьми, его удалить?!).

Спаммерам нужно предельно точно знать какой процент писем был реально доставлен и прочитан (поскольку, если этот показатель станет неожиданно низким — придется

разрабатывать новые технологии рассылки). Специально для этой цели и рассылаются письма в HTML-формате со ссылкой на рисунок, лежащий на web-сервере, подконтрольном спаммеру.

Почтовые клиенты автоматически загружают такие картинки при просмотре письма, что не только доказывает факт его получения, но и позволяет определить тип установленных фильтров и систем защиты. В частности, антивирусы загружают лишь заголовки графических файлов (поскольку некоторые из них содержат некорректные поля, приводящие к переполнению локальных буферов и как следствие — атакам на систему), анти-спаммерские фильтры так же загружают картинки (особенно когда все письмо целиком из одной картинки и состоит), но заголовок HTTP-запроса фильтра сильно отличается от HTTP-заголовка почтового клиента. Самое главное — если картинок больше одной и сервер умышленно замедляет их отдачу, то спамер без труда определит какое время потратил получатель письма перед отправлением его в корзину. Вот тебе бабушка и приватность!!! Все тайны — как на ладони!!!

Как избавиться от такой напасти? Единственный способ — отключить автоматическую загрузку картинок (в разных почтовых клиентах это делается по разному и тут надо курить руководство пользователя), а еще лучше вообще отключить HTML, чего, кстати, Outlook Express ну никак не позволяет, зато The Bat справляется с этим без проблем!!! Конечно, в текстовом виде письма смотрятся серо, однообразно и скучно, зато у спамеров не остается никакой возможности узнать — было ли письмо прочитано или нет.

Рисунок 2 "Make love, not smap" (трахайся как собака баскервилей, не распространяй спам) — девиз молодежи нового века!

трюк третий — обходим серверные фильтры

Вот два основных критерия по которым фильтры, установленные на почтовых серверах, распознают спам это или не спам. Первое — IP-адрес отправителя, второе — содержимое письма. Существующие распределенные антиспамерские базы оперативно заносят "проштрафившиеся" IP-адреса в "черные списки" и рассылка дохнет буквально через несколько часов после ее начала, конечно, при том условии, что она осуществляется с одного или нескольких фиксированных IP-адресов. Обходить "черные списки" не научился только ленивый. Спамеры рассылают червей, расползающихся по всей сети и проникающих в сотни тысяч компьютеров, захватывая над ними полный контроль. Пораженные узлы называются "дронами", а их совокупность образует ботнет, позволяющий спамеру вести рассылку сразу со всех направлений. Даже если каждый дрон разошлет всего десяток писем прежде, чем попадет в "черный список", база из ста тысяч дронов доставит корреспонденцию миллиону адресатов!!!

И вот чтобы этого не происходило, на крупных почтовых серверах установлены продвинутые фильтры, анализирующие содержимое всех писем и блокирующие спам независимо от того, с какого адреса он пришел. За минувшие годы спамеры испробовали множество методик борьбы с контентными фильтрами, слегка модифицируя содержимого каждого отправляемого письма (или серии писем) так, чтобы сигнатурный поиск не сработал. И вот тут-то разработчикам фильтров пригодились антивирусные движки, детектирующие полиморфные вирусы (т. е. изменяющие свое тело). Дольше всех продержался графический спам, поскольку, в графику очень легко вносить незначительные (с точки зрения человека) трансформации, совершенно преображающие байтовый поток с машинной точки зрения, но прогресс не стоит на месте и доля графического спама после внезапного всплеска сейчас пошла на спад.

Между тем, спамеры все это время не сидели сложа руки и вместо того, чтобы почевать на лаврах, ковали новое оружие возмездия, которое в ближайшее время будет запущено в промышленную эксплуатацию. Идея заключается все в тех же картинках, внедренных в HTML и расположенных на внешних серверах. Поскольку, заголовок HTTP-запроса позволяет с достаточной точностью идентифицировать клиентское приложение, то антиспаммерскому фильтру "подсовывается" одна картинка (сгенерированная абсолютно произвольным образом), а "честный" адресам получает рекламную рассылку.

Как можно этому противостоять? С клиентской стороны — никак (единственный выход — запретить загрузку картинок), но вот разработкам фильтров достаточно "прикинуться" настоящим почтовым клиентом и тогда спамер будет вынужден показать им рекламную картинку в том виде, в каком она есть, после чего защемить его — уже не проблема.

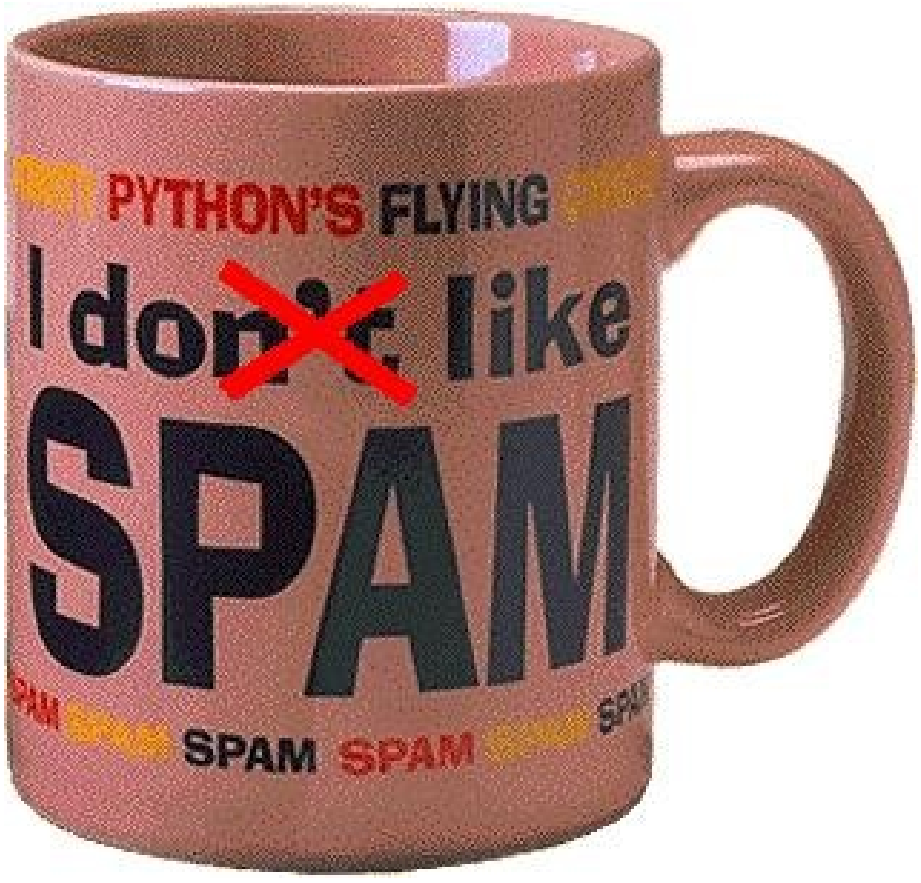

Рисунок 3 каждый протестует против спама как только может

трюк четвертый — спам или не спам?!

Несмотря на ожесточенную борьбу со спамом, какая-то часть непрошеной корреспонденции все-таки доходит до народа и тут самое главное, составить послание так, чтобы жертва прочитала его прежде, чем успела нажать на <DEL>. А для этого приходится мухлевать не по-детски.

Начнем с поля отправителя письма. "Слепые" поля — верный признак спама и большинство почтовых клиентов отправляет такие письма в Junk-folder или помечает их красным цветом, типа — внимание! возможно, это спам! А потому, крутись — не крутись, а какое-то имя вставить надо. Ну, скажем, Alex, Peter, Olga… Фамилию лучше не вставлять — фамилии у всех разные, а незнакомая фамилия сразу обостряет внимание получателя, заставляя его машинально тянуться к клавише <DEL>. Впрочем, голое имя без фамилии в нормальной жизни — явление не самое часто. Что делать?!

А вот что! Использовать шаблонные имена, типа "Интернет-Магазин…", "Служба поддержки…". Учитывая, что далеко не все пользователи используют широкие колонки для имени отправителя, то придумывать что это за магазин такой и чего мы поддерживаем — совершенно необязательно! С определенной долей вероятности пользователь вообще не увидит продолжения названия из-за узкой колонки, а письмо от магазина (в котором он, возможно, заказывал товар), а уж тем более службы поддержки он все-таки откроет.

Статистика показывает, что, как бы ни изощрялся спамер, ему отпущены считанные секунды, в течении которых пользователь (если он не даун, конечно) легко и безошибочно распознает спам, отправляя его в корзину. Некоторые (особо "одаренные") спаммеры пытаются подделывать стиль письма, посылая макулатуру в стиле "привет, любимый… бла-бла-бла, а я вот тут недавно озаботилась поиском чугунных труб и решила, что ничего лучше чем продукция фирмы Рога и Копыта в нашей округе не нашла. звони им по телефону 55-555-555, целую тебя в хвостик".

Теоретически, написать письмо, которое будет воспринято как послание от близкого человека, вполне возможно, но практически… полезный выхлоп у такой рассылки будет нулевой. Поэтому, новая волна спаммеров наконец-то наладила контакт с мозгами и, вспомнив давно забытую фразу, что кратность сестра таланта, стала бороться за каждое слово. "чугунные трубы любой длинны. самовывоз из мухосранска. 555-555-555". Тот, кому эти трубы совсем не приснились, все равно не клюнет на рекламу и не позвонит. А вот если получатель хотя бы потенциально способен совершить покупку, то он должен прочесть рекламный текст прежде, чем успеет его удалить, а потому текст должен быть предельно кратким и правильно оформленным с точки зрения дизайна.

Как бороться со спамом такого типа? Ответ — начинать чтения письма с конца, точнее даже не с конца, а с последней строки, отображающейся в окне предварительно просмотра. Даже у грамотно сконструированного спама шансы на выживание при этом резко сокращаются.

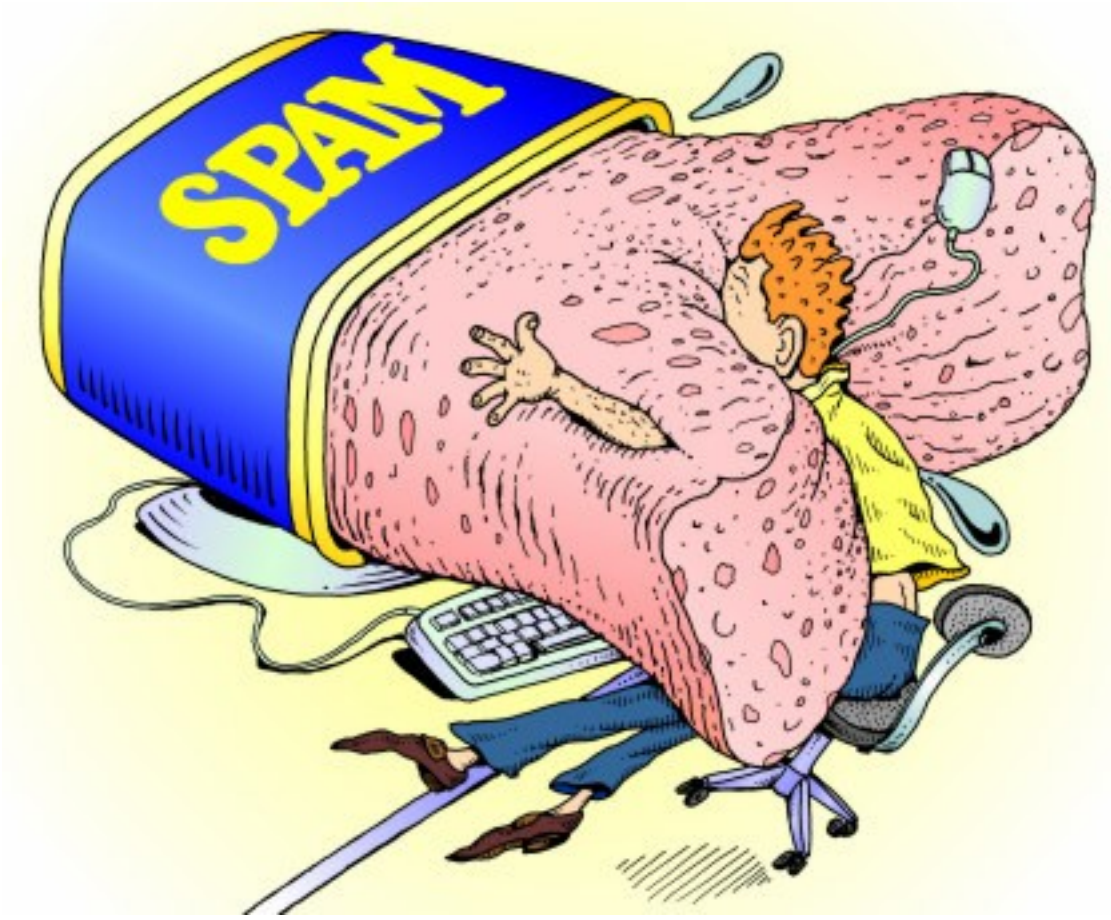

Рисунок 4 захлебнувшийся в потоке спама

трюк пятый — атака на поисковые машины

Почта — это, конечно, хорошо и очень правильно, но… в последнее время все большую актуальность приобретают нападки на поисковые машины. Цель спаммера — сформировать запрос, который поисковик выдаст в числе первых и по которому человек с высокой степенью вероятности зайдет на сайт, рекламирующий _совсем_ не то, что ожидалось. На первый взгляд, такое невозможно! Поисковые машины давно уже вышли из ясельного возраста и научились автоматически удалять "нарушителей" из индексной базы. К тому же никакой спаммер не может заранее знать, что наберет в строке поиска тот или иной пользователь.

На самом деле тут есть одна лазейка, позволяющая нечестным WEB-страницам подниматься вверх, довольно долго удерживая свои позиции. Всякий раз, когда пользователь щелкает по ссылке, его браузер посылает WEB-серверу предыдущую ссылку в специальном после Referer. В случае с поисковиками это поле, как правило, содержит полную строку запроса и номер текущей страницы поиска. То есть, если на наш сайт все-таки зашли (возможно, даже чисто случайно, по неполному совпадению ключевых слов), владельцу сервера ничего не стоит поднять логи и по строке "Referer" восстановить полную картину происходящего.

Вот пример из личной жизни. Смотрю я лог своего мыщъхиного сервера и вижу там: http://www.google.de/search?hl=de&q=**Remove**+**PAGE_NOACCESS**&btnG=Google-Suche&meta=, мне становится интересно что же реально искали и что нашли? Копирую ссылку в адресную строку браузера и… в первой же строке запроса вижу свою книгу — "Hacker Disassembling Uncovered". Поразительно по каким только ключевым словам ее не находят!!! Естественно, накапливая поисковые запросы, по которым люди заходят на мой сервер, мыщъх мог бы существенно повысить рейтинг посещаемости, только ему это на фиг не нужно, ибо сервер дохода не приносит и установлен исключительно из желания почувствовать себя администратором ;) Но вот владельцы других ресурсов, похоже, этой возможностью не брезгуют, активно ее используя, в результате чего на запрос "IR-mouse" поисковики зачастую выдают ответы вида: "best IR-mouse and hottest girls! lowest prices!!!" Ну, коза с поршнем от мотоцикла уже вошла в историю, но вот ночная фея с инфракрасной мышью — это что-то

новенькое ;) Вот только нажав на ссылку, мы с высокой степенью вероятности не получим ни того, ни другого и нам вновь предложат чугунные трубы или точную копию часов от версачи по цене 2 убитых енота за погонный метр.

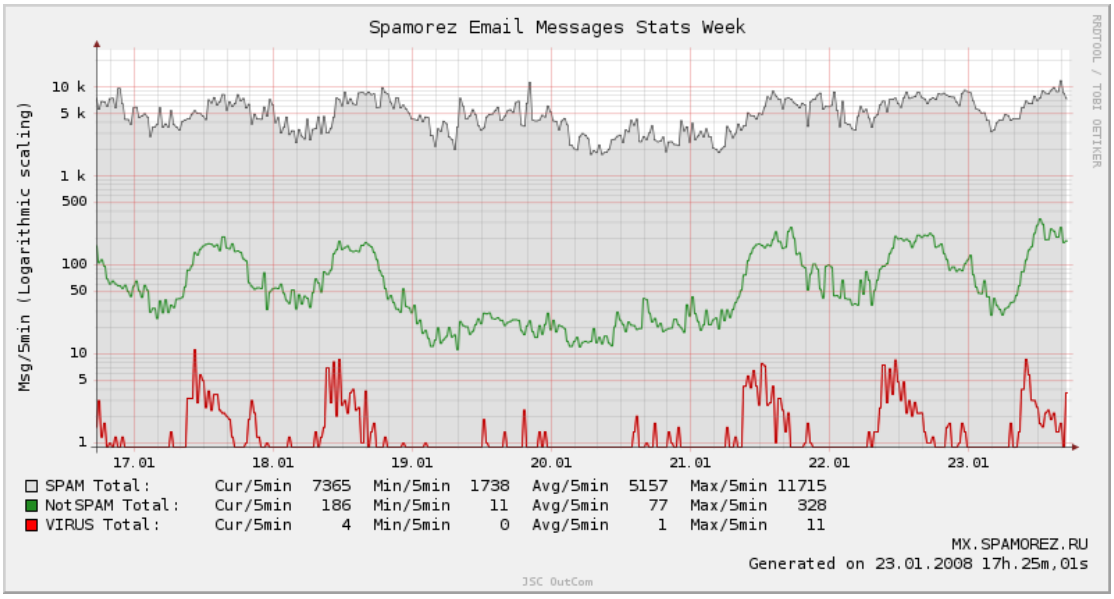

Рисунок 5 недельный суммарный почтовый трафик (логарифмическая шкала) по данным www.spamorez.ru/weekly.html

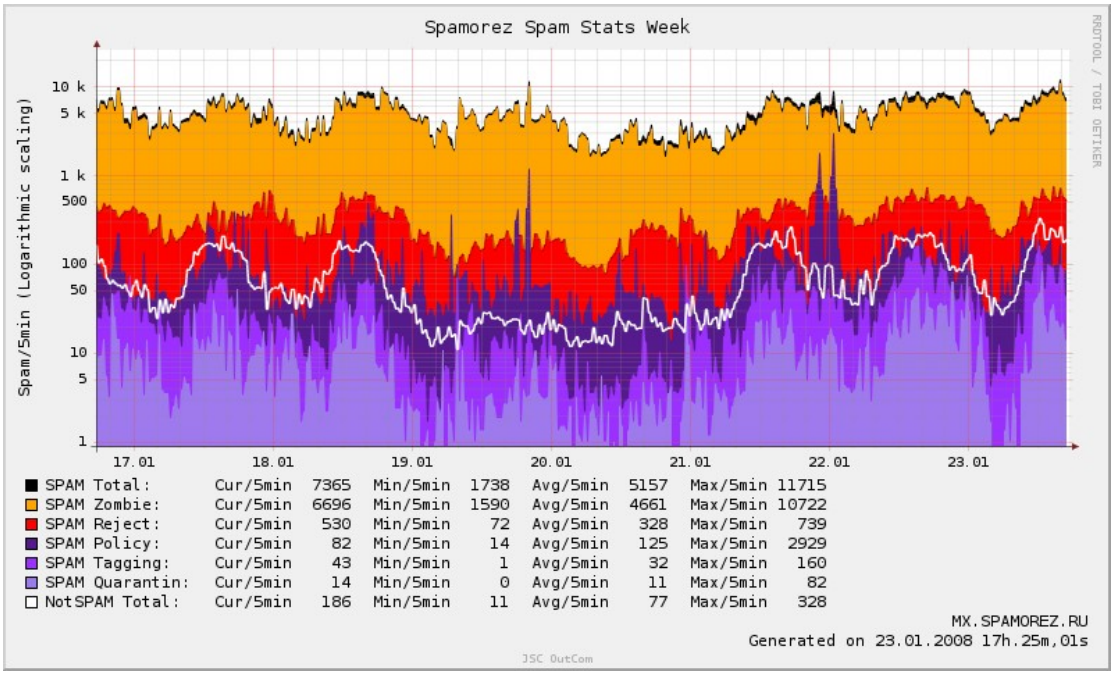

Рисунок 6 детализированный недельный SPAM трафик (логарифмическая шкала) по данным www.spamorez.ru/weekly.html

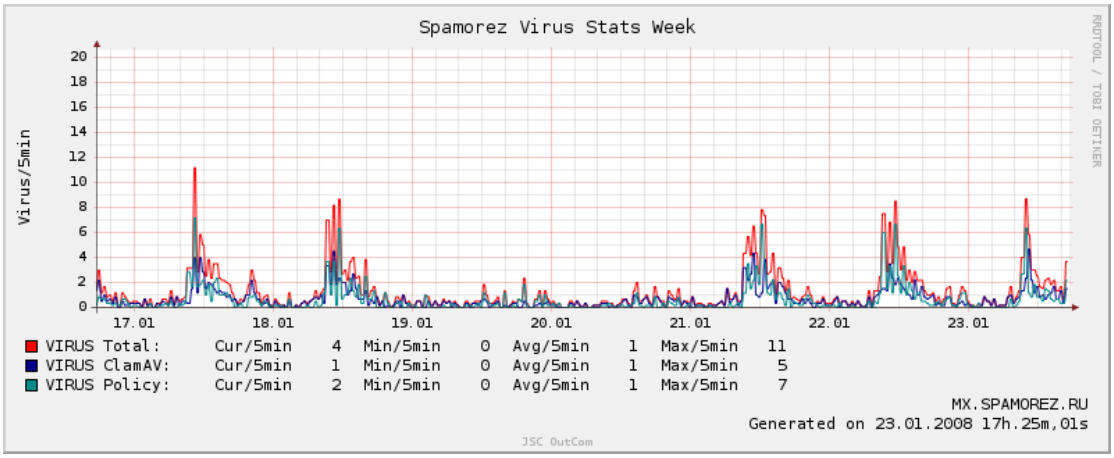

Рисунок 7 недельный virus трафик по данным www.spamorez.ru/weekly.html