шесть правил непопадания в спаммерские базы

крис касперски, ака мыщъх, ака nezumi, aka elraton, aka souriz, aka толстый хомяк, no-email

когда спаммерские харвестры бороздят сетевое пространство в поисках майл-адресов, а пользователи, погребенные под тоннами рекламной макулатуры, высаживаются на конкретную измену, не понимая каким же образом стервятникам удалось добыть их адрес на этот раз, ведь, казалось бы, были предприняты все меры предосторожности! методики сбора майл-адресов довольно продвинуты и одним лишь блужданием по паутине совсем не ограничиваются. ниже будет показано как максимально обезопасить себя от нежелательной корреспонденции.

введение

Чтобы не получать спама, достаточно "всего лишь" не попасть в спаммерские базы, прошмыгнув мимо них словно старая крыса Шушара из сказки про Рики-Тики-Тави. Но крысе было легко! У нее один хвост чего весит, а нам, бесхвостым, прошмыгнуть не так-то просто. Спамеры это не голые негры (простите, афро-африканцы), бегающими по пустыне с луками и копьями в поисках жратвы (см. рис. 1). Нет! Спамеры — это весьма технически продвинутые и невероятно циничные хакеры, оснащенные самым современным оружием, созданным не только для массовой рассылки, но и для автоматизированного поиска mail-адресов. В этой отрасли крутятся большие деньги (расценки на электронную рекламу регулярно приходит по сети сама) и бороться со спаммерами голыми руками все равно что падать грудью на амбразуру. Лучше незаметно раствориться во тьме, заныкав свой mail-адрес как можно глубже.

Существует ряд довольно простых правил, следование которым сокращает вероятность спаммерской атаки на 90%! Причем все они не требуют никаких дополнительных усилий или телодвижений. Ну… почти никаких!

Рисунок 1 вообще-то, изначально SPAM'ом назывались дрянные мясные консервы, агрессивно продвигаемые на рынок путем забрасывания почтовых ящиков (не электронных) горами рекламной макулатуры

правило N1: испытание сервера на прочность

Прежде чем выбрать mail-сервер для постоянной деловой переписки, необходимо удостовериться, что он надежно защищает адреса своих клиентов от чужих загребущих лап, но в тоже время не сильно усердствует в борьбе с нежелательной (с _его_ точки зрения) рассылкой, и не включает спаморезку на полную мощью.

Просто зарегистрируйтесь на подопытном сервере и периодически (в течении одной-двух недель) отправляйте письма на свои же адреса, зарегистрированные на других серверах — просто, чтобы имитировать сетевую активность (спаммерам "мертвые" ящики не интересны). Если за все это время не придет ни одного "левого" письма, сервер можно считать более или менее надежным, но прежде чем им начать пользоваться, необходимо зарегистрироваться на hotmail'e, yahoo и других бесплатных зарубежных серверах и попытаться отправить себе письмо оттуда. Довольно часто письма не проходят, попадая под нож спаморезки, в результате чего мы теряем возможность переписки с большим количеством респондентов. Ну и на хрена нам такая защита от спама?!

Из личного опыта: mail.ru — достаточно надежен, и мыщъх пользуется им долгое время, получая минимум спама и практически не теряя на спам-фильтрах ценных писем. Другой хороший сервис — www.fastmail.jp.

правило N2: легкая добыча — короткие и словарные имена

Каждый пользователь (я имею ввиду нормальный пользователь, а не какой-то там извращенный хакерский гугу, помешанный на безопасности) хочет иметь короткое и легко запоминающееся имя, которое можно передать друзьям по sms, записать в блокнот, напечатать на визитке и т. д. Что-нибудь в стиле n2k@mail.ru, kk@sendmail.ru. К сожалению, подобные имена (при всей их внешней привлекательности) становятся легкой добычей спаммеров, поскольку элементарно вскрываются методом лобового перебора. Спам валит мегатоннами и ничего другого не остается как идти сдаваться на мясокомбинат. Тоже самое относится и к словарным именам типа: SuperHero@yandex.ru — это вообще не вариант! Равно как и anton@zmail.ru (внимание! все вышеприведенные адреса взяты наобум методом взмаха хвоста и если они соответствуют _реальным_ адресам, то мыщъх тут совсем не причем и просьба его не пинать). Добавление цифр, указывающих на год рождения в стиле luba_76@rambler.ru, положения не спасает, поскольку существует не так уж много возможных вариантов.

Чем длиннее имя — тем лучше. Но и перебарщивать тоже не след. Восьми символов в большинстве случаев оказывается вполне достаточно и такие адреса уже не могут быть найдены методом перебора за разумное время, во всяком случае спамеры подобными атаками не занимаются.

Рисунок 2 программы для авторизированного сбора электронных адресов обычно называют либо пауками (spider), либо харвестрами (harvester) — по одной из первых утилит, написанной еще в середине девяностых

правило N3: мой друг — враг мой

Крайне нежелательно давать свой адрес людям, пренебрегающих установкой свежих заплаток и запускающих все вложения без разбору, что только приходят им по сети. Стоит только вступить с ними в переписку, как уже через короткое время можно обнаружить, что поток спама возрос на порядок, причем не двоичный порядок, а десятичный или даже… шестнадцатеричный!

Все очень просто — это раньше червей и вирусов писали из "любви" к человечеству или от нечего делать. Сейчас черви активно используются спаммерами и являются идеальным средством сбора майл-адресов. Проникнув на машину, червь первым делом лезет в адресную книгу Outlook Express или The Bat!, а так же сканирует почтовую базу на предмет наличия адресов отправителей и получателей, после чего передает накопленную информацию своему владельцу. Существует мнение, что в настоящее время данный механизм является основным способом добычи майл-адресов, и не порядка 60%-70% майл-адресов спаммеры добывают именно так!

Такова природа сети и против нее не попрешь. Мир тесен и через знакомых своих знакомых можно выйти на кого угодно. Математики говорят, что в среднем для этого достаточно построить цепочку длинной в десять человек. И ведь правда! Лично меня от Бориса Ельцина отделяет трое знакомых, а от Примакова (ну тот, который министр) всего один (точнее, одна очаровательная научная сотрудница, работающая под его руководством и занимающаяся эпиграфикой — эпиграфика: это наука о расшифровке коротких надписей на памятниках, если кто вдруг не в курсе)! И хотя я не знаю ни одного человека, чей знакомый "в десятом поколении" здоровался бы за руку с Клинтоном или на худой конец Билом Гейтсом, вся эта статистика относится к реальной жизни. В сети же правила другие и достаточно дорваться до одной-единственной почтовой базы… (что касается меня, то я почтовые базы не удаляю со дня своего первого вхождения в Сеть и за восемь лет там накопилось огромное количество как действующих, так и бездействующих адресов, но действующих все же больше!).

Ладно, для переписок (и писок тоже) с девушками и друзьями можно (и нужно!) завести отдельный ящик, еще один ящик — для регистрации на всяких там форумах или виртуальных магазинах… современные почтовые клиенты позволяют работать с любым количеством ящиков, обеспечивая при этом надлежащий уровень комфорта, но… проблема в том, что

никакое количество ящиков не решает проблемы, основной источник угрозы которой исходит от корпоративных респондентов, — тех самых, что (по идее!) должны быть железобетонно защищены. Увы! Сплошь и рядом администраторы вспоминают о заплатках только тогда, когда черви вовсю гуляют по сети, и что еще хуже — торгуют почтовыми адресами без всякого стеснения…

Лично мыщъх прибегает к такой тактике: сначала начинает переписку с компанией (даже очень крупной, значительной и именитой) со специально созданного ящика, и если только в течении месяца-двух на него не начинает сыпаться спам, "рассекречивает" свой основной адрес. Конечно, в первую очередь все эти игры в "секретность" неудобны мне самому. Приходится держать кучу ящиков, и постоянно помнить кому и какой адрес ты дал. Но зато основной ящик, автоматически проверяемый каждые 5 минут, в 99% содержит только полезную корреспонденцию, на которую можно отреагировать немедленно. А при необходимости и задействовать переадресацию на сотовый телефон с виброй и звонком, чтобы поднять сонную тушку из постели, поскольку, если пришло свежее письмо — то это же неспроста!

правило N4: не оставляйте адреса в сети

Сеть, изначально созданная для общения, со временем превратилась в лабиринт, опутанный колючей проволокой. Если _никто_ и _нигде_ не будет оставлять своих адресов, то, соответственно, никто никому не станет и писать. А ведь созерцать лаконичную надпись "новых сообщений нет" никому не хочется! Душа просит свободы! Душа хочет завести друзей во всех концах света, и просто красивых девушек азиатской внешности, и бесшабашных французских парней, что могут пригласить загадочного русского из заснеженной страны Сибири на концерт любимой группы, только потому что вы оба фэны, а фэнам всегда есть о чем поговорить. Наконец, программист (астроном, лингвист) какой бы он ни был крутой специалист, находясь в изоляции, всегда загнивает. Общение с коллегами — это словно свежего воздуха глоток. Без обмена идеями, без диспутов и споров (иногда переходящих в священные войны) мы бы никогда не стали бы теми, кто мы есть сейчас. Кто-то может мне резонно возразить: общаться-то можно и на форумах, не оставляя никаких адресов (ну разве что для регистрации, но это не в счет). Обломайтесь, мужики! На форумах уже давно в основном идет треп за жизнь, демонстрация собственной крутизны и надругательство над новичкам. Серьезные технические проблемы там обсуждаются крайне редко, поскольку, зачастую они тесно связаны с NDA, и к тому же драть свою задницу, выполняя чужую домашнюю работу никто просто так не будет! А вот по мылу (по принципу "ты — мне, я — тебе") — запросто!

Так что технические проблемы преимущество обсуждаются по мылу. Через списки рассылки или персонально. Ну если со списками рассылки все понятно (достаточно присоединиться к интересному проекту), то с мылом не все так просто… чтобы нам могли писать, нужно оставить адрес на форумах, блогах, собственных сайтах и куче других туссовочных мест. Ведь фокус в том, _как_ их оставлять. Запись вида kpnc@sendmail.ru любой харвестр схавает сразу, после чего спам хлынет мощным потоком как из прорвавшей канализационной трубы. Кое-то пытается хитрить: kpnc at mail dot ru. Та же самая запись, только по-английски — символ "@", прозванный в народе "собакой", в действительности, читается как "коммерческое АТ", следовательно, в русской нотации этот же адрес выглядит так: kpnc гав-гав mail точка ru.

Ставка делается на то, что человек (с IQ отличным от единицы) обязательно это поймет, а механический харвестр обломается. На самом деле все происходит с точностью до наоборот. Как на счет записи: jose.palanco perro eazel punto es? Подсказка — eazel: домен почтового сервера, а punto — "точка", но только по-испански. Так что, подобные извращения катят только среди своих, а иноземные граждане при попытке дешифровки "каракулей" даже не догадываются, что за ними скрываются действующий почтовый адрес на который предполагается что-то написать. Креативы в стиле kpnc_nospam_at_mail_ru из той же оперы.

Харвестры ведь возникают не сами по себе. Их люди пишут и эти люди отнюдь не дураки. И с IQ у них все в порядке. Очень часто используется следующий алгоритм: харвестр находит доменное имя популярного сервера (например, mail, yandex), после чего трактует все, что слева от него как потенциальное имя клиента. В частности, pedrilo perro yahoo punto com, превращается в: perro@yahoo.com; pedrilo@yahoo.com, после чего по обоим адресам производится пробная рассылка писем. Адреса "perro@yahoo.com" скорее всего не существует (т. к. "perro" и есть "@" только по-испански), а вот pedrilo@yahoo.com сразу палится.

Некоторые до сих пор по своей наивности считают, что харвестры в основном ищут адреса по символу @ вот и заменяют его всем чем ни попадя, в том числе и графическим

изображением. Но харвестрам это не помеха, поскольку символ "@" уже давно не единственный и совсем не характерный признак электронного адреса. Главный критерий — это доменные имена самих почтовых серверов, которые хорошо известны и которые так просто не спрячешь.

Единственное, что можно предпринять — это записать свой адрес целиком в графической форме и прикрепить на форум в виде изображения. Если только не называть его my-email, то харвестр обломается OCR'ить все графические изображения… хотя….может и не обломается, поскольку как показывает статистика, такие изображения имеют довольно характерные пропорции и размеры, поэтому, для облома харвестров изображение должно быть _большим_ (например, портрет в профиль ниже пояса) с надписью е-майла на ягодицах. Против ягодиц бессильны даже самые продвинутые харвестры. Правда, при этом возникает другая проблема. Чтобы отправить сообщение, наш респондент должен _вручную_ переписать его буква-за-буквой, нигде при этом не ошибавшись, иначе трынденц (причем полный). Следовательно, мыло должно быть коротким, незатейливым и простым, а желательно даже словарным, но это противоречит правилу два и мы оказываемся в позе буриданового осла, короче в полной прострации и ауте.

А если учесть, что не все форумы допускают присоединение графических изображений, становится совсем хреново. Пожалуй, единственный разумный выход — заменить email ссылкой на страницу, где он лежит. Заводим себе бесплатный хостинг, размещаем там изображение своего мыла в графической форме, а на формумах даем URL на эту страницу. И все! То есть нет, не все. Вместо графического изображения можно разместить Java-скрипт, содержащий зашифрованный email и расшифровывающий его (с выводом на экран в виде гиперссылки) только при нажатии на кнопку или иконку. Среди всех харвестров, которые только мыщъху доводилось видеть, с подобными защитами еще не справляется ни один. А нашим респондентам всего-то и достаточно совершить два клика мышью и не нужно дешифровывать никаких каракулей.

Чтобы не писать систему шифрования вручную, можно воспользоваться одной из готовых программ, специально написанных для этих целей, например: HTML Protector'ом (antssoft.fileburst.com/htmlprotector.zip), HTML Power'ом (www.pullsoft.com/htmlpower.zip) или Encrypt HTML Pro (www.mtopsoft.com/download/enchp.zip).

правило N5: сбивайте спаммеров ракетой класса mailer-daemon

Что же делать, если спамерское письмо все-таки пришло? Материться (первым делом) — это понятно. Ну а по существу?! Некоторые письма содержат адрес, написав на который можно якобы отказаться от дальнейшей рассылки. Но делать этого ни в коем случае не следует, иначе спамер поймет, что адрес "живой" и письма повалятся с новой силой!!!

Если есть желание рискнуть, можно попробовать накрыть спаммера баллистической ракетой типа **mailer-daemon**. В смысле послать поддельное письмо от имени сервера, что данный адрес не существует. Достаточно часто (хотя и не всегда) спаммеры отслеживают такие "ракеты" и вычеркивают недействительные адреса из своих баз, чтобы не распылять трафик впустую. Весь вопрос в том, как подделать такое письмо? Как сконструировать ракету класса mailer-daemon? Очень просто! Однако, не все почтовые клиенты для этого пригодны. Нам понадобиться The Bat! или… telnet. Работа с telnet'ом подробно описана в моей "технике сетевых атак", которую можно бесплатно скачать с ftp://nezumi.org.ru, ну а со скрытыми возможностями The Bat'a мы познакомимся прямо сейчас.

Для начала нам понадобится образец "ругательства" mail-daemon'a, который можно получить отправив письмо на заведомо несуществующий адрес, например, на putaaaaaaaaa@fastmail.jp и тогда через некоторое время придет ответ следующего содержания (см. рис. 3)

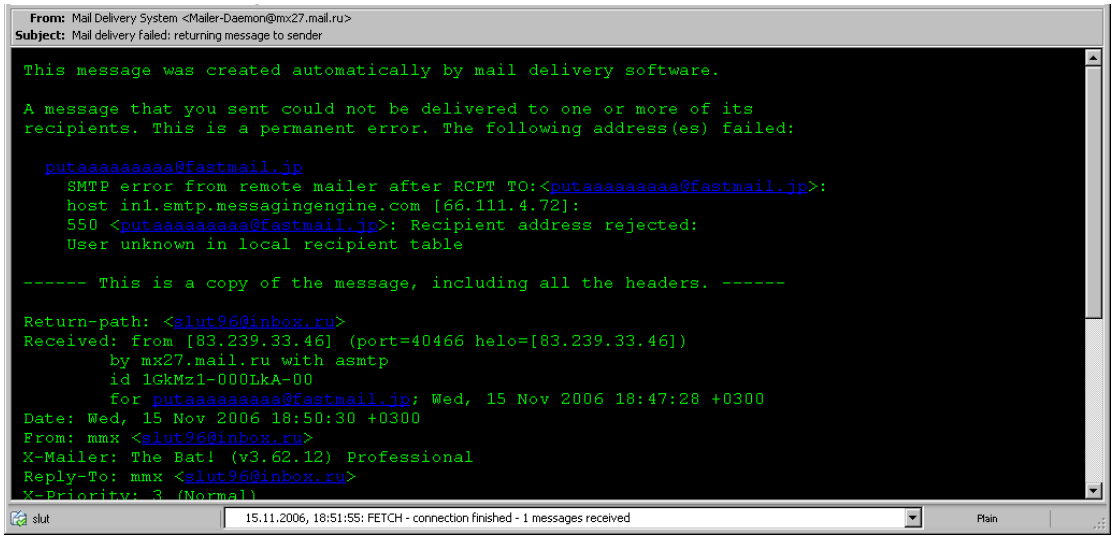

Рисунок 3 ругательство mail-daemon'а на попытку отправить письмо несуществующему адресату

Сейчас мы быстренько перетащим этот текст через буфер обмена и вставим его в новое письмо, запустив прямой наводкой в сторону спаммера, да? Ага! Вот так сейчас и разбежались! Еще надо найти того лоха, который купиться на столь грубую подделку! Тем более, что возращенные письма анализирует не человек, а автомат. И анализирует он их так…

Нажимаем <F9> (source) чтобы увидеть исходное содержимое письма, возращенного mailer-daemon'ом со всеми служебными заголовками и сосредоточенно вкуриваем:

```
Return-path: <>
Received: from mail by mx27.mail.ru with local
        id 1GkN0B-000N85-00
        for slut96@inbox.ru; Wed, 15 Nov 2006 18:48:39 +0300
X-Failed-Recipients: putaaaaaaaaa@fastmail.jp
From: Mail Delivery System <Mailer-Daemon@mx27.mail.ru>
To: slut96@inbox.ru
Subject: Mail delivery failed: returning message to sender
Message-Id: <E1GkN0B-000N85-00@mx27.mail.ru>
Date: Wed, 15 Nov 2006 18:48:39 +0300

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

  putaaaaaaaaa@fastmail.jp
    SMTP error from remote mailer after RCPT TO:<putaaaaaaaaa@fastmail.jp>:
    host in1.smtp.messagingengine.com [66.111.4.72]:
    550 <putaaaaaaaaa@fastmail.jp>: Recipient address rejected:
    User unknown in local recipient table

------ This is a copy of the message, including all the headers. ------

Return-path: <slut96@inbox.ru>
Received: from [83.239.33.46] (port=40466 helo=[83.239.33.46])
        by mx27.mail.ru with asmtp
        id 1GkMz1-000LkA-00
        for putaaaaaaaaa@fastmail.jp; Wed, 15 Nov 2006 18:47:28 +0300
Date: Wed, 15 Nov 2006 18:50:30 +0300
From: mmx <slut96@inbox.ru>
X-Mailer: The Bat! (v3.62.12) Professional
Reply-To: mmx <slut96@inbox.ru>
X-Priority: 3 (Normal)
Message-ID: <374497972.20061115185030@inbox.ru>
To: putaaaaaaaaa@fastmail.jp
Subject: test
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

hello, putaaaaaaaaa!
```

Листинг 1 как ругаются mail-daemon'a

Ответ mailer-daemon'a состоит из трех частей: служебных заголовков письма самого daemon'a, за которыми следует текст ругательства с приложенной копией исходного письма. Собственно говоря, различные mailer-daemon'ы отвечают слегка по разному и чтобы робот смог скурить их ответ он должен обращать внимание на определенные поля, описанные в RFC-1891 (ftp://ftp.rfc-editor.org/in-notes/rfc1891.txt). Да только кто же те RFC читает? Вот программисты и действуют наугад. Одни проверяют поле "subj" на предмет строки "Mail delivery failed: returning message to sender". Вообще-то, это не единственно возможный вариант ответа daemon'a, но, пожалуй, самый частый, а "subj" легко "подделывается" в любом почтовом клиенте. Другие же смотрят на нестандартное поле "X-Failed-Recipients: putaaaaaaaa@fastmail.jp", присутствие которого расценивается как трындец. Подделать это поле на порядок сложнее.

На помощь приходит могучий мышь в лице The Bat! Нажимаем <CTRL-N> для создания нового сообщения и в меню "View" видим пункт "Edit Headers", открывающий огромное окно с кучей настроек из которых нам нужны только "Message Headers" (сообщения заголовков). Нажимаем кнопку "ADD" и в поле "Display this header field as" (отображать данное поле заголовка как) вводим строку "X-Failed-Recipients:" (со знаком двоеточия на конце), а в поле "RFC Name (as it used in the RFC 822 header)" (RFC имя по стандарту RFC 822) пишем "X-Failed-Recipients" (уже _без_ знака двоеточия на конце). Взводим галочку напротив "Allow to edit this field in the Message Editor" (разрешить редактирование этого поля в редакторе сообщений) и дважды жмем на "OK".

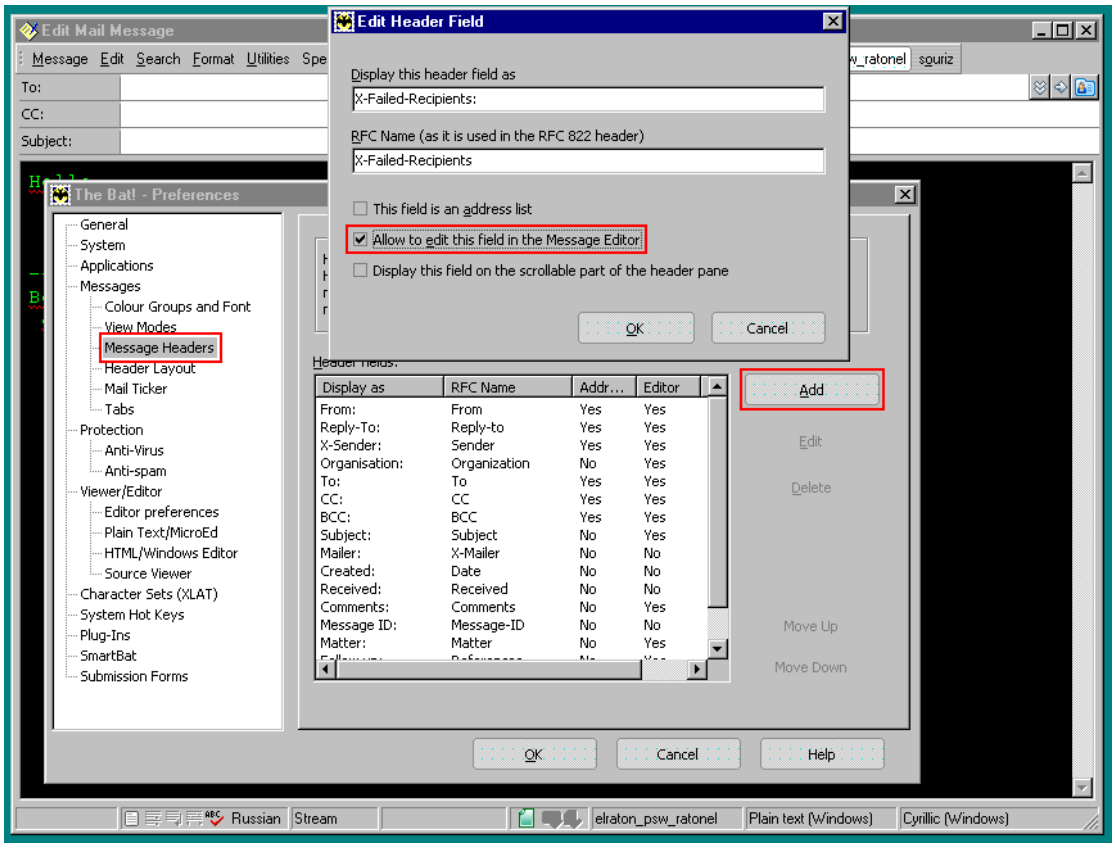

Рисунок 4 расширение функциональных возможностей The Bat'a, путем добавления поля X-Failed-Recipients в заголовок письма

Все! Теперь в меню "View" появляется новый пункт "X-Failed-Recipients:", поставив галочку напротив которого, мы получаем возможность редактировать его содержимое по своему усмотрению (там должен быть наш обратный адрес, вводящий спамера в заблуждение).

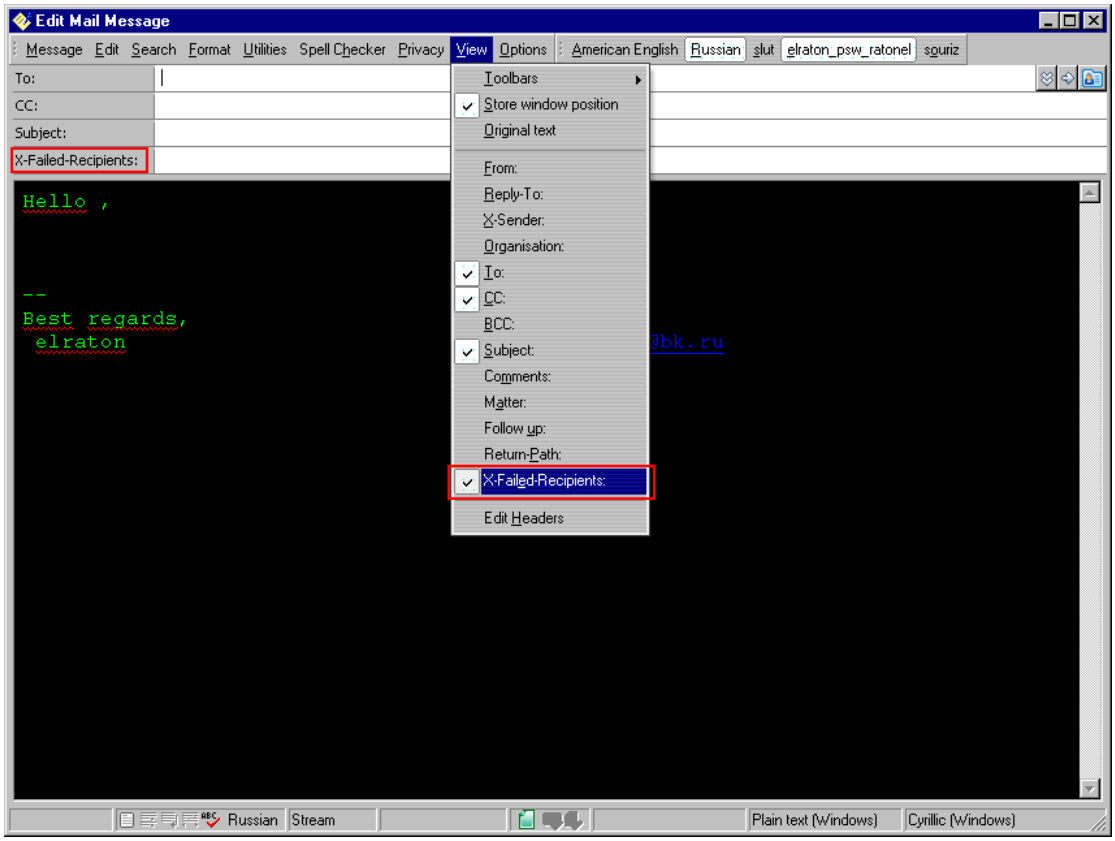

Рисунок 5 поле X-Failed-Recipients, появившееся в заголовке письма

Сам текст послания подделать нетрудно (достаточно скопировать его из листинга 1, где он выделен полужирным шрифтом, не забыв при этом заменить адрес putaaaaaaaaa@fastmail.jp на адрес своего почтового ящика), затем необходимо приложить **заголовок** оригинального спаммераского письма (в котором содержится его ID, помогающий спаммерскому роботу определить что именно отправлялось). Тело письма может в принципе и отсутствовать, но лучше для перестраховки присоединить и его.

Успешная подделка ответа mailer-daemon'a дает нам хорошие шансы на удаление адреса из спаммерской базы, но в случае провала поток рекламы только возрастет. Так что прежде, чем приступать к "работе", следует попрактиковаться на "кошках" — специально заведенных ящиках, "засвеченных" в спаммерских базах путем публикации адресов на популярных форумах и других сетевых ресурсах.

Необходимо только помнить, что ответ mailer-daemon'a должен приходить как можно быстрее, иначе у спаммера возникнут серьезные подозрения: а не пытаются ли провести его как лоха?! В этом отношении пословица "лучше поздно, чем никогда" уже не срабатывает и если спаммер не был торпедирован в течении нескольких часов с момента передачи (не получения!) письма, лучше вообще не пытаться его перехитрить.

правило N6: не сопротивляйтесь неизбежному

Как бы мы не извращались, попадание в спаммерские базы неизбежно (особенно при интенсивной переписке). Это всего лишь вопрос времени с течением которого поток нежелательной корреспонденции все возрастает и возрастает. Наконец, наступает момент, когда объем спама в несколько раз превышает полезную переписку, буквально теряющуюся на его фоне. Вариантов здесь всего два: либо продолжать терпеть это безобразие (ожесточая систему фильтрации пока она совсем не одичает и будет пожирать со спамом все подряд), либо сменить ящик, предварительно уведомив об этом каждого из своих респондентов, но… стоит только пойти по пути смены адресов, как куча людей не сможет вас найти, со всеми вытекающими отсюда последствиями. И если для домашней переписки это вполне терпимо (раз не нашли — значит так хотели найти), то в корпоративно-деловой среде одно-единственное неполученное письмо может стоить не только упущенной выгоды, но и потерянной карьеры.

Отсюда следует неутешительный вывод: электронная почта это, конечно, хорошо, дешево и удобно, но лучше вместе с майлом давать и номер телефона, который меняется гораздо реже, да и проблемами "кривых" спамморезок он не страдает.

Рисунок 6 результат деятельности агрессивно настроенной спаммеро-резалки