Технология спама

Мыльные игры

Электронная почта плотно вошла в нашу жизнь. Удобно, быстро и недорого. Но, как всегда, находятся люди, которые искренне надеются, что ее можно использовать для рекламирования себя или своих товаров. Эта статья посвящена тому, как это происходит и как с этим бороться.

Итак, для начала встанем на сторону спамера, чтобы понять механизмы возникновения спама в вашем почтовом ящике. Первая проблема — откуда взять почтовые адреса? Для начала — купить, благо в Интернете подобных объявлений полно. И неважно, что ваш личный адрес попал в базу «Промышленные предприятия России», у таких продавцов на первом месте стоит количество. Затем можно просто взять у нечистого на руку администратора какого-либо интернет-магазина или другого подобного сайта, для которого необходима регистрация по e-mail. Такие спам-листы обладают наибольшей ценностью, ведь целевая аудитория в них заранее известна, и адреса все рабочие.

Поиск адресов

И наконец, можно запустить специального робота, который будет ходить по страничкам и отфильтровывать все строчки с символами @, (at) и т. п. Такой робот пишется квалифицированным программистом за день. В дальнейшем результат работы этого робота преобразуется в спам-лист. К примеру, у нас есть новые супердухи, которые заставляют всех девушек обращать внимание на мужчин, и наоборот. Для пущей убедительности сделаем все руками:

- Заходим на ya.ru и вводим запрос «красота духи симпатичная». Это даст первичный отсев по категории.
- Ходим по выданным адресам страниц и выбираем e-mail (в данном примере я ис- »

пользовал возможности, предоставляемые любым Linux).

Шаг первый:

```
$ links -source http://www.krasota.ru/advert/|grep mailto: (выбираем все строчки, содержащие mailto:, из страницы)
В ответ получаем:
<a href=«<mailto:valex@krasota.ru>»>отдел рекламы портала «Красота-онлайн»</a>.
```

Шаг второй:

```
$ links -source http://antology.rchgi.spb.ru/autor_list.rus.htm|grep mailto: Руководитель проекта:<a href=«mailto:bourlaka@rchgi.spb.ru» class=«unnamed1»>E-Mail:bourlaka@rchgi.spb.ru</a><br>
Замечания:<a href=«mailto:webmaster@rchgi.spb.ru» class=«unnamed1»>E-Mail:webmaster@rchgi.spb.ru</a><br>
</font> <font face=«Arial, Helvetica, sans-serif» size=«1»><a href=«mailto:rector@rchgi.spb.ru%20»><span class=«unnamed1»>E-mail: rector@rchgi.spb.ru</span></a></font>
```

Улыбаемся и записываем получившиеся строки в файл, который будет «сырым спам-листом». Конечно, руками это делать тяжело и муторно, но простейший скрипт повыдергивает почтовые адреса со странички гораздо быстрее человека. Но, как видите, даже в случае ручной обработки времени уйдет гораздо меньше (получили четыре e-mail с двух адресов), чем просто выискивать и копировать адреса.

Отсев

На этом этапе обрабатываем «сырой спам-лист» до получения чистых e-mail. Здесь происходит замена адресов типа user(at)host.ru, user(sobaka)host.ru на нормальные user@host.ru.

Итак, у нас есть спам-лист. Следующая проблема — проверить реальность адресов. Конечно, можно и так разослать, но тогда нет никакой уверенности, что реклама дойдет до получателя.

Для этого пишется еще один робот, который будет соединяться с серверами получателей и узнавать у них, есть ли такие адреса (реальный домен host.ru не имеет отношения к нижеприведенному примеру):

```
$ telnet host.ru 25
Trying x.x.x.x...
Connected to host.ru
Escape character is '^]'.
220 host.ru ESMTP Postfix
vrfy multik@host.ru
252 multik@host.ru
vrfy user@host.ru
550 <user@host.ru>: User unknown
```

Как видите, сервер нам честно сообщил, что адрес multik@host.ru <mailto:multik@host.ru> существует, а user@host.ru <mailto:user@host.ru> — нет. Таким образом, у нас отсеиваются нерабочие адреса. Но на нормальных почтовых серверах команда VRFY отключена, там используется метод с неправильным mail-from с существующего домена и затем rcpt to.

И наконец, рассылаем по полученному спам-листу свою рекламу, к примеру, от имени президента США:

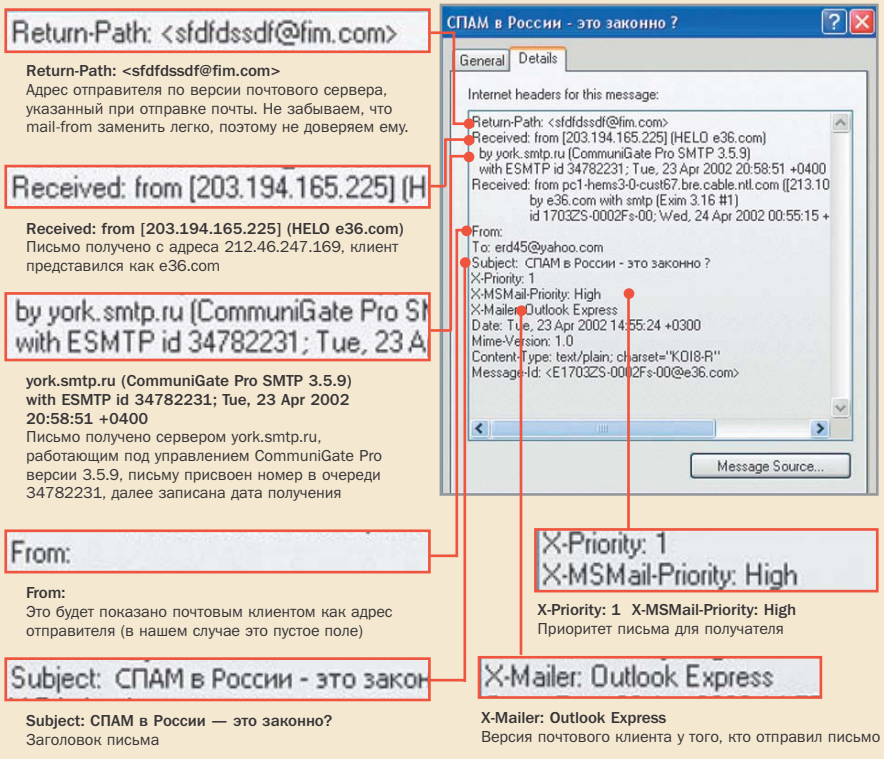
```
$ telnet host.ru 25
Trying x.x.x.x...
Connected to host.ru.
Escape character is '^]'.
220 host.ru ESMTP Postfix
mail from: president@whitehouse.gov
250 Ok
rcpt to: multik@host.ru
250 Ok
```

Анализ заголовка письма

Знание — сила

Если вы чувствуете в себе силы, то можете здорово упростить работу службе поддержки провайдера. Давайте попробуем сами разобраться, от кого могло прийти письмо со спамом. Для этого необходимо узнать, какими путями оно попало к вам.

Для начала надо просмотреть служебные заголовки письма (к примеру, пользователям Outlook достаточно щелкнуть по письму правой кнопкой мыши и выбрать «Параметры» — в поле «Заголовки Интернета» будет искомое. Порядок просмотра простой — самый последний сервер оставляет свои следы в самом верху заголовка. По скупости заголовков этого письма можно понять, что письмо отправлено напрямую от спамера, без использования промежуточных серверов. В данном случае надо выяснить, какому провайдеру принадлежит адрес 203.194.165.225 (с помощью команды nslookup или tracert). Если повезет, то вы узнаете, от какого провайдера писал письмо отправитель, и сможете обратиться с жалобой в службу технической поддержки.



Return-Path: <sfdfdssdf@fim.com>
Адрес отправителя по версии почтового сервера, указанный при отправке почты. Не забываем, что mail-from заменить легко, поэтому не доверяем ему.

Received: from [203.194.165.225] (HELO e36.com)
Письмо получено с адреса 212.46.247.169, клиент представился как e36.com

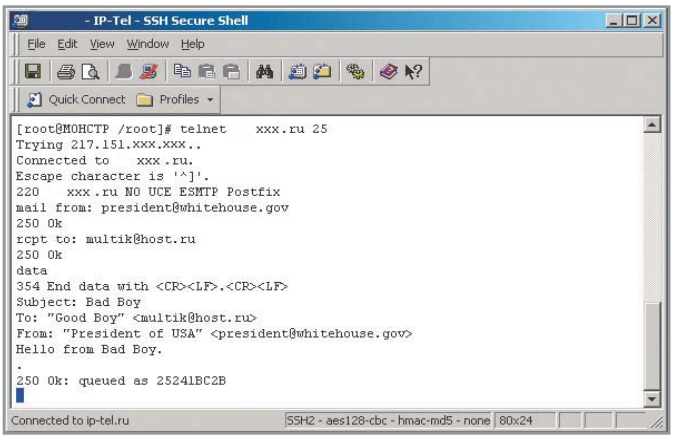
york.smtp.ru (CommuniGate Pro SMTP 3.5.9) with ESMTP id 34782231; Tue, 23 Apr 2002 20:58:51 +0400
Письмо получено сервером york.smtp.ru, работающим под управлением CommuniGate Pro версии 3.5.9, письму присвоен номер в очереди 34782231, далее записана дата получения

From:
Это будет показано почтовым клиентом как адрес отправителя (в нашем случае это пустое поле)

Subject: СПАМ в России — это законно?
Заголовок письма

X-Priority: 1 X-MSMail-Priority: High
Приоритет письма для получателя

X-Mailer: Outlook Express
Версия почтового клиента у того, кто отправил письмо



▲ Процесс отсылки подложного письма с помощью обычного telnet-клиента

▲ Такое письмо от американского президента получит наш пользователь

» Data
354 End data with <CR><LF>.<CR><LF>
Subject: Bad Boy
To: «Good Boy» <multik@host.ru>
From: «President of USA»
<president@whitehouse.gov>
Hello from Bad Boy.
.
250 Ok: queued as 9F452BC2B
quit
221 Bye
Connection closed by foreign host.

В итоге удивленный пользователь получит письмо, в котором он узнает, что плохой президент посылает ему привет, одновременно обзывая его хорошим парнем.

Как видим по вышеприведенному примеру, адрес отправителя подделать не составляет какого-либо труда. Так что выходит, никакая защита от спама невозможна?

Ссылки по теме

- **http://www.ezhe.ru/ses/list.html** — СпамЭпидемСтанция. База с большим количеством адресов людей, рассылающих спам.
- **http://spam.abuse.net** — сайт на английском языке, полностью посвященный проблемам спама.
- **http://www.cybernothing.org/faqs/net-abuse-faq.html** — хорошая подборка ответов на часто задаваемые вопросы по спаму (на англ. языке).
- **http://www.grandspam.com** — группа энтузиастов, предлагающих свои услуги по распространению спама.
- **http://www.antispam.ru** — все о спаме и том, как с ним бороться, по-русски.

Противостояние

К счастью, возможна. Сейчас мы рассмотрим методы борьбы с спамом со стороны обычного пользователя.

Для начала: никогда и нигде не оставляете свой e-mail. Если его надо указать для какой-нибудь регистрации, чтобы получить что-то, укажите что-нибудь типа email@domain.ru — в большинстве случаев этого достаточно. Если на этот e-mail должны прислать пароль или что-то подобное, то заведите ящик на бесплатном почтовом сервере только для этого случая. Получите пароль и забудьте про этот ящик.

Но вы все равно рано или поздно получите спам — ваш адрес попадет к спамерам, так как нет совершенства в этом мире. Ни в коем случае не отвечайте на него! Не верьте призывам в тексте письма, что послав письмо по такому-то адресу, вы отпишитесь. На самом деле вы просто подтвердите существование своего адреса.

Напишите жалобу провайдеру, от которого вы получили спам. Самое простое — это написать на адрес abuse@имя_вашего_провайдера письмо с жалобой, обязательно приложив оригинал спама. Далее специалисты сами разберутся, как спам попал к вам.

Только не предпринимайте каких-либо атак на этот адрес: в итоге вы сами для своего провайдера станете потенциальным кандидатом на отключение. Просто пишем письмо на адрес провайдера и прикладываем заголовки письма. Техническая служба, может быть, разберется с нарушителем и проведет воспитательные работы. А может, и не будет связываться — все зависит от конкретных людей. В среднем по статистике из 10 отправленных писем отвечают на одно-два.

В иных письмах служебных заголовков может быть огромное количество, поэтому будьте аккуратны — не пытайтесь проследить путь письма до самого отправителя. Если не уверены в своих силах — лучше отправьте письмо специалистам из технической службы вашего провайдера.

Но если вам лень искать заголовки или проявлять свою активность — воспользуйтесь пассивной защитой, предоставляемой любым современным почтовым клиентом. Ниже дан список правил, срабатывание которых должно приводить к удалению или перемещению писем куда подальше от глаз:

- Адрес отправителя и получателя совпадают или адрес получателя не ваш. Если письмо написали не вам — зачем его читать? В это правило автоматически попадают письма, где не указан получатель.
- В теле письма есть слова «друзья», «просим Вас извинить нас», «электронное пространство», «открытых источников», «Конституции», «разовое сообщение».

Этот небольшой, на первый взгляд, набор слов отсекает практически 99% всего спама. Если вы присмотритесь внимательно, то заметите, что в обычной переписке таких слов и выражений вы не употребляете. Конечно, список необходимо подкорректировать под ваши требования. Задачу облегчает и то, что интеллект у спамеров обычно небольшой: в итоге письма от них похожи друг на друга.

Итого

Вроде ничего сложного, а значит, сделать работу спамеров бесполезной в ваших силах. Если никто не будет читать спама, то сама идея спама будет дискредитирована...

Вячеслав Калошин