КАНАЛЫ И МЕХАНИЗМЫ РАСПРОСТРАНЕНИЯ СПАМ-СООБЩЕНИЙ

Бусыгин Сергей Евгеньевич

Московский технологический университет (119454, г. Москва, Проспект Вернадского, д.78) e-mail:rector@mirea.ru

Традиционным каналом, применительно к которому несанкционированные массовые сообщения называются термином «спам», является электронная почта. Самый большой спам-поток генерируется как раз через электронные почтовые серверы, превышая 70 % от общего трафика.

Реальные адреса электронной почты собираются либо вручную (крайне редкий случай), либо с использованием программных роботов, за час разыскивающих в сети тысячи и десятки тысяч e-mail[3]. Источниками информации в данном случае могут стать сайты знакомств, электронные доски бесплатных объявлений, социальны сети, форумы и чаты, сайты предприятий и прочие открытые данные. Иногда интернет-магазины и различные виртуальные сервисы при регистрации запрашивают электронный адрес, а затем сформированные базы идут на продажу. Базы данных электронных адресов становятся коммерческим продуктом, и некоторые компании сосредоточивают свою деятельность исключительно на этом.

Существует еще один способ сформировать базу данных, которая позволила бы организовать массовую спам-рассылку. При помощи программы генерируются случайные сочетания символов, которые могли бы теоретически быть электронным адресом. Затем специальная программа-валидатор проверяет каждую такую комбинацию, выявляя из полного списка те программы, которые реально существуют[1].

Ключевые слова: канал , механизм, спам

CHANNELS AND MECHANISMS OF SPAM SPEECH DISSEMINATION

Busygin Sergey Evgenyevich

Moscow University of Technology (119454, Moscow, Vernadsky Prospekt d.78) e-mail: rector@mirea.ru

The traditional channel for which unauthorized mass messages are called "spam" is e-mail. The largest spam stream is generated just through e-mail servers, exceeding 70% of the total traffic.

Real e-mail addresses are collected either manually (an extremely rare case), or using software robots that search for thousands of e-mails in the network in the course of an hour[3]. Sources of information in this case can be dating sites, e-boards free ads, social

networks, forums and chat rooms, business sites and other public data. Sometimes online stores and various virtual services ask for an e-mail address at registration, and then the formed databases go on sale. E-mail databases are becoming a commercial product, and some companies focus exclusively on this.

There is one more way to create a database, which would allow organizing mass spam mailing. The program generates random combinations of symbols that could theoretically be an electronic address. Then a special validator program checks each such combination, revealing from the full list those programs that actually exist[1].

The Key Words: channel, mechanism, spam

Традиционным каналом, применительно к которому несанкционированные массовые сообщения называются термином «спам», является электронная почта. Самый большой спам-поток генерируется как раз через электронные почтовые серверы, превышая 70 % от общего трафика.

Реальные адреса электронной почты собираются либо вручную (крайне редкий случай), либо с использованием программных роботов, за час разыскивающих в сети тысячи и десятки тысяч e-mail[3]. Источниками информации в данном случае могут стать сайты знакомств, электронные доски бесплатных объявлений, социальны сети, форумы и чаты, сайты предприятий и прочие открытые данные. Иногда интернет-магазины и различные виртуальные сервисы при регистрации запрашивают электронный адрес, а затем сформированные базы идут на продажу. Базы данных электронных адресов становятся коммерческим продуктом, и некоторые компании сосредоточивают свою деятельность исключительно на этом.

Существует еще один способ сформировать базу данных, которая позволила бы организовать массовую спам-рассылку. При помощи программы генерируются случайные сочетания символов, которые могли бы теоретически быть электронным адресом. Затем специальная программа-валидатор проверяет каждую такую комбинацию, выявляя из полного списка те программы, которые реально существуют[1].

В ряде случаев пользователь сам инициирует спам-атаку, оформляя электронную подписку (зачастую просто случайно или по незнанию кликнув на ссылку), либо не поставив галочку «по умолчанию» при регистрации на каком-либо ресурсе, либо заполняя анкету торгового предприятия или банка, и т.д.

Спам получает возможность распространения, если речь идет об имеющих выход в Интернет и не имеющих хорошей защиты персональных компьютеров. Случается также, что компьютер неправильно настроен.

Примерами могут послужить такие ситуации:

- Сервер ошибочно настроен таким образом, что стоит галочка, обозначающая разрешение свободно пересылать почтовые сообщения (например, open proxy).

- Webmail-серверы дают разрешение для доступа вообще без регистрации, или регистрация нового пользователя настолько примитивна, что ее могут пройти роботы.

- Поврежденные вредоносными вирусами или подвергшиеся хакерским атакам компьютеры, имеющие доступ в глобальную сеть, могут находиться без ведома владельца под внешним управлением и использоваться для различных целей, в том числе и для рассылки спама.

Существуют способы усложнить автоматически осуществляемую фильтрацию поступающего спама. Одним из них является сознательное искажение текста сообщения – например, использование похожих по написанию цифр и латинских букв вместо нормальных русских, произвольное добавление пробелов или пропуск их между словами, и другие подобные приемы[2].

Принципиально важным является определение того, получено ли сообщение адресатом, или как минимум определение того, реален ли данный электронный почтовый ящик. Для этого также используются разные приемы, например:

- запрашивается сообщение о доставке / прочтении (иногда в автоматическом режиме;

- предлагается отменить оформленную ранее подписку на данную спам-рассылку, отослав какое-либо сообщение на определенный адрес (обычно спам это не прекращает);

- предлагается перейти по ссылке, чтобы получить дополнительную информацию.

Получив такое подтверждение того факта, что электронный почтовый ящик используется, и письма с него читаются, спамеры обычно увеличивают в несколько раз количество посылаемых сообщений.

В интернете также немало полузаброшенных форумов, устаревших новостийных сайтов, с которых давно ушла большая часть пользователей. При этом новые сообщения содержат в основном рекламную информацию, даже если она выходит за рамки темы этого форума.

Каналом распространения спам-сообщений становятся и набравшие огромную популярность СМС-сервисы. Телефонные компании продают списки своих абонентов, и в результате они становятся объектами массовых рассылок[4].

Социальные сети, а также сайты знакомств располагают огромным объемом персональной информации, и их пользователи зачастую не видят особых проблем в том, чтобы разместить свои данные (электронный почтовый ящик, мобильный телефон) в открытом доступе. Кроме того, что эти каналы подвергаются спам-атакам, хакеры также могут взломать аккаунты для того, чтобы от чужого имени распространять рекламную информацию, отправлять и принимать приглашения в группы, рассылать в закрытые группы контент, содержащий рекламные сообщения.

Еще одна возможность использовать интернет-ресурсы для рассылки спама – это редактируемые и комментируемые форумы, блоги, вики. Как раз под предлогом комментирования или редактирования спамеры размещают там рекламу, которая получила отдельное название – сплог. Данный вид спама непросто удалить (для этого нужно как минимум связаться с модератором), поэтому он вызывает особенно негативную реакцию пользователей. Комментарии, по большому счету, используются спамерами для улучшения показателей посещаемости сайта (индексы за количество входящих ссылок).

Блоги иногда подвержены такому явлению, как френдоспам – когда чуть ли не в автоматическом режиме идет поиск пользователей и приглашение их без разбору в «друзья» только для того, чтобы увеличить собственный рейтинг и через журнал спамера привлечь внимание людей в массовом порядке к рекламному спам-сообщению.

Из-за обилия спама сейчас практически невозможным стало существование бесплатных досок объявлений без модерации. Спамеры могут разместить на одной электронной доске объявлений сотни спамовых сообщений во всех возможных разделах. При этом тексты спам-сообщений маскируются под обычное объявление коммерческого или полукоммерческого характера. Иногда каждое слово подобного объявления представляет из себя гиперссылку, что создает определенные трудности для пользователей электронной доски объявлений. Спамеры даже на модерируемых сайтах данного уровня часто могут воспользоваться элементарной невнимательностью, так как объявлений ежесуточно поступает очень много.

Поисковый спам — страницы и web-сайты, созданные с целью манипулирования результатами в выдаче поисковых систем, например, дорвеи —

страницы с ключевыми словами и автоматическим перенаправлением на «нужный» сайт.

За последние годы алгоритмы поисковых систем стали намного сложнее и лучше в плане борьбы с поисковым спамом.

Когда-то давно спам рассылали по локальной сети через встроенную в Microsoft Windows SMB-службу Messenger. Такие сообщения появляются в виде всплывающих окон (если не установлено стороннего ПО, обрабатывающего их по-другому)[5].

В этом случае для отключения их приёма можно, например, остановить службу Messenger командой net stop messenger. В версиях Windows NT, начиная с Windows XP SP2, эта служба уже остановлена по умолчанию, поэтому данный способ рассылки встречается всё реже. Соединения извне на порты SMB закрыты с начала 2000-х после массового распространения SMB-червей.

Спам может распространяться не только через Интернет. Рекламные сообщения, присылаемые на мобильные телефоны с помощью SMS-сообщений, особенно неприятны тем, что от них труднее защититься.

Во многих странах введены законодательные ограничения на рассылки рекламных SMS сообщений людям, не давшим своё явное согласие на это.

Телефонные номера для рассылок спама могут получать как полузаконными путями (из сервисов, сайтов, магазинов и прочих, где человек оставил свой телефонный номер), так и незаконным путём.

СПИСОК ЛИТЕРАТУРЫ

1. **Дерешко Б.Ю. Развитие дистанционного обучения на базе новых инфотехнологий / Дерешко Б.Ю., Лукьянов С.П. // Дистанционное и виртуальное обучение. - 2014. - № 1. - С. 17-27.**
2. **Еляков А. Д. Проблемы человека в условиях современной информационной среды // Науч.-техн. информ. Сер. 1, Орг. и метод. информ. раб. — 2015. — № 4. — С. 1-10.**
3. **Матвиенко В.В. Безопасность личности в условиях информатизации общества // Актуальные проблемы гуманитар. и естественных наук. – 2012. - № 10. – С. 287-294.**
4. **Музурова З.М. Сущность и классификация электронных образовательных ресурсов. // Мир науки, культуры и образования. – 2015. - № 2 (51). – С. 221-225.**

5. **Петраков А.В. Основы практической защиты информации. Учебное пособие. - М., 2015.- 281 с.**