УДК 004.056.57

МЕТОДЫ РАССЫЛКИ И СПОСОБЫ БОРЬБЫ С НЕЖЕЛАТЕЛЬНОЙ КОРРЕСПОНДЕНЦИЕЙ (СПАМОМ)

Кресан Е.А.
Научный руководитель — к.ф.-м.н. Кучеров М.М.
Сибирский федеральный университет

Последние несколько лет Россия стабильно входит в пятерку стран-лидеров по рассылке спам-сообщений. Что же этому способствует, и какие технологии применяются современными спаммерами для рассылки нежелательной корреспонденции?

Для начала определимся, что же считается спамом. Согласно определению «Лаборатории Касперского», спам — это анонимная, массовая, незапрошенная рассылка.

Анонимная - все страдают, в основном, именно от автоматических рассылок со скрытым или фальсифицированным обратным адресом.

Массовая - эти рассылки именно массовые, и только они являются настоящим бизнесом для спаммеров и настоящей проблемой для пользователей.

Незапрошенная - подписные рассылки и конференции не должны подпадать под определение (хотя условие анонимности и так в значительной мере это гарантирует).

Новая редакция закона "О рекламе" требует предварительного согласия получателя на отправку рекламных писем. Однако, по мнению экспертов, вступление закона в силу не повлияло на ситуацию со спамом в России.

Вступившая в действие 1 июля 2006 г. редакция российского закона «О рекламе» закрепила принцип «Opt-in». Это значит, что распространять рекламу по сетям электросвязи можно только при наличии предварительного согласия получателя. Ранее действовал принцип «Opt-out», в соответствии с которым, получатель имел право только отписаться от нежелательных сообщений.

Однако отраслевые эксперты считают, что обновленный закон не повлиял на ситуацию со спамом. Доля спама в Рунете несколько снизилась сразу после вступления в силу закона «О рекламе» (возможно, заказчики спама ожидали первых результатов вступления в силу поправок к закону), но затем вновь начала расти, и с того времени спам составляет примерно 80% почтового трафика Рунета.

Проблема заключается еще и в том, что, в отличие от западных стран, спам в России многими рекламодателями до сих пор не воспринимается как «нереспектабельный» вид рекламы.

Обращаясь к мировому опыту, можно отметить, что, к сожалению, законы против спама пока что не показали серьёзной действенности. Так в США количество спама остаётся весьма большим, несмотря на отдельные успешные судебные процессы против спамеров. В частности, спамеры активно используют компьютеры за пределами США, чтобы избежать попадания под действие закона.

Но эффективные законы против спама — необходимая составляющая борьбы с ним. Однако специалисты подчеркивают, что наличие в одной стране даже совершенных антиспамовых законов не решит данную проблему, которая носит международный характер.

К основным технологиям рассылки нежелательной корреспонденции, которые применялись ранее и применяются по сей день, можно отнести:

- прямые рассылки. Спам начинался с прямых рассылок — спамеры рассылали сообщения от собственного имени с собственных почтовых серверов. Такой спам блокируется достаточно просто (по адресу почтового сервера или адресу отправителя). Как только такие блокировки стали распространенными, спамеры

были вынуждены начать подделывать адреса отправителей и другую техническую информацию.

- Рассылки через «открытые релеи». Открытый релей (open relay) — это почтовый сервер, который позволяет произвольному пользователю отправить произвольное электронное письмо на произвольный адрес. В середине 90-х годов все почтовые серверы представляли собой открытые релеи, поэтому понадобилось изменять и перенастраивать программное обеспечение на всех почтовых серверах мира. На сегодняшний день этот метод рассылки все еще применяется, т. к. открытые релеи до сих пор существуют.
- Рассылки с модемных пулов. Как только рассылки через открытые релеи перестали быть эффективными, спамеры стали применять рассылку с dialup-подключений. Как правило, почтовый сервер провайдера принимает почту от своих клиентов и пересылает ее дальше. Dialup-подключение получает динамический IP-адрес, таким образом, спамер может рассылать почту со множества IP-адресов. В качестве ответной меры, провайдеры стали вводить лимиты на число писем, посланных от одного пользователя, появились черные списки dialup-адресов и блокировка приема почты с «чужих» модемных пулов.
- Рассылки с proxy-серверов. В начале 2000-х, годов одновременно с распространением высокоскоростных подключений (ADSL, Cable), спамеры стали использовать уязвимости в клиентском оборудовании. Многие ADSL-модемы имели встроенный SOCKS-сервер или HTTP proxy. Доступ к ним был доступен со всего мира без паролей и контроля доступа. Таким образом, можно было произвести любое действие (в том числе и рассылку спама) с IP-адреса ADSL-пользователя.
- Взлом пользовательских машин. В настоящее время основная масса рассылок производится с пользовательских компьютеров, на которые тем или иным способом установлено «троянское» программное обеспечение, позволяющее спамерам осуществлять доступ к пользовательским машинам без ведома и контроля пользователя. Для взлома пользовательских машин используются следующие методы:

- троянские программы, распространяемые вместе с пиратским ПО по файлообменным сетям;
- использование уязвимостей в различных версиях Windows и широко распространенного ПО для установки бэкдоров на пользовательских компьютерах;
- email-черви последних поколений, также используемые для установки бэкдоров.

По самым скромным оценкам троянские программы установлены на нескольких миллионах машин по всему миру. По данным компании Return Path, 96,7% компьютеров, с которых рассылается электронная почта, контролируются спамерами, т.е. входят в так называемые зомби-сети.

Итак, ни один из существующих методов борьбы со спамом (включая и технические и законодательные варианты) пока что не приблизился к решению проблемы. Однозначного решения проблемы спама не существует. Пока массовые рассылки обеспечивают прибыли, спамеры будут находить слабые места в любых методах защиты, а ужесточение этих методов будет иметь неминуемые побочные эффекты.

Сочетая различные методы борьбы со спамом, возможно добиться некоего оптимального соотношения между фильтруемым спамом и вероятностью потери доброкачественных писем. Однако стоит помнить, что потеря, пусть даже и одного, но очень важного письма, в конечном итоге, может свести на нет все усилия по противодействию спам-атакам.