программы различных типов, обеспечивающие эффективную защиту исключительно только против известных мониторинговых программ с помощью сигнатурного анализа. Примеры таких программ – eTrust PestPatrol, Anti-SpyWare (компания Computer Associates) Ad-aware (Lavasoft), расширенные базы антивируса Лаборатории Касперского, Microsoft Anti-SpyWare и другие [4].

Выводы

В статье были приведены результаты анализа наиболее часто встречающихся программ типов spyware. Основные результаты анализа можно изложить в следующем:

- Spyware - программное обеспечение, которое собирает информацию о пользователе, как правило без его ведома или согласия, и затем передает эти данные другим лицам;
- к классу «spyware» можно отнести целое семейство программ, в которое входят: программы дозвона, утилиты для закачивания файлов из интернета, различные серверы (FTP, Proxy, Web, Telnet), IRC-клиенты, средства мониторинга, PSW-утилиты, средства удаленного администрирования, программы-шутки;
- к основным методам борьбы со шпионским программным обеспечением можно отнести установку на компьютере антивирусов, брандмауэров, мониторинговых программ и настройку операционной системы.

Список литературы

1. «Шпионскими программами заражены 90 процентов компьютеров», http://anti-malware.ru/index.phtml?part=news1&newsid=112&arc=1
2. «Spyware — потенциально опасные программы», Алексей Доля, http://www.viruslist.com/ru/analysis?pubid=164453811
3. «Шпионские войны: spyware и борьба с ним», Родион Насакин, http://anti-malware.ru/index.phtml?part=survey&surid=spyware
4. http://www.vnunet.com/vnunet/specials/2127675/spyware.

Надійшла 17.12.2007р.

УДК 004.681.3

Чернышев А. Н.

ОБЗОР СОВРЕМЕННЫХ «СПАМ» ТЕХНОЛОГИЙ. МЕТОДЫ ФИЛЬТРАЦИИ СПАМА

Термин "спам", как анонимная массовая не запрошенная рассылка электронных сообщений адресату, стало для пользователей электронной почты привычным и повседневным. Как правило, с помощью спама продают товары и услуги мелкие фирмы, которые не имеют возможности прибегнуть к более традиционным (и более дорогостоящим) рекламным каналам.

С точки зрения теории коммуникации, спам, это средство влияния на поведение людей, его получающих. Обычно спам направлен на побуждение получателей приобрести какие-либо товары и услуги непосредственно у заказчика спама. Однако заказчик может извлечь выгоду и косвенным способом – призывая покупать или продавать акции, обращающиеся на внебиржевом рынке в электронных торговых системах (так называемый "инвестиционным спамом").

Кроме спама и целевых коммерческих предложений существует еще один вид почтовых сообщений, который часто путают со спамом. Это нежелательная почта. В некоторых случаях не запрошенное и ненужное сообщение спамом не является. Наиболее частыми примерами нежелательной почты являются: разного рода отчеты об ошибках (ошибки автоматических рассыльщиков); различная техническая корреспонденция (сообщения о недоставке письма); новые возможности общения и бизнеса (деловое письмо о новом сотрудничестве); личные письма от тех, с кем получатель никогда ранее не

переписывался.

Любое из этих писем является незапрошенным, ибо принимающая сторона его явно не запрашивала. С другой стороны, выбрасывать подобную почту без прочтения нельзя. Из этого следует, что признаки массовости и анонимности являются необходимыми для распознавания тех, кто делает бизнес на спаме.

Согласно постоянно проводимым онлайн-опросам, в прошедшем году более половины участников производили покупку товаров и/или услуг после прочтения нелегитимного рекламного письма.

Так же более половины респондентов признались, что не могут побороть искушение и каждый день проверяют содержимое спам-карантина. 16% опрошенных совершали покупки, воспользовавшись найденной в спам-карантине информацией.

Результаты опроса, в котором приняло участие 7500 пользователей (79,4% респондентов - женщины), подтвердили мнение специалистов по рекламе и маркетингу о том, что лучшей мотивацией для совершения покупки является привлекательность и клиент-центричность предложения, 40% опрошенных приняли решение совершить покупку, посчитав предложение выгодным, четверть участников опроса были заинтересованы в приобретении рекламируемых товаров и услуг.

Согласно итогам опроса, немаловажную роль в принятии решения о покупке играло также указанное рекламодателями известное имя или бренд. 47% респондентов признались, что были просто привлечены удачным заголовком нелегитимного письма.

Доля спама в почтовом трафике составляет в среднем 85%. Наиболее популярными тематиками спама являются: рубрики «Медикаменты; другие товары и услуги для здоровья» (30%), «Другие товары и услуги» (8%), «Образование» (10%), также постоянно увеличивается относительное количество рассылок, рекламирующих юридические услуги (7%) и посвященных операциям с недвижимостью (4%) (рис.1).

No	Тематика	Описание	Доля тематики
1	Медикаменты; товары/услуги для здоровья	Предложения приобрести лекарственные препараты, БАДы и т.п. в online. Предложения медицинских и оздоровительных услуг, а также сопутствующих товаров.	30%
2	Другие товары и услуги	Предложения других товаров и услуг	8%
3	Образование	Реклама семинаров, тренингов, курсов	7%
4	Отдых и путешествия	Предложения туристических поездок, а также организации и проведения различных развлекательных мероприятий.	4%
5	Юридические услуги и аудит	Предложения юридических услуг	7%

Рис 1. Популярные тематики в сети

Большая часть «юридического» спама предлагает услуги по регистрации и ликвидации предприятий, оформлению разрешений на работу и получению виз. Предложения по

недвижимости также стандартны — главным образом это продажа и сдача в аренду офисных помещений и складов, продажа земли и жилых коттеджей.

Приведенная статистика показывает, что рассылка спама приобретает все большие масштабы – что в свою очередь требует со стороны спамеров существенных вложений в развитие технологий рассылок.

Технологическая цепочка спамеров выглядит таким образом:

1. Сбор и верификация E-mail-адресов получателей. Классификация адресов по типам.
2. Подготовка "точек рассылки"- компьютеров, через которые будет рассылаться спам.
3. Создание программного обеспечения для рассылки.
4. Поиск клиентов.
5. Создание рекламных объявлений для конкретной рассылки.
6. Произведение рассылки.

Все основные технологические составляющие бизнеса спамеров могут быть использованы независимо. Как следствие, в настоящее время существуют отдельные "производители" вирусов и троянских компонент, отдельные авторы программ для рассылки, отдельные сборщики адресов. Спамеры - а именно те, кто собирает с клиентов деньги и производит рассылку - могут просто арендовать необходимые им сервисы, покупать базы данных, списки рассылающих машин и использовать их.

В то же время, очевидно разделение рынка на профессионалов (которые, как правило, обладают чем-то своим: базой данных адресов или программой для рассылки или собственным вирусом), для которых спам является основным источником дохода, и любителей, пытающихся заработать чуть-чуть денег.

Среди множества хитроумных трюков, применяемых спамерами, особое внимание привлекают NDR-атаки, поскольку они основаны на фундаментальных спецификациях, описывающих работу протокола SMTP (Simple Mail Transfer Protocol – простой протокол доставки почты) – основной протокол, прямых конкурентов у которого нет и, по-видимому, уже не будет.

Свое название NDR-атаки получили по первым буквам выражения Non-Delivery Report (отчет о недоставке почты). Всякий раз, когда SMTP-сервер не может доставить письмо (скажем, по причине отсутствия указанного адреса), он возвращает сообщение об ошибке с кодом 5xx, которое может выглядеть, например, так: «550 5.7.1 Unable to relay for mail@mail.ru», после чего разрывает TCP/IP-соединение. Однако сервер может и принять сообщение, отложить его в очередь, оповещая отправителя положительным кодом завершения операции (250).

Когда же в процессе обработки письма выяснится, что доставлять его некому, сервер, как правило, возвращает письмо адресату с объяснением причины невозможности доставки. Вот это самое уведомление и называется Non-Delivery Report, или сокращенно NDR. Теоретически формат отчета специфицирован в RFC-3464 (An Extensible Message Format for Delivery Status Notifications — Открытый формат сообщений, уведомляющих о статусе доставки), однако в реальной жизни он варьируется в весьма широких пределах. Одни серверы помещают исходную копию письма во вложение, а сам отчет кладут в основное тело сообщения. Другие же в целях экономии трафика отправляют только отчет, добавляя к нему короткий фрагмент исходного письма, включающий как минимум заголовок и несколько первых строк (чтобы отправитель мог разобраться, какое именно письмо «пострадало»).

В общем, уведомления о недоставке - стандартная и внешне вполне безобидная настройка сервера. Однако с ней связано целых две атаки: использование SMTP-сервера в качестве proxy (bounce message или backscatter-attack) и поиск валидных адресов (trial-n-error attack).

Термин backscatter перекочевал в компьютерную среду из физики, где он означает отклонение волн от исходной траектории по тем или иным причинам (например, рэлеевское рассеяние света на молекулах воздуха). Применительно к SMTP-серверам backscatter «символизирует» процесс отскока или отбивания посланного сообщения. Такая атака также часто называется bounce message attack.

Один из крупнейших дефектов SMTP-протокола заключается в отсутствии штатных механизмов проверки аутентичности обратного адреса отправителя сообщения. Сервер всецело полагается на адрес, оставленный отправителем в поле «MAIL FROM:», не делая никаких попыток его проверки, а потому злоумышленник может запросто подставить любой адрес, какой ему вздумается, и именно туда сервер возвратит сообщение при невозможности его доставки конечному получателю. Пользуясь этим, злоумышленник берет адрес жертвы, прописывает его в поле «MAIL FROM:», а в поле «RCPT TO:» подставляет координаты заведомо несуществующего получателя. Если сервер не является ретранслятором (также называемым релеем — от английского relay), то есть берется за доставку корреспонденции лишь своим локальным адресатам, то он с вероятностью, близкой к единице, отобьет сообщение еще на стадии заполнения поля «RCPT TO:» и атака не состоится. Впрочем, некоторые серверы, в частности Microsoft Exchange Server, имеют сложную систему поиска имен и зачастую принимают сообщения до проверки пользователя на существование.

Что же касается ретрансляторов (к которым принадлежат все публичные серверы, такие, например, как mail.ru), то они вообще не в состоянии определить существование нелокальных пользователей и потому принимают все письма без разбора. Лишь потом, в случае невозможности доставки, они посылают отправителю (или, точнее говоря, тому лицу, чей адрес указан в поле «MAIL FROM:») соответствующее уведомление.

Рассылка уведомлений по множественным адресам запрещена, и потому атакующему для отправки N писем размером в K мегабайт придется израсходовать N*K мегабайт своего трафика. А это ровно столько, сколько тратится при так называемой директивной рассылке, когда атакующий вообще не прибегает к услугам промежуточных SMTP-серверов, а связывается с каждым получателем напрямую и кладет в его почтовый ящик конверт со спамом. Поэтому спамеры и стремятся использовать открытые ретрансляторы, допускающие задание в поле «MAIL TO:» множества адресатов. В идеале (если количество адресов неограниченно) атакующий тратит лишь K мегабайт собственного трафика, остальные же почтовый сервер оплачивает из за свой счет. Однако с каждым днем находить открытые ретрансляторы становится все труднее и труднее. Практически все почтовые серверы устанавливают жесткие лимиты на максимальное количество сообщений, передаваемых в единицу времени, и либо вообще запрещают множественную рассылку, либо соглашаются доставлять письмо ограниченному числу получателей.

С другой стороны можно заменить открытые ретрансляторы современными широкими DSL-каналами, в которых исходящий трафик либо совсем бесплатный, либо тарифицируется по весьма льготным ценам, но существует ряд ограничений. При практической реализации атаки большинство корпоративных (да и публичных) серверов попросту не примут письмо неизвестно от кого. Поэтому как минимум потребуется зарегистрировать доменное имя третьего уровня и настроить собственный почтовый сервер. А для этого уже желательно иметь статический IP, хотя доменное имя третьего уровня можно бесплатно зарегистрировать и на динамическом.

В результате настройки собственного почтового сервера мы добились того, что почтовые серверы начинают принимать от нас корреспонденцию. Но стоит только начать рассылать спам, как уже через несколько часов атака потухнет. Используя распределенные черные списки (они же блэк-листы), почтовые серверы очень быстро заблокируют наш IP-адрес (а то и всю подсеть). В случае статического адреса это еще ничего, а вот блокировка динамического IP (или всей подсети) создает огромные проблемы для провайдера, который тут же отключает спамера.

Следовательно, директивная рассылка оправдывает себя только на ботнетах — сетях из зараженных злоумышленником персональных машин ретранслирующих почтовые сообщения в сети. Но в отличие от спама (юридический статус которого до сих пор не определен), создание бот сетей это уже является довольно серьезным правонарушением, особенно если в число зараженных узлов попадут компьютеры различных секретных ведомств.

Более эффективными являются backscatter-атаки. Злоумышленник, используя различные SMTP-серверы, рассылает корреспонденцию, подставляя адрес получателя в поле «MAIL FROM:» и указывая заведомо несуществующего пользователя в поле «RCPT TO:». Несмотря на то, что подлинный IP-адрес спамера остается в заголовке письма (помещаемого сервером во вложение или в основное тело сообщения), существующие фильтры не настолько интеллектуальны, чтобы достать его оттуда, и потому заносят в черный список IP почтового сервера, рассылающего уведомления о невозможности доставки сообщений. Данным условиям отвечает практически любой SMTP-сервер, даже не являющийся ретранслятором.

Так как спамеры заинтересованы в отправке сообщений только на действующие адреса, то уведомления о недоставке тут приходятся как нельзя кстати. В частности, ошибка типа «mailbox is full» говорит, что получатель, скорее всего, не пользуется данным ящиком и потому он заполнен до предела. Одной из основных проблем спамеров является— сбор адресов. Для их поиска разрабатываются различные программы-харвестеры (от английского harvester — «собиратель»), блуждающие по Сети и анализирующие web-странички, а также проникающие на уязвимые узлы и сканирующие адресную книгу. Применяется так же метод перебора по словарю, основанный на склонности пользователей выбирать короткие и легко запоминающиеся адреса, как правило, состоящие из имени (с добавленным к нему годом, когда такое имя уже кем-то занято), популярных слов или инициалов. Атакующий просто отправляет большое количество писем, перебирая различные буквенно-цифровые комбинации, и ловит NDR-уведомления от почтового сервера. Несуществующие адреса отметаются сразу, а вот на остальные направляется поток незапрошенной корреспонденции. Для экономии трафика тело тестового письма обычно содержит минимум символов и зачастую просто состоит из нескольких байт. Одно-, двух- и трехсимвольные комбинации представлены на популярных почтовых серверах достаточно полно и покрывают около двух десятков тысяч действующих адресов, короткие имена намного медленнее устаревают, поскольку их владельцам жалко с ними расставаться. Четырехсимвольные имена перебирать труднее, поскольку из двух миллионов комбинаций, реально используется не более сотни тысяч адресов. Для пятисимвольных имен применение метода перебора не целесообразно. Еще один метод выявления адресов - перебор по словарю. Данный метод становится возможным благодаря различным система раздачи адресов в корпорациях (например по имени и/или фамилии сотрудников).

Обзор основных методов борьбы со спамом

Защиту от спамерских атак условно можно разделить на два уровня: защита на уровне администратора сети и защита на уровне пользователя.

Рассмотрим методы применяемые администраторами.

Основной вред от спама на уровне почтового сервера - увеличение входящего трафика и значительная трата времени. Следуя из этого средства борьбы со спамом, можно разделить на две категории: ориентированные на снижение трафика и ставящие своей первоочередной задачей снижение нагрузки на конечного получателя.

Решение задачи снижение трафика

Один из наиболее простых методов - непосредственный запрет на прием почты с IP-адресов, замеченных в рассылке спама. Ранее данная операция реализовалась вручную. Администратор, обнаружив у себя нежелательную рассылку, пытался убедить владельца соответствующей сети прекратить рассылку, если это не помогало, то IP-адрес отправителя помечался в файле access почтового сервера как REJECT.

В наши дни ручная борьба совершенно бесполезна. Но access-файл тоже помогает только в редких случаях. Когда администратор точно знает все серверы, с которых должна приходить нужная почта, вся остальная корреспонденция отбрасывается без промедления.

Дальнейшим развитием этой идеи стали черные списки - когда неблагонадежные IP-адреса целенаправленно собираются специальными компаниями или сообществами пользователей и предоставляются остальным. Поскольку такие списки довольно динамичны (в них постоянно кого-то добавляют, а кого-то исключают), то наиболее простым способом их распространения явилась система DNS.

Суть блокировки по черным спискам на основе DNS довольно проста - на сервере (например, spamcop.net) устанавливается DNS-сервер, который хранит у себя не традиционные зоны, а информацию по спамерским IP-адресам. Запросив у такого сервера поиск по специальному адресу, включающему IP отправителя, и получив положительный ответ, администратор делает вывод, что адрес засвечен как спамерский. В современных почтовых серверах существуют настройки по работе с такими черными списками.

Одним из недостатков DNSBL является их неразборчивость: убивать, так все. Однако случаются ситуации, когда через сервер крупного провайдера передаются и официальная почта крупного банка, и рекламные рассылки спама, подключенного по ADSL. Занести адрес такого сервера в черный список - значит лишить серьезных пользователей услуги электронной почты, а если не заносить, тысячи пользователей будут страдать от спама.

При настройке защиты от атак на SMTP-серверы, в отчет о недоставке следует включать только фрагмент исходного сообщения (заголовок плюс пару строк), что сделает его совершенно бесполезным для спамеров. Если же это невозможно (например, сервер не поддерживает таких настроек), задействуй режим замедления SMTP-ответов, установив задержку в несколько секунд для неавторизованных пользователей.

Решение задачи снижение нагрузки на конечного получателя

Спам, несомненно, нужно фильтровать, а затем сохранять в особых папках или помещать в карантин, а иногда сразу удалять — согласно политике обслуживаемой организации. Письма, относящиеся к категориям целевых коммерческих предложений и нежелательной почты так же возможно распознавать и фильтровать, но с ними нужно обращаться более осторожно. В компании могут быть разные отделы, которые хотели бы получать различные категории непрошеной почты (администраторам нужны сообщения от сервисов и антивирусов, кадровикам — приглашения на семинары).

Таким образом, системный администратор должен вводить тщательно продуманную политику обработки почты, включающую не только уничтожение спама, но маршрутизацию и хранение незапрошенной и даже нежелательной почты.

Создавая списки пользователей на сервере, следует избегать коротких логинов (2-3 символа) которые могут быть найдены методом тривиального подбора. Формировать имена необходимо из длинных комбинаций — свыше пяти-шести символов — состоящие из одних согласных букв, цифр и спецсимволов.

Так же рекомендуется генерировать сообщение о недоставке в ответ на все подозрительные сообщения и даже на все сообщения с неизвестным адресатом (то есть таким адресатом, которому получатель сообщения ранее не отправлял никакой корреспонденции). Практика показывает, что честные пользователи сразу (или через некоторое время) повторяют попытку отправки вновь, в то время как спамеры тут же заносят такой адрес в список несуществующих. Поскольку спамеры анализируют уведомления о недоставке не вручную, а с помощью программ, выдирающих из тела письма код ошибки, то имеет смысл добавить в уведомление русский текст, предлагающий пользователю отправить сообщение еще раз.

На уровне пользователя, задача защиты от спама сводится к установке анти спам программ и обучении их фильтров. Популярны как программы встроенные в почтовые клиенты так и самостоятельные анти спам приложения, такие как: McAfee Secure Messaging Service for Enterprise - автоматически защищает почтовые системы от угроз таких, как спам,

фишинг, вирусы и т.д.; Agava Spamprotexx - интеллектуальный спам-фильтр которой работает быстро, эффективно и максимально лёгок в использовании.

Выводы

Во времена разработки базовых почтовых протоколов первоочередной задачей была передача почтовых сообщений, а не защита от злоумышленников, конечно протоколы постепенно дорабатываются, появляются новые механизмы аутентификации, однако в силу децентрализованной природы интернета их внедрение требует времени.

Почта каждого человека очень индивидуальна и зависит от области интересов, деятельности и т.д. Что считать спамом или не-спамом — решает только конкретный пользователь. Системный администратор, в свою очередь, должен вести тщательно продуманную политику обработки почты, включающую не только уничтожение спама, но маршрутизацию и хранение незапрошенной и даже нежелательной почты.

УДК 004.681

Сєрєнко В.Є.

ВИЗНАЧЕННЯ ІНФОРМАЦІЇ, ЩО ПІДЛЯГАЄ ЗАХИСТУ – ПЕРШИЙ ЕТАП ПРИ ПОБУДОВІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Вступ

Захист інформації на підприємстві починається з визначення самої інформації, втрата, порушення цілісності або доступності якої можуть призвести до непередбачених фінансових витрат та завдати маральної чи фізичної шкоди.

Організацією процесу визначення інформації на підприємстві повинен займатися підрозділ, на якого покладено функції з адміністрування процесами управління підприємством, та який має організаційно-розпорядчий вплив на всі структурні підрозділи підприємства (як приклад служба забезпечення діяльності керівника підприємства).

Вихідними даними даного етапу є аналітична інформація про інформаційну систему підприємства, що використовується підрозділом захисту інформації підприємства у подальшому, при створенні комплексної системи захисту інформації.

Класифікатор інформації

Основним організаційним документом, який регулює діяльність підприємства у сфері інформаційних відносин є класифікатор інформації.

Класифікатор інформації – це офіційний документ, який в загальних рисах описує інформаційну систему підприємства.

Формують класифікатор інформації структурні підрозділи підприємства, спираючись на положення про підрозділи (функціональні обов'язки підрозділу).

Формування класифікатору проходить в три етапи (як приклад рис. 1):

- на першому етапі структурні підрозділи підприємства подають відомості до класифікатору стосовно інформації, яку вони використовують при виконанні своїх функціональних обов'язків. При цьому вказані структурні підрозділи визначаються як *користувачі* поданої інформації;
- на другому етапі структурні підрозділи подають відомості до класифікатору стосовно інформації, яку вони отримують на виході при виконанні своїх функціональних обов'язків. При цьому вказані структурні підрозділи визначаються як *джерела* поданої інформації;
-