Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 9 (136)/2004

БОРЬБА СО СПАМОМ

КОРПОРАТИВНЫЕ СИСТЕМЫ

БОРЬБА СО СПАМОМ

Олег Слепов
компания "Инфосистемы Джет"
консультант по информационной безопасности

СОДЕРЖАНИЕ

Вступление

В последние годы специалисты в области информационной безопасности начали заниматься, казалось бы, несвойственной им задачей: бороться со спамом — массовыми рассылками, которые в большинстве своем носят рекламный характер. А происходит это потому, что такие рассылки наносят серьезный ущерб информационным системам. Автор данной статьи ставит своей целью раскрыть суть явления и предлагает на рассмотрение подход к решению данной проблемы, который может быть применим в локальных вычислительных системах организаций и предприятий вне зависимости от их размеров и сфер деятельности.

Распространение спама приобрело в последние годы угрожающие масштабы. С начала 2004 года рост количества спама превзошел все, даже самые пессимистичные, прогнозы, дававшиеся в конце прошлого года. Если по оценкам специалистов в конце 2002 года спам составлял 30-40% от общего числа электронных писем в мире, то уже в 2003 году доля спама превысила отметку 50%. По сведениям ведущих провайдеров России, на начало 2004 года спам составляет около 75-80% всей входящей корреспонденции в публичных почтовых службах Рунета.

Убытки от спама, на первый взгляд незначительные для отдельного пользователя, в масштабах всей индустрии и даже отдельной крупной компании выглядят впечатляюще. По разным оценкам, на спаме компании теряют от $50 до $200 в год в расчете на одного офисного сотрудника. В результате в 2003 году ущерб от спама по порядку величины стал сравним с потерями, которые нанесли мировому сообществу компьютерные вирусы и хакеры. По данным из европейских источников, ущерб от спама во всем мире составляет $10 миллиардов ежегодно. В России этот ущерб оценивается в $200-250 миллионов.

Массовые рассылки рекламного характера получили свое название от английского слова Spam (далее - спам), которое в настоящее время известно практически всем пользователям Интернета. Оно ведет свое происхождение от старого скетча английской комик-группы Monty Python Flying Circus, музыканты которой в 1972 году распевали посетителям ресторана о всех прелестях мясных консервов Spam. В меню этого ресторана многие блюда состояли из их содержимого. Все было бы хорошо, но у посетителей не брали заказ до завершения выступления группы.

Немного истории…

Борьба со спамом в настоящее время напоминает реальные военные действия, имеющие свою историю и своих "героев". Первая рекламная рассылка была выполнена 3 мая 1978 года представителем компании производителя компьютеров Digital Equipment Corporation с сообщением о дате выхода новой модели. Применительно к навязчивой сетевой рекламе в современном ее понимании термин "спам" стал употребляться только в середине 90-х годов, когда рекламные компании начали публиковать в новостных конференциях Usenet свои объявления. На счастье подписчиков таких групп новостей продолжалось это недолго, так как технология Usenet предусматривала любую фильтрацию сообщений, и администраторы конференций просто удаляли спам ранее, чем он достигал почтовых ящиков. Потерпев здесь неудачу, спамеры переключились на рассылку рекламы с помощью электронной почты по группам адресатов.

Первый спам, рассылаемый по каналам электронной почты, не отличался большой сложностью. Одно и то же письмо рассылалось через сравнительно небольшое, по сегодняшним меркам, количество почтовых систем, позволяющих произвести "через себя" транзитную доставку почты произвольным адресатам (open relay). Боролись с таким спамом, помещая IP-адреса используемых спамерами почтовых серверов в черные списки. В 1997-м году появился первый черный список — MAPS RBL, использовавший технологии DNS и BGP, что позволяло достаточно оперативно обновлять его.

До 1998 года проблема спама усугублялась тем, что популярный в то время почтовый сервер Sendmail при использовании настроек "по умолчанию" работал как open relay. Хотя рекомендации по устранению этого недостатка появились еще в 1996 году для Sendmail версии 8.8, однако при настройке "по умолчанию" Sendmail перестал использовать open relay только с версии 8.9, вышедшей в мае 1998 года. Но и после этого понадобилось время на то, чтобы основной парк почтовых серверов был обновлен.

Другими словами не составляло проблем найти open relay для отправки спама — нужно было просто поискать. Это делали как спамеры, так и анти-спамеры (например, популярный в

свое время сервис ORBS.org автоматически искал такие почтовые сервисы и помещал их в свою базу данных). И RBL, и спамерские списки машин для рассылки стали пополняться автоматически.

В дальнейшем вместе с open relay для рассылки спама начали использоваться и другие способы доступа к ресурсам чужих компьютеров, в первую очередь, так называемые, socks- и proxy-серверы, к которым был возможен неавторизованный доступ. Данные серверы предназначены для сведения всего интернет-трафика небольших компаний к одной единственной машине, имеющей доступ в Интернет. Для работы они обычно используют порты, отличные от портов для SMTP. Если машина допускает неавторизованное соединение с произвольного IP-адреса, ее также могут использовать спамеры для направления своего SMTP-трафика. Интересно отметить, что логи использования socks-серверов обычно не ведутся, поэтому отслеживание истинных источников рассылки даже самими администраторами socks-серверов чаще всего невозможно.

Почти сразу же обнаружилось, что и стандартные открытые HTTP-прокси (типичные порты 3128, 8080 и т.д.), поддерживающие метод CONNECT, можно легко использовать для этой же цели, достаточно в команде CONNECT указать не только имя сервера, но и задать порт для передачи почтового сообщения. Даже любимый всеми "народный" Web-сервер Apache, собранный с модулем *mod_proxy* и неправильно настроенный, нередко используют как средство рассылки почтового спама.

К несчастью, socks- и proxy- сервисы имеются в составе программного обеспечения, предназначенного для конечных пользователей, причем во многих случаях неавторизованный доступ разрешен по умолчанию. В результате количество клиентских компьютеров, которые могут быть использованы для рассылки спама (и прочих действий под контролем третьих лиц) увеличилось вместе с ростом количества высокоскоростных подключений к Интернет.

В течение 2003 года технологии спамеров получили существенное развитие, приспосабливаясь к новым условиям существования. Основное количество спама рассылалалось уже не напрямую, а с помощью сетей, состоящих из захваченных спамерами пользовательских машин. Теперь спамеры рассылают "троянские" программы, которые, заражая машины пользователей, служат площадкой для рассылки спама. В рассылках участвуют сотни тысяч зараженных компьютеров, пользователи которых могут даже не подозревать об этом.

Среди возможностей "троянских" программ есть даже самообновление (upgrade), автоматическое распространение, автоматическое перемещение на другие взломанные машины и т.д. Например, функция такой программы может быть следующей: сходить по HTTP на записанный в нем адрес в заданное время, взять оттуда списки адресов и писем, разослать почту, узнать время и место следующего захода. Иногда "троянские" программы прослушивают каналы IRC и используют команды данной сети, что позволяет скрыть источник команд. В отличие от HTTP, где открытие сайта или закачка новых файлов отслеживаются довольно легко, сообщения по каналу IRC могут передаваться через любой из серверов IRC-сети, и для отслеживания источника необходим оперативный доступ к логам всех серверов сразу. Таким образом, есть много способов скрыть рассылку спама: использовать нестандартные порты, сети управления, протоколы и т.д. Наличие большого количества таких способов приводит к резкому всплеску потоков спама.

Постоянно увеличивающееся количество IP-адресов, с которых потенциально возможна рассылка спама, сделало классические системы RBL не слишком эффективными. В списки помещались только IP-адреса машин, которые действительно могут быть использованы для рассылки спама, либо реально использовались для этого. Такие списки назывались "консервативными". Чтобы увеличить эффективность RBL-систем были созданы "превентивные" черные списки, в которые включали целые диапазоны почтовых адресов (иногда — десятки миллионов): среди них адреса, принадлежащие определенным ISP (Internet Service Provider - провайдер услуг сети Интернет), а иногда — целым странам и даже группам стран. Такой подход, с одной стороны, увеличивал эффективность RBL в борьбе со спамом, с другой, не позволял доставить легальную почту.

На сегодняшний день консервативные RBL предоставляют возможность улавливать около 30-40% спама ценой потерь 2-3% обычной почты. Для "превентивных" RBL-сервисов оба показателя выше, однако большое количество потерь легитимной почты делает использование подобных сервисов мало приемлемым. А увеличение эффективности метода фильтрации спама с использованием RBL-списков без роста доли ложных срабатываний является в настоящее время нереальным.

Проблемы RBL — не слишком высокая эффективность против спама и существенная вероятность потерь легальной почты — привели к появлению других способов борьбы со спамом. К ним, в частности, относятся:

- DNS-проверки — проверяется соответствие данных, сообщаемых в SMTP-сессии. В реальности речь идет о данных, сообщаемых в SMTP HELO.
- Анализ заголовков сообщения. В частности массовые рассылки спама могут быть обнаружены по содержимому заголовков электронной почты.

Каждый из этих методов непосредственно после своего появления был достаточно эффективным, однако ни один из них не является панацеей против спама — технически возможно сделать абсолютно "легальное" (с точки зрения рассматриваемых методов) спам-сообщение.

Дальнейшая эволюция методов борьбы со спамом привела к появлению контекстной фильтрации электронной почты и статистических методов анализа текстов сообщений. Данные методы фильтрации спама являются на сегодня наиболее эффективными и позволяют справиться со все возрастающим потоком спама.

Экономика спама

Спам существует потому, что имеются экономические предпосылки для его существования. Если рассматривать спам как объект информационного обмена, то между его субъектами устанавливаются определенные экономические отношения. К субъектам таких отношений относятся:

1. **Заказчики.** Они заинтересованы в широком распространении по каналам электронной почты определенной информации. Именно заказчики первоначально инвестируют в спам часть своих финансовых средств, предназначенных на рекламу продуктов, решений и услуг.
2. **Создатели/распространители спама.** К ним принадлежат непосредственно спамеры, которые производят и распространяют спам, а также недобросовестные провайдеры, которые заинтересованы в увеличении объема использования трафика. У спамеров, в свою очередь, существует свое разделение труда: среди них можно выделить две категории: "взломщики" и "рассылочники". "Взломщики" проникают в любые доступные компьютеры и устанавливают на них "троянские" программы, обеспечивающие скрытую рассылку спама. "Рассылочники" работают с использованием обычного списка. Именно они являются основными покупателями списков почтовых адресов.
3. **Потребители спама.** Самое ужасное, что потребителями спама становятся поневоле. Мы получаем спам вне зависимости от нашего желания. Мы понимаем, что часть трафика была задействована на транспортировку спама, и при этом вынуждены его оплачивать. Кроме того, существует некоторое противоречие в наших действиях. С одной стороны, мы резко выступаем против спама, с другой — иногда поддаемся на "уговоры" и реагируем на рекламу (иначе заказчики вряд ли бы тратили деньги впустую).

Разрешить проблему спама возможно только путем устранения условий его существования. Во-первых, можно постараться разрушить экономические отношения между субъектами, участвующими в производстве и потреблении спама. Например, исключить хотя бы один субъект из данной цепочки. Представьте, если не будет заказчиков или потребителей, тогда создатели спама "вымрут" как таковые. Во-вторых, развернуть активную борьбу со спамом, которая должна вестись на всех возможных фронтах, начиная с конечных пользователей, заканчивая государственными и общественными организациями.

В настоящее время существует несколько различных организационных способов борьбы со спамом. К ним относятся:

- **Юридические способы.** Предполагают принятие законов о запрещении спама, создание государственных служб для выявления и преследования спамеров, наделение провайдеров определенной ответственностью и полномочиями по фильтрации почты.
- **Социальные способы.** Создание условий, в которых спам становится процедурно невозможным или экономически невыгодным. Предполагают введение новых способов обмена электронной почтой (введение платных электронных марок, подтверждение отправки писем и т.п.). Создание сообществ и объединений (например, провайдеров) для борьбы со спамерами.
- **Пропаганда.** Предполагает разъяснение негативной роли спама как на государственном, так и общественном уровнях.
- **Технические способы.** Предполагают внедрение технических средств контроля за рас-

пространением спама, выделение спама из информационного потока, а также его блокировка.

Первые три способа не будут рассматриваться в данной статье, поскольку они имеют отношение скорее к деятельности общества и государства по борьбе со спамом. Речь в статье пойдет о "средствах индивидуальной защиты" организации, то есть программных средствах, которые обеспечивают фильтрацию спама на корпоративном уровне. Основное внимание будет уделено техническим способам борьбы со спамом, которые обеспечивают фильтрацию почтового трафика в локальных вычислительных сетях.

Определение спама

При рассмотрении и изучении какого-либо явления необходимо дать четкое определение используемым понятиям. При рассмотрении проблем, связанных со спамом, это особенно важно, так как имеется большое количество различных определений, многие из которых не раскрывают сути спама, являются слишком расплывчатыми и не применимыми для практического использования. На сегодняшний день в Российской Федерации определения термина "спам", закрепленного в рамках федерального законодательства, не существует, поэтому используется лишь "обиходное" определение данного понятия.

Итак, мы рассматриваем спам, распространяемый по каналам электронной почты*. С нашей точки зрения, наиболее полным и раскрывающим данное понятие является слеюдущее определение:

"Спам – это анонимная безадресная массовая незапрошенная рассылка почтовых сообщений".

При этом:

- "Анонимная" означает автоматическую рассылку со скрытым или фальсифицированным обратным адресом.
- "Безадресная" – отсутствие указания на конкретного человека (обращения) в тексте письма.
- "Массовая" – рассылки с одинаковым (либо сходным) содержимым, направляемые одновременно на несколько десятков тысяч (и более) адресов.
- "Незапрошенная" – рассылки, которые навязываются пользователю вне зависимости от того, хочет ли он получать данную корреспонденцию или нет (подписные рассылки и конференции не подпадают под данное определение).

Однако необходимо отметить, что нас в первую очередь должно интересовать не столько определение понятия "спам", сколько выявление признаков спама, которые позволяют применять технические средства фильтрации для его эффективного выделения из почтового потока.

Признаки спама

Признаки, которые позволяют отнести то или иное письмо к категории "спам", условно можно разделить на две группы – формальные и лингвистические. Формальные признаки включают в себя:

1. Почтовые адреса, IP-адреса (это позволяет обеспечить фильтрацию по спискам).
2. Отсутствие адреса отправителя.
3. Отсутствие адреса получателя или наоборот наличие большого количества получателей.
4. Отсутствие IP-адреса в системе интернет-адресов DNS.
5. Определенный размер и формат сообщения.
6. Путь доставки электронной почты и т.п.

Лингвистические признаки включают в себя (распознавание спама по содержанию письма):

1. Слова и фразы, построенные определенным образом.
2. Эвристические признаки.
3. Статистические признаки.

Если рассматривать данную проблему с технической точки зрения, то к признакам спама также можно отнести:

- одновременную рассылку по множеству адресов или неоднократное направление сообщения по одному адресу (что позволяет сделать вывод о массовой рассылке и применить фильтрацию по данному признаку);
- наличие текстового сообщения (как бы спамеры не маскировали спам, текст и адрес электронного письма всегда будут настоящими, что позволяет осуществлять контекстную фильтрацию почтовых сообщений);
- спам-сообщение должно быть легко читаемым для получателя. Другими словами, оно

*Понимать это необходимо, поскольку спам распространяется не только по каналам электронной почты. Есть другие всевозможные способы его распространения: Web, СМИ и т.п.

не может быть зашифровано, основной объем информации должен быть передан адресату в составе сообщения. Количество случайных последовательностей ("мусора"), видимых пользователем, должно быть небольшим. При нарушении этих правил снижается читаемость, а следовательно, и отклик на рекламу;
- безадресность текстового сообщения (наличие обращения к конкретному сотруднику компании в теле письма позволяет сделать однозначный вывод о том, что письмо не относится к массовой рассылке);
- наличие признаков подделки адресов (что позволяет применить, так называемую, функцию anti-spoofing).

Кроме того, необходимо выделить некоторые признаки, при наличии которых невозможно однозначно определить, является ли данное сообщение спамом, однако в совокупности с вышеназванными техническими признаками, они помогают убедиться в том, что письмо действительно относится к категории "спам". В первую очередь, это размер спам-сообщений, который в большинстве случаев не превышает 10 килобайт. Кроме того, спам-сообщения имеют простую структуру. Вряд ли письма размером в несколько десятков килобайт со сложной структурой, в состав которых входят различные вложения и другие объекты, могут относиться к спаму.

Технологические особенности распространения спама

Развитие технологий рассылки спама привело к тому, что на сегодняшний день спам-почта имеет ряд технологических особенностей, важных для рассматриваемой далее темы:

- **Распределенность.** Существенная доля спам-сообщений рассылается через оборудование, установленное у конечных пользователей (будь то отдельные частные пользователи или целые локальные вычислительные сети). Используются как проблемы в программном обеспечении, так и вредоносные "троянские" программы, которые пользователь получает вместе с вирусами либо по файлообменным сетям. Как правило, отдельный пользовательский компьютер применяется для рассылки небольшой доли сообщений, при этом в рассылке участвуют сотни и тысячи пользовательских машин. Кроме того, крупные спамеры применяют при рассылке спама сквозной мониторинг доставки сообщений, в результате которого письмо, отвергнутое при попытке доставки с одного IP-адреса, будет отправлено заново с другого IP. Это делает запрет на получение почты (reject) по RBL-спискам неэффективным — попытки доставки сообщения повторятся с других IP-адресов.
- **"Мимикрия" под легальные письма.** Спамеры делают техническую информацию в рассылаемых письмах максимально похожей на легальную переписку. В результате большая часть спама легко проходит через формальные фильтры.
- **Уникальность.** Большая доля спам-сообщений уникальна. Другими словами, в письмо вносятся случайные последовательности символов (часто невидимые для читателя), персональные обращения, анекдоты, большие куски связного текста и тому подобное.

Технические способы борьбы со спамом

Фильтрация спама осуществляется исходя из вышеперечисленных признаков и особенностей электронных писем. Она производится автоматически с помощью специализированных технических средств. Как правило, это программные средства, которые выделяют спам из общего потока сообщений и обеспечивают определенные действия над ним (блокировку, архивирование, дополнительную обработку и т.п.). В настоящее время существует множество различных технических средств борьбы со спамом. Они различаются по технологиям, которые они применяют для выделения спама. Применение той или иной технологии фильтрации спама зависит от разных факторов, однако определяющим является то, в каком месте сети применяются анти-спам фильтры. Исходя из наиболее общих подходов, можно выделить три места расположения таких фильтров:

1. Фильтрация на стороне провайдера.
2. Фильтрация на корпоративном сервере.
3. Фильтрация на стороне клиента*.

*В данной статье фильтрация спама на стороне клиента рассматриваться не будет, поскольку речь идет о корпоративных решениях.

Фильтрация спама на стороне провайдера

Стремительно возрастающее количество спама вынуждает крупные интернет-сервисы Рунета внедрять новые технологии фильтрации почты. Усиливается борьба со спамом на Hotmail, Yahoo! и MSN, которые внедряют новые технологии фильтрации. В Рунете запущен бесплатный фильтр спама Spamtest.ru, на крупнейшем российском почтовом сервисе Mail.ru внедрен "Антиспам Касперского", Yandex объявил о запуске собственного сервиса "Спамооборона", почтовый сервис портала KM.RU внедрил защиту от спама "Карантин", компании E-Style ISP", "Петерлинк" установили "Антиспам Касперского", "Корбина Телеком" объявила о внедрении собственного фильтра спама, построенного на бесплатном программном обеспечении SpamAssassin.

Провайдеры могут фильтровать спам для клиентов, которые держат у них свои почтовые ящики. Обычно это домашние пользователи, использующие доступ по телефонной линии, либо пользователи выделенных линий. Среди них также есть некоторое количество корпоративных пользователей. Это характерно только для компаний, у которых не создана собственная почтовая система, и они держат почту исключительно у провайдера. В некоторых случаях это достаточно удобно и не требует больших затрат. Однако для компаний, у которых создана своя почтовая система, такой способ фильтрации не применим по следующим причинам:

- Конфиденциальность электронной почты. Эффективная фильтрация почты требует как минимум контроля текстовой составляющей письма, а это означает, что провайдер будет осведомлен о содержании электронной переписки компании.
- Невозможность построения гибкой политики использования электронной почты. Компании, как правило, имеют сложную структуру, в которой различные группы пользователей могут получать определенные категории писем. При этом одно и то же письмо может относиться одновременно к нескольким категориям (письмо может быть спамом для одной категории пользователей и деловым письмом для другой, к примеру, рекламное письмо о выставке профильной продукции для отдела маркетинга будет деловым, а для отдела информационных технологий — спамом).
- Методы и технологии фильтрации на стороне провайдера не применимы для корпоративного пользователя.

Если с первыми двумя причинами все предельно ясно, то последняя причина требует некоторого пояснения. Для фильтрации спама провайдеры используют следующие методы фильтрации спама:

- С использованием RBL-сервисов (по почтовым адресам).
- Распределенные методы обнаружения спама.

Каждый из способов имеет свои преимущества и недостатки. Попробуем показать, почему эти методы неприменимы для корпоративного пользователя.

Фильтрация спама с использованием сервисов RBL

Фильтрация по RBL-спискам является наиболее стандартным и легко реализуемым методом обнаружения спама, и с учетом этих обстоятельств этот метод в настоящий момент доминирует среди провайдеров. Сервисы RBL (Realtime Blackhole List) были первым эффективным средством борьбы со спамом. Эти сервисы устроены одинаково — имеются списки почтовых адресов известных спамеров, адресов открытых почтовых пересылок (open relay), используемых спамерами эпизодически или регулярно, и списки диапазонов адресов тех сетей, которые не борются со спамерами или слишком к ним либеральны. Доступ к данным спискам осуществляется в реальном времени по протоколу DNS. Почтовые серверы, использующие RBL, в момент приема очередного сообщения запрашивают сервис (или несколько RBL-сервисов) о том, является ли почтовый адрес отправителя письма "плохим", и на основании ответа RBL либо принимают, либо отвергают письмо. Простота идеи имеет и очевидный недостаток — сообщение принимается или отвергается только на основании адреса посылающей стороны (пользователя или другого почтового сервера). В результате, если какой-то почтовый сервер попал в RBL-список, то вся почта (как спам, так и "не спам") с этого сервера уже приниматься не будет. А это не всегда "плохие" серверы. В эти списки могут быть по ошибке внесены и "хорошие" серверы, например, дружественных Вам провайдеров.

RBL-сервисы в настоящее время широко используются интернет-провайдерами, почтовыми службами и организациями. Во многих случаях качество RBL оценивается по единст-

венному параметру — количеству спама, который проходит через почтовый сервер. Если количество спама удается уменьшить, данный RBL-сервис считается "хорошим". В то же время есть и другая, не менее важная характеристика — сколько "нормальных" писем не попало к получателям. Здесь речь идет о проблеме ложных срабатываний. Ложным срабатыванием (False Positive) принято считать тот случай, когда "нормальное" письмо (которое получатель не посчитал бы спамом) до получателя не дошло. Сам получатель об этом обычно не узнает, либо узнает по другим каналам связи ("я тебе писал" — "а я ничего не получил"), поэтому проблема во многих случаях остается незамеченной.

В результате проведенных исследований в сети Рунета было установлено, что процент ложных срабатываний при фильтрации спама с использованием RBL-списков в среднем составляет 2,1%*. Другими словами, среднестатистический пользователь (который активно использует электронную почту в бизнес-процессах) потерял бы каждое 40-60-е письмо, что приблизительно составляет одно-два важных письма в день. При этом анти-спам средства, использующие RBL-списки, способны отфильтровывать не более 30-40% спама. А это говорит о том, что этот метод фильтрации в настоящее время не является эффективным средством борьбы со спамом.

Однако практика показала, что несмотря на отмеченные недостатки, метод фильтрации спама с использование RBL-списков обязательно должен применяться. Да, он один не в состоянии решить проблему, но применение его в комплексе с другими решениями, обеспечивающими блокировку спама, дает положительные результаты. Как правило, проверка IP-адреса по RBL-спискам проводится на начальном этапе фильтрации спама и позволяет отсечь почту (20-30%), относящуюся к стопроцентному спаму. Очень важно понять это, поскольку многие провайдеры, использующие только этот способ фильтрации, "подают" его как панацею, объясняя, что списки они составляют сами, а проверки на ошибки проводятся регулярно.

Распределенные методы обнаружения спама

Распределенные методы обнаружения спама используют в основном провайдеры и то только крупные, поскольку анализ и принятие решения осуществляется на основе информации, получаемой из крупных почтовых систем с миллионами пользователей. Смысл распределенных методов обнаружения спама заключается в сборе данных о спам-почте из максимально возможного количества точек сети. Эти данные обрабатываются и делаются доступными для всех заинтересованных участников информационного обмена в сети.

В настоящее время реализованы следующие способы сбора данных о рассылках спама:

- Прием спама в специальные "ловушки" (honeypot).
- Голосование пользователей — пользователь, получивший спам, информирует об этом систему сбора данных, предоставляя образец спама. Одним из сервисов такого рода является, так называемая, *"бритва Вайпула"* (Vipul Razor). Основная идея сервиса заключается в создании сигнатур спамерских писем, причем письма присылают сами пользователи, а в базу сигнатуры спамерских писем заносятся по принципу голосования (если приславших данное письмо много или они достаточно авторитетны).
- Анализ всей проходящей через почтовую систему почты с целью определения контрольных сумм спам-сообщений и передачи их на центральный сервер, установленный в сети.

На основании собранных данных, которые выглядят как "такое-то письмо принято в мире столько-то раз", либо "на такое-то письмо пожаловались столько-то раз", строятся списки массовых на данный момент времени рассылок, которые становятся доступными участникам системы в реальном времени. Почтовые системы, приняв письмо, могут узнать его статус и либо отвергнуть (уничтожить, перенаправить в архив или карантин) как спам, либо передать получателю.

К недостаткам распределенных методов фильтрации спама относится, прежде всего, возможность компрометации данных систем. В качестве примера можно привести случай, когда в руки спамеров попадает часть списков "ловушек". В результате они "заваливают" ловушки легитимной почтой, что приводит к увеличению количества ложных срабатываний. Снижение качества работы системы, как правило, проис-

*Соответствующие тесты проводились в течение двух месяцев 2003 года. Была использована подборка из 42 542 писем, среди которых важные письма составляли 60%, а спам — 40% (письма были выделены вручную, что исключало ошибки). Подборка была проверена на двух RBL-списках реальных почтовых систем, активно используемых в настоящее время провайдерами и другими организациями в сети Рунет.

ходит в случаях, когда спам в эти "ловушки" перестает поступать.

Качество работы систем с голосованием пользователей напрямую зависит от активности пользователей. Влиять на такую активность практически невозможно, а скомпроментировать систему легко. Достаточно спамерам стать голосующими участниками и голосовать "против" легитимных рассылок.

Кроме того, серьезной проблемой для описанных методов детектирования массовых рассылок является уникальность каждого отдельно взятого спам-сообщения — каждое современное спамерское письмо существует в огромном количестве вариантов с незначительными отличиями в тексте. На сегодняшний день ни одна из распределенных систем полностью разрешить данную проблему не способна.

Вторая проблема связана с ложными определениями легальных рассылок как спама. Эта проблема характерна как для методов, анализирующих всю почту, так и для систем с голосованием пользователей.

В настоящее время большинство публичных почтовых сервисов (Hotmail, Lycos, Mail.ru, Yandex) активно используют те или иные технические средства, позволяющие заметить факт массовой рассылки на почтовые ящики, зарегистрированные в системе. Данный способ распознавания спама доступен только публичным почтовым службам с большим количеством пользователей, однако в действительности он распознает не спам, а именно массовые рассылки, в том числе санкционированные пользователями (подписные). По имеющимся оценкам, штатные средства фильтрации публичной почты пока не совсем эффективно справляются со своей работой. Эти системы позволяют обеспечивать блокировку только 50% спама. Кроме того, существенной проблемой до сих пор остаются ложные срабатывания.

Почтовый сервер провайдера характеризуется большим потоком писем. На нем можно обеспечить гарантированную производительность, на нем есть постоянная связь с другими серверами в сети. Однако именно из-за массового характера поступления почты на стороне провайдера практически неприменимы в чистом виде алгоритмы, осуществляющие фильтрацию по смысловому содержимому текста письма. Массовость предполагает, кроме того, использование неперсонализированных анти-спам продуктов. Ведь в неперсонализированной анти-спам системе, которой известны предпочтения только усредненного пользователя, высокий показатель определения спама (как заявляют представители провайдеров, качество фильтрации таких систем составляет 98%) теоретически недостижим.

У корпоративного клиента совершенно иная картина. Почтовый поток не такой массовый, как у провайдера. Кроме того, невозможно или слишком дорого постоянно "закачивать" массивы контрольных суммы писем или IP "черных дыр". Зато очень точно можно отличить чужие письма, они всегда не похожи на ваши по смыслу; стиль одного пользователя (группы пользователей) выявить несложно. Корпоративному пользователю необходимы системы, которые имеют возможность работать с текстом письма и не просто определять его содержимое, а уметь относить данное письмо к определенной категории, предназначенной для той или иной группы пользователей. Именно алгоритмы фильтрации, основанные на разборе и анализе текста, способны сегодня обеспечить эффективное определение спама. Они имеют возможность проводить более гибкую фильтрацию и персонализировать процесс обработки почты. Технически осуществить решение данной задачи возможно путем обеспечения фильтрации спама на корпоративном сервере.

Фильтрация спама на корпоративном сервере

Большинство средних и крупных компаний имеют свой корпоративный почтовый сервер, установленный в офисе компании. Это значит, что средства фильтрации провайдера в данном случае неприменимы. Для таких компаний существует категория специального серверного программного обеспечения — продуктов, позволяющих фильтровать спам на корпоративном почтовом сервере до рассылки его по рабочим местам сотрудников.

Такие почтовые серверы, как Microsoft Exchange, Sendmail, Postfix, обычно включают средства для обеспечения фильтрации содержания почтовых сообщений (спама и вирусов), однако эти средства обычно довольно примитивны и представляют собой "пустые рамки" для правил, то есть предлагают администратору почтовой системы самостоятельно создавать и настраивать правила фильтрации. Этот подход работает не очень хорошо, так как для фильтрации спама нужна гибкая политика, множество правил, которые постоянно обновляются и корректируются.

Данная проблема решается за счет того, что почти все почтовые серверы имеют возмож-

ность встраивать или интегрировать системы третьих производителей. Современный рынок информационной безопасности предлагает много продуктов, обеспечивающих фильтрацию спама на корпоративном сервере. Это могут быть как коммерческие, так и бесплатные продукты, распространяемые на условиях лицензии GPL (General Public License) или подобных ей.

Бесплатные фильтры. Наиболее известный бесплатный фильтр — *SpamAssassin*. Это весьма эффективная программа, фильтрующая 90-95% спама. SpamAssassin поставляется с постоянно обновляемой базой правил фильтрации как по формальным признакам письма, так и по содержанию (ключевым словам). Недостатки этого фильтра заключаются в том, что он не имеет локальной привязки к языкам и регионам, ориентируясь в основном на англоязычный спам. Набор правил SpamAssassin очень велик и непрозрачен (понять, какое правило сработало можно, но трудно предугадать, к чему приведет его отмена), что очень затрудняет настройку.

Коммерческие продукты. Средства фильтрации спама, реализуемой на корпоративном сервере, предлагают многие производители. Сложность заключается в выборе продукта, который наиболее подходит для решения задач контроля использования электронной почты компании.

В настоящее время на рынке анти-спам систем представлены два основных типа фильтров:

- фильтры, работа которых основана на поиске в электронных письмах определенных признаков (так называемые, традиционные фильтры);
- фильтры, применяющие статистические (вероятностные) методы для обеспечения фильтрации спама.

И те, и другие осуществляют контекстную фильтрацию электронной почты, то есть содержание письма для них является одним из важнейших критериев, по которому его можно отнести к спаму. Однако традиционные фильтры обладают довольно серьезными недостатками.

Некачественное разделение спама и обычных писем обусловлено некоторой "однобокостью" традиционных фильтров. При отбраковке писем учитываются "плохие" признаки и не учитываются "хорошие", характерные для деловой переписки.

Этих недостатков лишен метод построения анти-спам фильтров, предложенный американским программистом и предпринимателем Полом Грэмом*. Метод Грэма позволяет автоматически настроить фильтры согласно особенностям индивидуальной переписки, а при обработке учитывает признаки как "плохих", так и "хороших" писем. Такой метод фильтрации спама называют статистическим или вероятностным.

Статистические (вероятностные) методы фильтрации спама

Статистический метод основывается на теории вероятностей и использует для фильтрации спама статистический алгоритм Байеса. Каждому встречающемуся в электронной переписке слову или тегу присваивается два значения: вероятность его наличия в спаме и вероятность его присутствия в письмах, разрешенных для прохождения. Баланс этих двух значений и определяет вероятность того, что письмо, в котором встречаются данные слова и теги, является спамом.

Как справедливо заметил Пол Грэм в своей статье A Plan for Spam, "ахиллесова пята спамеров — их сообщения. Они могут преодолеть любой барьер, какой вы установите... Но они должны доставить свое сообщение, каким бы оно ни было". Иначе говоря, спамеры могут идти на любые уловки с IP-адресами и подгонкой текста сообщений, но продать-то вам свою виагру, американский английский, виллу на Канарских островах и "мужа на час" они все-таки должны! Если посланное ими сообщение из-за вынужденного применения "эзопова языка" будет непонято читателями, то толку от такой рассылки совершенно нет. "Читать между строк" покупатель не будет. Значит они все-таки должны написать в письме нечто понятное, призывающее нас к какому-то действию. Вот этот признак спам-сообщения и является основой для работы фильтров, основанных на статистических алгоритмах Байеса.

Для вычисления вероятности спама используются таблицы вероятности (принадлежности слов из письма, относящегося к категории "спам"), созданные в процессе обучения фильтра. А именно: берутся как минимум два списка слов различных категорий писем (например, "разрешенных" и "запрещенных") и передаются на обработку программе обучения. Она вычисляет частотные словари для каждой катего-

*Пол Грэм (Paul Graham) - американский программист и предприниматель, один из разработчиков электронного магазина Viaweb Store, известного в настоящее время как Yahoo! Store.

рии сообщений — сколько раз какое слово встречалось в письмах этой категории (в данном случае спама). Когда словари заполнены, вычисление вероятности принадлежности конкретного нового письма к тому или иному типу производится по формуле Байеса для каждого слова этого нового письма. Суммированием и нормализацией вероятностей слов получают вероятности для всего письма. Как правило, вероятность принадлежности электронного письма к одной из категорий на порядок выше, чем к другим. К данной категории и следует относить сообщение.

Сразу после начального "обучения" фильтра точность определения спама этим методом достигает значительной величины — 97—99% и продолжает уверенно двигаться к 100% после проведения дальнейших корректировок фильтра.

Корректировка фильтра заключается в обработке случаев неправильной классификации писем — фильтру указывается, к какой категории следует впредь относить эти письма, и он добавляет слова из этих писем в соответствующие таблицы вероятностей. Обратите внимание — администратору не приходится вручную анализировать письмо и пополнять на основе проведенного анализа списки правил фильтрации, как это делается в традиционных фильтрах. Достаточно добавить письмо в архив писем данной категории, заново запустить процесс "обучения" фильтра и статистический "портрет" письма меняется полностью и автоматически. Практически байесовский фильтр заменяет все те лингвистические лаборатории, которые осуществляют анализ вновь поступающего спама. Ведь они осуществляют корректировку антиспам фильтров тем же способом ("впредь считай такие письма спамом").

Приведем основные отличия статистической технологии фильтрации от технологии фильтрации на основе признаков, присущих спаму:

1. Особенность статистической технологии заключается в возможности индивидуальной автоматической настройки фильтра, что является важным преимуществом, поскольку разные люди или же компании (если фильтр устанавливается на корпоративном почтовом сервере) используют в электронной переписке разную лексику. Настройка фильтра производится по результатам статистического анализа имеющегося архива электронной почты или выборки, полученной за определенный период времени. Такой анализ дает возможность накопить достаточно информации для эффективной фильтрации электронной почты.
2. И в том, и в другом случае результатом оценки является, так называемый, "вес" письма. Однако при применении метода с использованием признаков спама "вес" письма вычисляется только на основе "плохих" признаков, что приводит к "обвинительному уклону" фильтра, и, как следствие, появляются ложные срабатывания.
3. В алгоритме Байеса наборы признаков определяются не субъективно, а в результате статистического анализа реальных подборок писем. Получающиеся наборы признаков оказываются весьма нетривиальными и эффективными. Например, в качестве "плохого" признака может появиться строка "0Xffffff" — ярко красный цвет; а в качестве "хорошего" признака — Ваш номер телефона. И действительно, письмо, содержащее Ваши персональные данные, в любом случае следует прочесть.

По имеющимся оценкам, статистический метод борьбы со спамом является весьма эффективным. Так, в процессе испытания через фильтр были пропущены 8 000 писем, половина из которых являлась спамом. В результате система не смогла распознать лишь 0,5% спам-сообщений, а количество ошибочных срабатываний фильтра оказалось нулевым.

Самое важное преимущество байесовского фильтра заключается в том, что он надежно исключает ложные срабатывания. Ведь процесс принятия решения (относится письмо к спаму или нет) осуществляется в соответствии с особенностями индивидуальной переписки, а при обработке учитываются признаки как "плохих", так и "хороших" писем. Именно за счет баланса этих признаков и удается свести к минимуму количество ложных срабатываний фильтра.

Другим преимуществом теоремы Байеса является возможность ее использования для классификации любых текстов письма по любым категориям, и поэтому он имеет более широкое применение, чем тривиальная фильтрация спама. Например, для построения политики использования электронной почты, речь о которой пойдет в следующих главах.

Таким образом, в настоящее время наиболее эффективным и оптимальным для корпоративных пользователей являются системы, основанные на статистических (вероятностных) методах фильтрации спама.

Подход компании “Инфосистемы Джет” к проблеме борьбы со спамом

Главная задача, которую решают традиционные спам-фильтры, — это разделить входящий поток сообщений на спам и “нормальную” почту. Однако такой подход является заведомо обреченным на поражение. Осуществить такое разделение чрезвычайно сложно, а если разобраться, то без определенных потерь практически невозможно (чтобы избежать ложных срабатываний, администраторы вынуждены снижать качество фильтрации за счет “разрешения” некоторого количества спама). В следующих главах будет проанализирован подход компании “Инфосистемы Джет” к вопросу борьбы со спамом. Фильтрация спама рассматривается специалистами компании как одна из задач в рамках общекорпоративной политики использования электронной почты, а значит, в контексте общей политики информационной безопасности. Изначально задача отфильтровать спам не ставится, а наоборот предлагается обеспечить фильтрацию важной для компании электронной почты, при этом главная цель — это обеспечить безопасное, эффективное и наиболее оптимальное функционирование корпоративной почтовой системы.

Почему данный подход является наиболее оптимальным?

Во-первых, необходимо отдавать себе отчет в том, что спам хотя и доставляет массу хлопот, однако не является угрозой номер один. Если определять по степени уязвимости информационных систем данному типу угроз и последствиям воздействия на локальные вычислительные сети, спам не наносит такого значительного урона, как, например, вредоносный мобильный код или утечка конфиденциальной информации. Следовательно, предпринимаемые против спама меры должны быть пропорциональны степени угроз корпоративным сетям. Однако не стоит также пренебрегать проблемой спама, что чревато негативными последствиями для компаний.

Таким образом, чрезмерный интерес к проблеме спама в ущерб другим мерам по защите, с одной стороны, и слабое внимание, уделяемое фильтрации спама, с другой, может привести к серьезным последствиям для безопасности корпоративных информационных систем. Необходим только комплексный и взвешенный подход к обеспечению безопасности, где каждой проблеме уделяется соответствующее внимание.

Во-вторых, внедряя такой подход, борьба со спамом в значительной мере облегчается, что можно подтвердить следующим примером: в настоящее время насчитывается более 500 категорий спама, в то время как в среднестатистической компании можно выделить не более 10-15 категорий писем, “важных” с точки зрения бизнес-процессов, происходящих в компании. Естественно, что отфильтровывать и пропускать “важные” письма проще, чем выделять из почтового потока все письма, относящиеся к спаму.

В-третьих, данный подход обеспечивает комплексность, которая предполагает использование для фильтрации спама одновременно нескольких технологий и методов. В частности, система “Дозор-Джет”, разработанная специалистами компании “Инфосистемы Джет”, имеет возможность обеспечивать фильтрацию спама как с использованием статистических алгоритмов письма, так и по признакам электронного письма.

В-четвертых, такой подход дает возможность построить и реализовать политику использования корпоративной электронной почты, в которой одному и тому же письму может быть присвоено несколько различных категорий, и данное письмо будет доставлено (или перенаправлено) определенным группам пользователей. Это предполагает, что одно письмо может быть отнесено к спам-сообщениям для одной группы пользователей, и к деловым письмам для другой.

Что касается политики использования электронной почты, то она обычно принимается в компаниях на административном уровне. Такая политика устанавливает правила использования электронной почты, то есть определяет следующие параметры:

- ***Что контролируется*** — прохождение *каких категорий* сообщений электронной почты должно быть разрешено или запрещено.
- ***На кого распространяется*** — *пользователи/группы пользователей*, которым разрешено или запрещено получать сообщения электронной почты определенной категории.
- ***Как реагирует система*** — *что необходимо делать* с теми или иными сообщениями электронной почты, которые удовлетворяют или не удовлетворяют критериям, опреде-

ленным правилами использования электронной почты.

Категории почтовых сообщений

В компании обычно разрешен обмен только деловыми письмами, то есть письмами, связанными с ее повседневной деятельностью. Сложность заключается лишь в том, чтобы составить наиболее точный "портрет" таких писем. Ведь даже спам в некоторых случаях можно отнести к деловой корреспонденции. Рекламный или маркетинговый отделы часто получают и отправляют сообщения рекламного характера. Кроме того, даже отдел закупок может запросить у компании, предоставляющей какие-либо товары, их описание и характеристики. Как правило, такие материалы имеют содержание, анализ которого позволяет отнести их к рекламе, а значит и к спаму.

Пользователи/группы пользователей

Согласно принятой в компании политике использования электронной почты, всех сотрудников можно условно разделить на следующие группы, каждой из которых могут предназначаться только письма определенного содержания:

1. Сотрудники, для которых возможно составить "портрет" письма.
2. Сотрудники, для которых составление "портрета" письма имеет определенные сложности.
3. Сотрудники, для которых фильтрация писем по каким-либо причинам не осуществляется.

Если взять первую группу пользователей, то к ним можно отнести сотрудников, на чьи почтовые ящики, как правило, приходит формализованная корреспонденция (отчеты, заявки, уведомления и т.п.). Кроме того, к этой группе пользователей относят сотрудников, получающих письма только от определенных отправителей, а получение сообщений из других источников запрещается (либо администратором безопасности, либо самим пользователем).

Ко второй группе пользователей относятся сотрудники, которые получают письма из различных источников, а содержание их почты не поддается формализации или описанию. Для таких пользователей составить "портрет" делового письма сложно, поэтому их корреспонденция отфильтровывается только на наличие писем запрещенного содержания и спама. Этим пользователям нельзя блокировать прохождение важных писем. И во многих случаях, чтобы избежать ложных срабатываний, администраторы снижают уровень полноты фильтрации (количественное соотношение выявленных писем рекламного характера к спам-сообщениям, пропущенным в ходе фильтрации), повышая при этом ее точность (способность средства фильтрации избегать ложных срабатываний).

Третья группа пользователей вообще отказывается от фильтрации своей электронной почты. К ним, как правило, относятся люди творческих профессий, например, журналисты, а также VIP-сотрудники. Их почта анализируется только на содержание вирусов и другого вредоносного мобильного кода.

Средство реализации политики использования электронной почты

Исходя из всего вышесказанного, основной задачей средств реализации политики использования электронной почты является разделение почтового потока по категориям сообщений (деловая почта, спам, частная переписка, письма запрещенного содержания и т.п.), а также по пользователям/группам пользователей. Такое разделение обеспечивается за счет проверки почтовых сообщений на соответствие определенным условиям и реагирования по результатам такой проверки. Условия отбора писем должны, по меньшей мере, быть следующими:

- условия на почтовые заголовки;
- условия на структуру письма (наличие, число и структура вложений);
- условия на типы вложений (MS Office, исполнимые файлы, архивы и т.п.);
- условия на содержимое (текст) писем и вложений;
- условия на результат обработки письма.

Что касается такой категории писем, как "спам", то наиболее эффективной является фильтрация на основе содержания текстов писем и вложений.

Специалисты компании "Инфосистемы Джет" разработали **систему мониторинга и архивирования почтовых сообщений "Дозор-Джет"**, которая обеспечивает фильтрацию почты по всем вышеназванным условиям, а с точки зрения контекстной фильтрации является в настоящее время наиболее эффективным и производительным средством на российском рынке. Система имеет в своем составе Модуль катего-

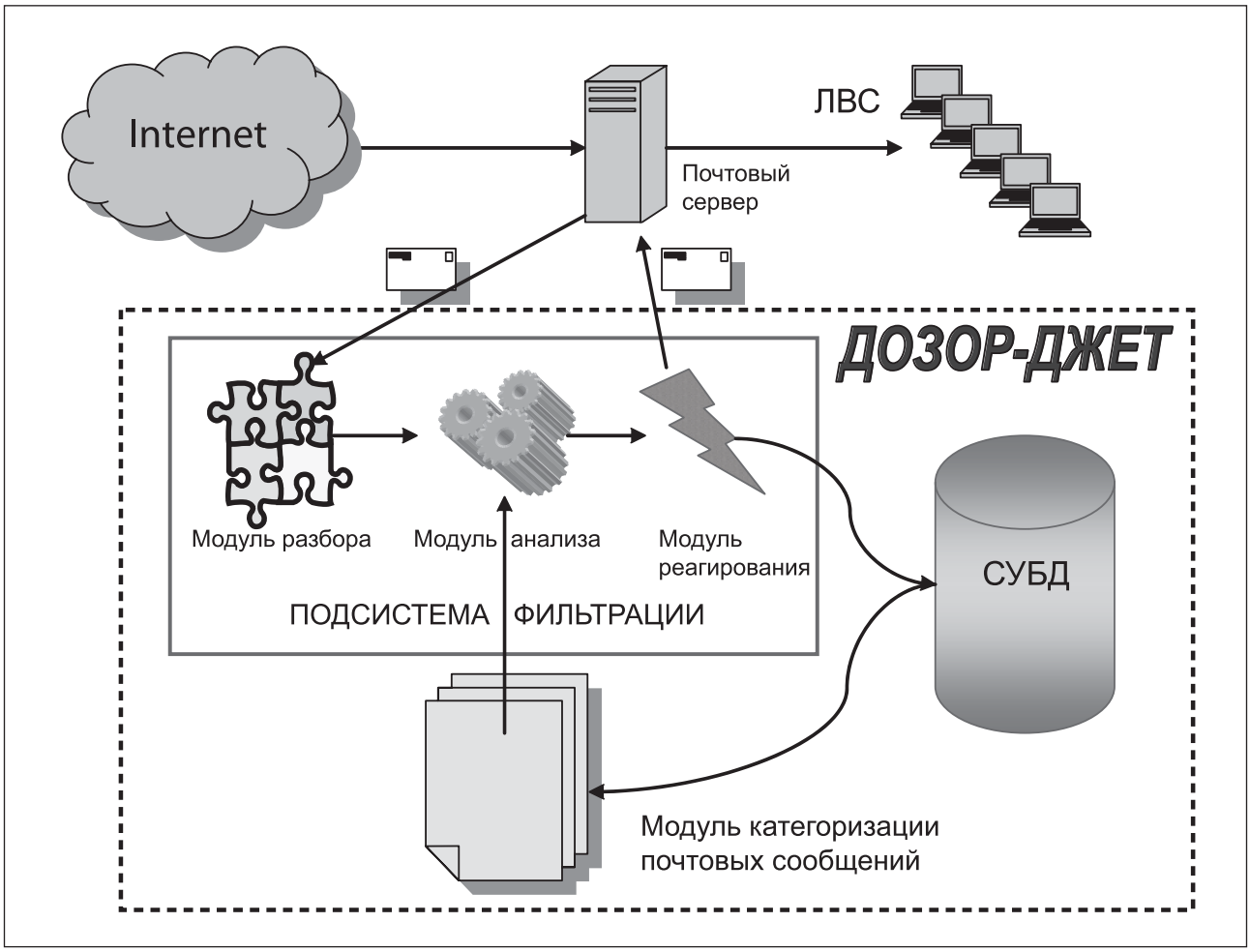

Рис. 1 Структура системы «Дозор-Джет»

ризации почтовых сообщений, работа которого основана на применении статистического алгоритма Байеса. Модуль предназначен для отфильтровывания электронных писем определенной категории. Письма автоматически относятся к той или иной категории на основании ранее выполненного анализа выбранной администратором базы образцов писем.

Структура системы "Дозор-Джет"

Система "Дозор-Джет" имеет такую структуру, которая позволяет обеспечивать высокий уровень защиты почтовой системы от различных угроз. В ее состав входят (см. рис. 1):

- Подсистема фильтрации.
- Подсистема архивирования, реализованная на основе реляционной СУБД.
- Модули, расширяющие возможности системы (в том числе Модуль категоризации почтовых сообщений, который обеспечивает фильтрацию спама).

Фильтрация спама в системе "Дозор-Джет" проходит в несколько этапов. На первом этапе часть спама отсекается уже "на подступах" к системе (30-40%), то есть во время получения почты SMTP-прокси*:

1. Проверка по RBL-спискам. Необходимо подчеркнуть, что в системе "Дозор-Джет" возможны "мягкие" настройки, которые учитывают возможность того, что письмо, отправленное с определенного адреса, может быть "скомпрометировано по ошибке".
2. Anti-spoofing — проверка подлинности адресов путем поиска соответствующей записи в DNS (или проверки существования такого домена в DNS).

*Перечисленные далее утилиты входят в стандартный комплект системы «Дозор-Джет» и при необходимости могут быть отключены администратором.

3. Anti-relay — запрет вхождения и отправки писем, адреса которых отличны от внутренних.

Подсистема фильтрации

После прохождения первого этапа проверки при получении письма SMTP-прокси, наступает следующий этап: письмо передается на обработку подсистеме фильтрации (см. рис. 1). Данная подсистема производит декомпозицию письма (то есть разбор на составляющие компоненты, который обеспечивается Модулем разбора) и проверку его на соответствие заданным администратором безопасности условиям (обеспечивается Модулем анализа и Модулем категоризации почтовых сообщений). По результатам такой проверки осуществляются определенные действия над письмом (обеспечивается Модулем реагирования).

Система имеет мощную подсистему фильтрации, которая обеспечивает глубокую и детальную обработку почты. Ее отличительными особенностями являются:

- полная декомпозиция письма;
- эффективная работа с русскоязычной текстовой частью письма;
- эвристическое определение кодировок;
- гарантированное раскрытие сжатых файлов и "чтение" текстов в них;
- определение типов OLE-объектов;
- наличие условия "ошибка при распаковке".

Осуществление полной декомпозиции письма является одной из самых важных особенностей системы "Дозор-Джет". Ведь от того, как будет произведен разбор письма, зависит качество его анализа, а значит и точное определение, относится письмо к спаму или нет.

Условие "ошибка при распаковке"

Эффективность системы "Дозор-Джет" в борьбе со спамом в значительной степени повышается за счет наличия такого условия обработки писем, как "ошибка при распаковке". Это значит, что в случае невозможности распознать или распаковать какой-либо объект письма, система предпринимает дополнительные действия, которые позволяют довести до конца анализ письма. Как правило, такое письмо помещается в карантин, а администратору системы отправляется соответствующее письмо с указанием причины данного действия. После этого администратор имеет возможность провести дополнительную обработку "нераскрывшегося" письма, в том числе с помощью программного обеспечения третьих производителей. На основании произведенного анализа принимается решение о дальнейшем действии над письмом.

Действия над письмом

В случае со спамом такими действиями могут быть:

- пропустить письмо;
- запретить прохождение письма;
- поместить письмо в архив (целиком или только регистрационную информацию о нем);
- пометить письмо;
- послать уведомление администратору;
- отправить письмо на дополнительную обработку другой программе;
- модифицировать письмо.

Отличительной особенностью системы "Дозор-Джет" является возможность выполнения всех действий одновременно, поскольку они не противоречат друг другу. При первом приближении исключение могут составить лишь первые два действия, а именно "пропустить письмо" и "запретить его прохождение". Однако система "Дозор-Джет" обладает способностью присвоения письму определенной категории. Одному и тому же письму присваивается несколько категорий. Если мы говорим о спаме, то таких категорий может быть как минимум две, например, "спам для финансового отдела" и "деловое письмо для отдела рекламы". Таким образом, данное письмо можно одновременно пропустить в отдел рекламы и блокировать его прохождение в отдел финансов.

Модуль категоризации почтовых сообщений

С учетом подхода борьбы со спамом в контексте общей политики информационной безопасности, спам-сообщения относятся системой к одной из категорий, которую необходимо будет фильтровать в соответствии с политикой использования электронной почты. Такую задачу в системе выполняет Модуль категоризации почтовых сообщений.

Письма автоматически относятся к той или иной категории на основании выполненного ранее анализа выбранной администратором базы образцов писем. Задача администратора сделать наиболее "точную" выборку писем, которые соответствовали бы данной категории. Необходимо избегать попадания в выборку "лишних" писем. Иначе это может привести к ложным срабатываниям фильтра. Наиболее "точная" выборка обеспечивается за счет составления детального SQL-запроса, в котором

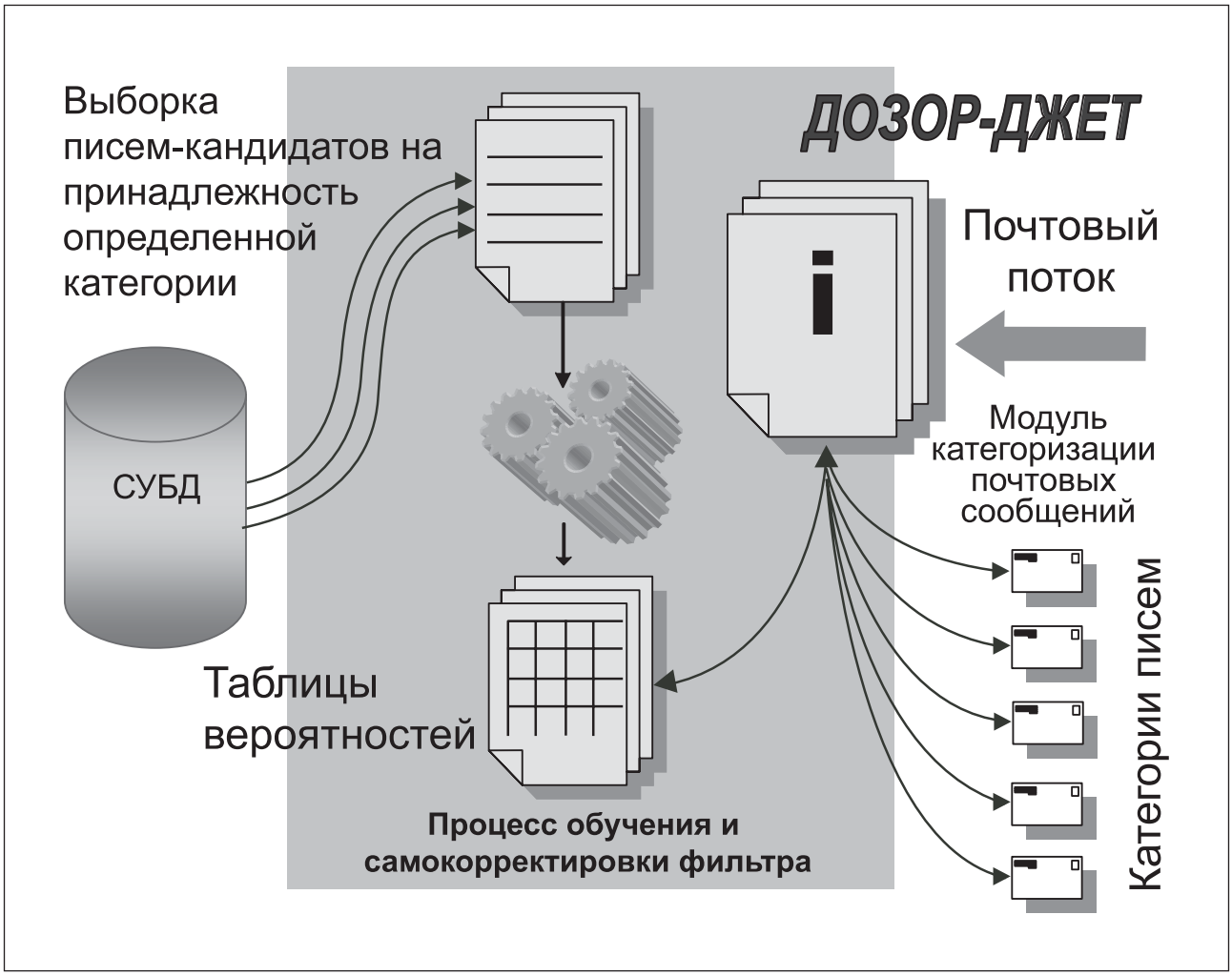

Рис. 2 Модуль категоризации почтовых сообщений

учитываются все признаки писем определенной категории.

После того, как такая выборка сделана, письма проходят обработку, на основании которой составляются таблицы вероятности наличия определенных слов в письмах той или иной категории. При этом таких таблиц составляется как минимум две. Например, категория "спам" для отдела маркетинга и "деловые письма" для отдела маркетинга. Каждому слову выставляется соответствующий "вес": вероятность его наличия в спаме и вероятность его присутствия в письмах, разрешенных для прохождения. Баланс этих двух значений и определяет вероятность того, что письмо, в котором встречаются данные слова, является спамом (в данном случае для отдела маркетинга).

Исходные данные в дальнейшем используются для вычисления по формуле Байеса вероятности принадлежности к той или иной категории каждого нового письма, поступающего в Модуль категоризации почтовых сообщений (см. рис. 2).

Архив электронной почты

Архив электронной почты играет значительную роль в системе. Во-первых, он исключает потерю важной информации при фильтрации. Даже при ложных срабатываниях системы письма никогда не потеряются. Их всегда можно восстановить из почтового архива.

Во-вторых, с помощью архива осуществляется первичное "обучение" Модуля категоризации почтовых сообщений и автоматическая корректировка его работы. Первичное "обучение" фильтра производится на базе выбранной из архива подборки писем, которые, по мнению администратора системы, относятся, например, к категории "спам". Такая подборка осуществляется средствами системы "Дозор-Джет" с помощью встроенного в систему мастера построения запросов либо с помощью SQL-запроса, созданного администратором системы. Корректи-

ровка фильтра также осуществляется на основании данной выборки, только с добавлением писем, которые по тем или иным причинам не смог отфильтровать Модуль категоризации почтовых сообщений.

Необходимо отметить, что в системе "Дозор-Джет" используется СУБД промышленного уровня, которая способна эффективно и быстро производить автоматический поиск и выборку писем любой категории по всем атрибутам письма.

Методы фильтрации на основе признаков спама

Система "Дозор-Джет" подходит к фильтрации спама комплексно. Она не только использует статистические алгоритмы, но и технологию фильтрации на основе признаков спама. При этом фильтрация осуществляется двумя основными способами — по формальным признакам и по содержанию текстовой составляющей писем, то есть с помощью лингвистического метода.

Формальные методы включают в себя:

1. Фильтрацию по спискам (почтовых адресов, IP-адресов).
2. Фильтрацию по следующим признакам письма:
   - отсутствие адреса отправителя;
   - отсутствие или наличие большого количества получателей;
   - отсутствие IP-адреса в системе интернет-адресов DNS.
3. Фильтрацию по размеру.
4. Фильтрацию по формату сообщения.

Лингвистический метод включает в себя: распознавание по содержанию письма (письмо проверяется на наличие признаков спам-сообщений — определенного набора специфических слов или словосочетаний. Отметим, что система "Дозор-Джет" анализирует не только текст самого письма, но и вложений в него).

Работа с текстом

Эффективность фильтрации спама заключается, прежде всего, в производительной работе с текстовой составляющей письма. Ведь именно анализируя текст, мы со стопроцентной уверенностью можем определить, относится письмо к спаму или нет. Система "Дозор-Джет" обеспечивает производительную работу с текстом почтового сообщения. Это осуществляется за счет того, что текст при проведении декомпозиции выделяется из всего сообщения и приводится к единому формату.

При этом работа с текстом включает два этапа:

Первый — выделение текста из письма.

Второй — анализ текста.

Выделение текста из письма

От того, как будет выделен текст, будет зависеть сможет ли система в дальнейшем с данным текстом работать. Поэтому очень важно, чтобы такое выделение было как можно более качественным.

Не секрет, что одной из серьезных проблем обмена информацией на русском языке является кодировка текста, вернее их бесчисленное количество. Поэтому качество распознавания текста зависит от того, как система справилась с определением кодировки. "Дозор-Джет" способен осуществлять анализ русскоязычных почтовых сообщений независимо от используемой кодировки кириллицы (CP1251, CP866, ISO88595, KOI-8R, MAC), включая тексты, кодировка которых не декларирована (например, тестовые файлы в сжатых форматах) или декларирована неверно. При этом декодирование осуществляется с применением технологии эвристического анализа.

Кроме того, необходимо учитывать тот факт, что различные объекты почтового сообщения также имеют различную кодировку, что усложняет процесс последующего анализа письма в целом. В системе "Дозор-Джет" удается избежать данной проблемы за счет, так называемой, нормализации текстовой составляющей почтового сообщения. Нормализация осуществляется следующим образом: весь текст письма вне зависимости от того, где он находится (в заголовках, теле письма, вложенных файлах), выделяется из указанных объектов и приводится к единой кодировке. В дальнейшем все выделенные текстовые части рассматриваются как отдельные объекты (заголовки и файлы) в одной кодировке.

Анализ текста

После того, как текст выделен и приведен к единому формату, можно осуществлять работу с текстом, а именно проводить его анализ. Применительно к проблеме борьбы со спамом, анализ текста будет заключаться в поиске в письмах признаков спама. В системе "Дозор-Джет" такой поиск может осуществляться как базовыми средствами, так и с помощью специального Модуля категоризации почтовых сообщений.

Фильтрация спама базовыми средствами подразумевает создание фильтра с помощью специального интерфейса управления* и зависит только от администратора системы, вернее от его опыта в борьбе со спамом. Администратор должен знать, какой спам получает его компания, какие признаки присущи данному спаму и по каким из этих признаков необходимо фильтровать почту, чтобы эффективно блокировать спамерские сообщения. Ясно, что администратор должен обладать "незаурядными" способностями и постоянно отслеживать ситуацию в данной области. Спамеры постоянно модифицируют свои сообщения, поэтому признаки спама будут все время изменяться. Чтобы избежать зависимости качества работы фильтра от способностей администратора, разработчики системы "Дозор-Джет" включили в состав системы специальный модуль, который обеспечивает автоматическую категоризацию почтовых сообщений. Администратор в данном случае выполняет лишь функцию контроля за организацией процесса фильтрации.

Работа с разными языками

Главная сила байесовского фильтра заключается в том, что он может работать с любыми европейскими языками. В предыдущих главах рассказывалось, что "обучение" фильтра осуществляется на основе выборки писем, сделанной в базе почтовых сообщений. При этом не имеет значения, какой используется язык. Основой для анализа являются символы, теги и их сочетания. Байесовский фильтр при их анализе ориентируется на последовательность байт, поэтому даже отдельная буква после анализа будет иметь соответствующий "вес" вне зависимости от ее значения.

Работа с вложениями

Система "Дозор-Джет" работает не только с текстом письма, но и с вложениями. Она может определять практически все используемые в настоящее время форматы и типы данных. Они определяются не по тому, как они продекларированы в MIME-типах, а по бинарному следу, что исключает ошибки при определении формата и типа файлов.

Кроме того, система работает с OLE-объектами файлов-приложений MS Office. Анализ OLE-объектов осуществляется по тому же принципу, что и анализ архивных файлов. Файл рассматривается как контейнер, в который могут входить любые объекты, в том числе в форматах, отличных от MS Office (например, exe-файлы).

Трудности в распознавании могут быть только с сообщениями в виде графических файлов без текста. Однако большинство спам-сообщений распространяется с вложенными файлами формата html. А ведь сам html-код, несущий картинку (и URL рекламируемого сайта в этом коде), и заголовок письма (с IP-адресами, подставными почтовыми адресами и полем "Subject") — все является простым текстом, и этого обычно хватает системе для правильной категоризации. Бывает достаточно одного слова с большим статистическим "спам-весом" для вынесения решения о том, стоит ли блокировать данное письмо. Кроме того, система "Дозор-Джет" имеет возможность выполнять действие "отправить сообщение на обработку третьей программе", чтобы попытаться "заглянуть" и внутрь графического файла. Надо сказать, что необходимость применения данной возможности возникает крайне редко.

Наконец, система "Дозор-Джет" способна раскрывать сжатые файлы всех распространенных типов архиваторов при любом уровне вложенности. Даже если данный архив по какой-то причине не смог раскрыться, осуществляется действие "ошибка при распаковке". Данный файл отправляется в карантин для дальнейшей обработки и принятия решения.

*В «Дозор-Джет» система правил представляет собой практически полнофункциональный язык программирования и позволяет создание модели обработки писем достаточной сложности.

Выводы

Спам давно уже перестал быть просто навязчивой рекламой. Технологии, которые используют спамеры для рассылки почты, небезопасны для корпоративных информационных систем. Они используют вредоносный мобильный код, заражают почтовые системы, используют компьютеры-жертвы для распространения спама.

Проблемы спама могут быть успешно решены только в контексте общей политики информационной безопасности, поскольку комплексное решение задач позволяет бороться с многочисленными угрозами корпоративной информационной системе, которые несет в себе спам.

Система "Дозор-Джет" обладает рядом специфических возможностей, которые делают данную систему эффективной с точки зрения борьбы со спамом. К таким возможностям, в первую очередь, относятся:

- фильтрация спама в рамках политики использования электронной почты;
- применение контекстной фильтрации для категоризации писем;
- эффективное обучение и автоматическая самокорректировка фильтра;
- объединение всех методов фильтрации (по формальным признакам и по содержанию) в едином модуле, возможность их комбинирования;
- централизованное управление всеми правилами фильтрации через единый Web-интерфейс.

Главным показателем качества работы фильтра является низкий уровень ложных срабатываний. В настоящее время система "Дозор-Джет" позволяет отсеивать 98-99% спамерских писем, при уровне ложных срабатываний в 0,001-0,01% (1-10 писем на 100 000). Нужно сказать, что ложные срабатывания у фильтра "Дозор-Джет" обычно вызывают не деловые письма, а пресс-релизы и рассылки с преобладанием рекламной лексики. Значительно снизить риск ложных срабатываний позволяет, так называемый, белый список, то есть "список друзей", в который администратор системы может добавить всю адресную книгу компании, в том числе всех сотрудников, деловых партнеров и т.п.

Другое серьезное преимущество заключается в том, что есть возможность воспользоваться статистикой архива, входящего в состав системы, а это позволяет автоматически анализировать почтовый поток и периодически корректировать работу анти-спам фильтра. Этот факт позволяет назвать систему "Дозор-Джет" самообучающейся. Благодаря этому свойству практически исключены ошибочные срабатывания фильтра и, следовательно, потери важной информации. Кроме того, автоматическая самокорректировка значительно облегчает задачу администратора системы по ее контролю и настройке, а также сокращает время на ее обслуживание.

И, наконец, в отличие от других фильтров, использующих статистическую технологию, данный модуль может применяться не только для борьбы со спамом, но и для фильтрации любых других категорий писем в зависимости от желания пользователя. Кроме того, как было отмечено выше, особенностью данного модуля является возможность индивидуальной настройки фильтра под условия заказчика.

Если сравнивать "Дозор-Джет" с традиционными анти-спам фильтрами, то необходимо отметить, что он одновременно использует как статистические (вероятностные) методы фильтрации, так и фильтрацию спама на основе признаков электронного письма. Это позволяет обеспечить более гибкую и глубокую контекстную фильтрацию и повысить эффективность работы системы по борьбе со спамом.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555