Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 10 (149)/2005

Контентная фильтрация

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Контентная фильтрация

Олег Слепов,
консультант по информационной безопасности

СОДЕРЖАНИЕ

Введение

В последние годы специалисты в области информационной безопасности (ИБ) большое внимание уделяют контентной фильтрации. Происходит это потому, что современные угрозы ИБ невозможно устранить без применения данной технологии. Обоснование этого утверждения является одной из основных целей настоящей статьи. Раскрывая проблемы контентной фильтрации, автор определяет такие подходы к их решению, которые могут быть применимы в локальных вычислительных системах организаций вне зависимости от размеров и сфер деятельности предприятий.

Суть контентной фильтрации заключается в декомпозиции объектов информационного обмена, анализе содержимого этих компонентов, определении соответствия их параметров принятой в компании политике использования Интернет-ресурсов и осуществлении определенных действий по результатам анализа.

Под декомпозицией понимается разбор объекта на составляющие его компоненты. Ясно, что без полного разбора объектов информационного обмена последующие шаги (анализ, определение соответствия параметров политике безопасности и т.п.) потеряют всякий смысл. Если хоть один из компонентов окажется не разобранным или будет разобран некачественно, то анализ не даст объективной картины, поскольку в неразобранном компоненте могут скрываться объекты, представляющие угрозу для информационной безопасности. Например, в случае фильтрации веб-трафика под объектами информационного обмена подразумеваются веб-запросы пользователей, содержимое веб-страниц, передаваемые по запросу пользователя файлы и т.д. Если мы разберем только веб-запрос и убедимся в том, что пользователь «идет» на разрешенный сайт в соответствии со своими правами (что делают большинство современных систем контроля веб-трафика), но оставим без внимания содержимое запрашиваемой им веб-страницы и загружаемых файлов (как чаще всего и происходит!), то мы заранее подвергаем свою систему опасности быть зараженной вредоносным кодом или получить закладку в виде троянской программы либо программы-шпиона. Понятно, что важной составляющей контентной фильтрации в данном случае является комплексность и способность обеспечить фильтрацию по всем компонентам. Но это не означает, что проверять надо «всё и вся». В этом нет необходимости. В проверке должна быть гибкость. Например, чтобы пресечь лишь «походы» пользователей на порнографические сайты, достаточно проанализировать запрос пользователя, установить, не находится ли запрашиваемый URL сайта в категорированной базе URL (которых сейчас появилось большое количество, в том числе и бесплатных), и заблокировать этот запрос.

Когда же речь идет о построении политики использования Интернет-ресурсов, то необходим детальный и многоуровневый анализ всех компонентов. Иначе цель контентной фильтрации, а именно обеспечение контроля содержимого информационного обмена, не будет достигнута.

Таким образом, несмотря на то, что некоторые функции контентной фильтрации реализуемы во многих средствах защиты, только комплексные системы, способные обеспечить фильтрацию по всем компонентам, можно отнести к классу специализированных средств контентной фильтрации.

Прежде чем перейти к описанию этих средств, определим причины, приведшие к появлению данных продуктов.

Современные угрозы и способы борьбы с ними

Время крупных вирусных эпидемий и массовых атак в сети Интернет постепенно заканчивается. Такие действия становятся дорогим удовольствием для их организаторов и в большинстве случаев являются неэффективными.

Кроме того, бизнес стал внимательнее относиться к информационной безопасности. Большую популярность приобретают различные средства защиты, а поскольку есть спрос, есть и предложение. Сегодня рынок средств ИБ предлагает широкий выбор решений и услуг, отвечающих современным требованиям по защите корпоративных сетей.

Однако злоумышленники находят более изощренные методы, тщательнее выбирают цели для атак, используют все более сложные технологии. В целом, приходится признать, что мастерство киберпреступности растет. Вредо-

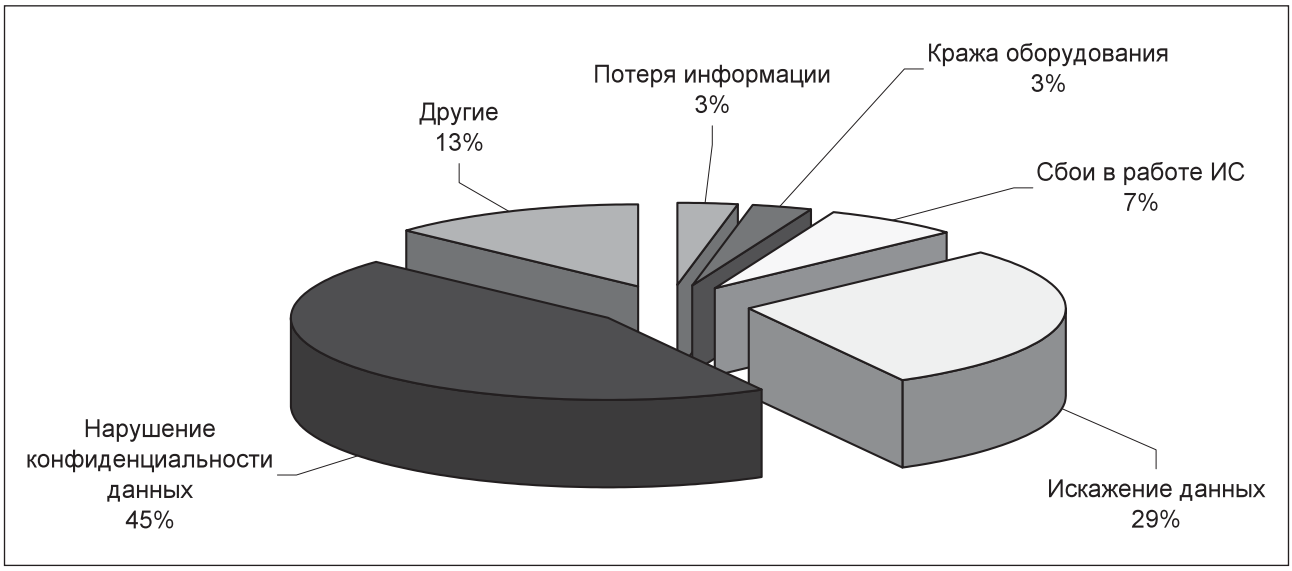

Рис. 1. Внутренние угрозы

носные программы разрабатываются профессиональными программистами, деятельность которых имеет экономическую основу.

В настоящее время главной целью атак злоумышленников является так называемая чувствительная информация: персональная информация пользователей (имена, пароли, аккаунты, идентификационные номера, банковские реквизиты и т.п.) и данные о корпоративных сетях. С помощью такого рода сведений возможен обход многоуровневых систем защиты от вторжений.

Наиболее уязвима инфраструктура безопасности крупных компаний и организаций. Большое количество сотрудников, множество компьютеров, разнородные сети и права доступа — эти дополнительные факторы, облегчают задачу злоумышленникам. В крупной сети зачастую трудно найти даже известный документ, не говоря уж об обнаружении троянской программы, искусно маскирующей свое присутствие в системе.

Атака — это специально выстроенная сложная цепочка взаимосвязанных действий злоумышленников, для осуществления которой применяются различные технологии. Например, чтобы доставить вредоносную программу на компьютер жертвы используются спам-рассылки через специально создаваемые «зомби-сети». Проникновение в систему осуществляют при помощи троянских программ. Некоторые троянцы используют способы проникновения в систему традиционных файловых вирусов (например, вредоносная программа дописывает свой код к файлам легальных приложений — winrar.exe, Explorer.exe и т.п.). Для сокрытия присутствия в системе вирусов широко используются rootkit-технологии и методы внедрения кода вредоносной программы в системные файлы и память, что делает многие антивирусные программы бесполезными в борьбе с вредоносными программами.

Неправомерные действия сотрудников

Сегодня внутренние угрозы являются одной из наиболее актуальных проблем информационной безопасности. Согласно статистике, неправомерные действия сотрудников самих организаций причиняют наибольший ущерб. Однако это обстоятельство пока остается без должного внимания руководителей российских компаний, и до 90% средств, выделяемых на информационную безопасность, тратится на обеспечение защиты от внешних атак.

Неправомерные действия пользователей приводят к значительному ущербу, широко распространенными являются (Рис. 1):

- нарушение конфиденциальности данных;
- кража информации;
- искажение информации;
- действия, приводящие к сбоям информационных систем;
- утрата информации.

Лидирующую позицию в этом списке уже многие годы занимают нарушения конфиденциальности данных, приводящие к утечке закрытой информации. По сведениям специалистов, из 100 случаев неправомерных действий сотруд-

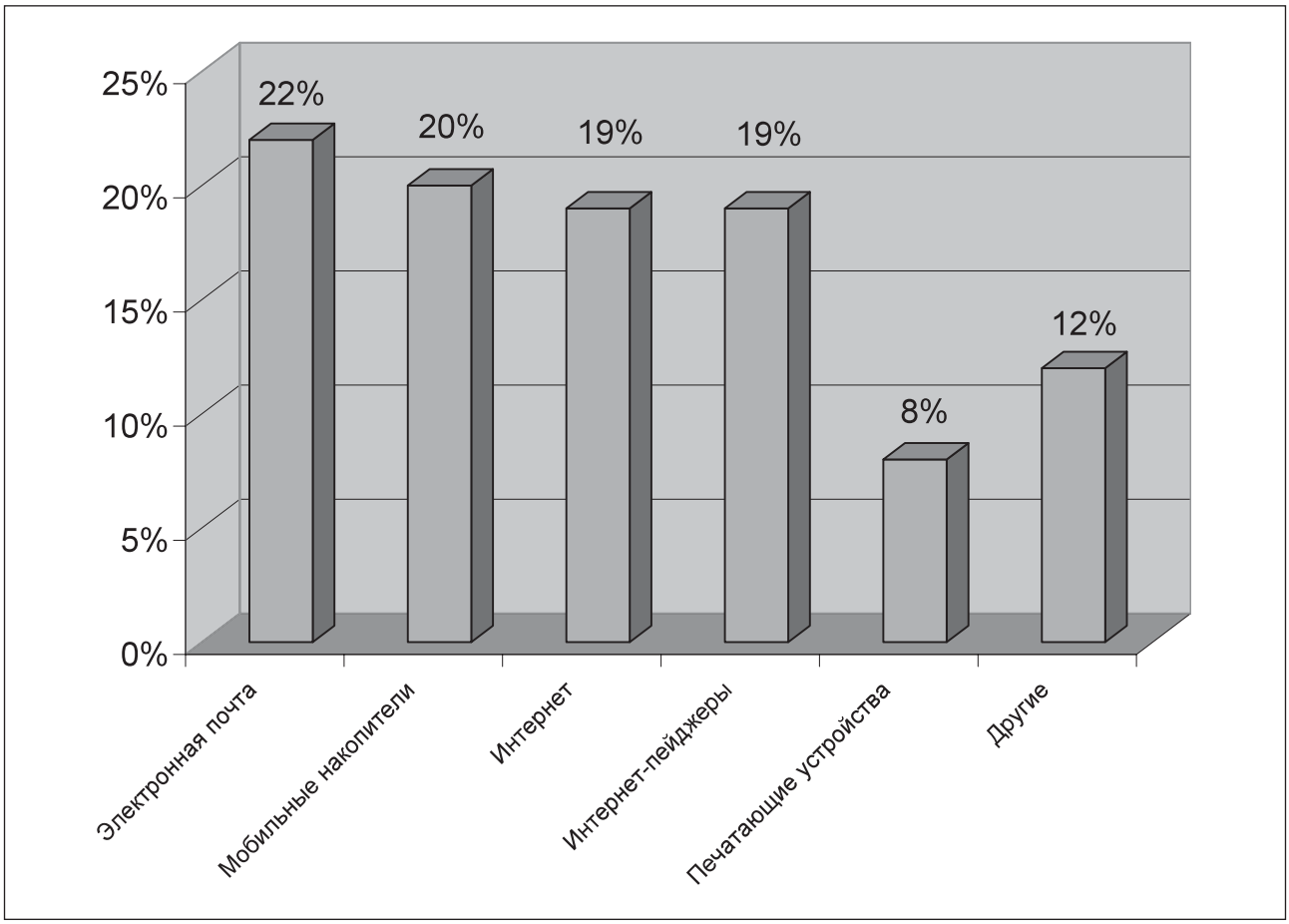

Рис. 2. Пути утечки конфиденциальной информации

ников 65 относятся к нарушению конфиденциальности данных.

Самым распространенным путем утечки информации, согласно статистике, является электронная почта (Рис. 2). Ее доля составляет 22%. Далее следуют соответственно: Интернет (сайты, чаты, форумы, бесплатные почтовые сервисы) — 20%, интернет-пейджеры (ICQ/AOL, AIM, MSN, Yahoo!) и мобильные накопители (компакт-диски, USB-накопители) — по 19%, печатающие устройства — 8% и другие источники данной опасности — 12%.

Первой причиной, приводящей к утечке конфиденциальных сведений, в большинстве случаев является открытый доступ сотрудников к большому объему информации, зачастую не требующейся для выполнения их служебных обязанностей. Вторая по значимости причина — это несвоевременная деактивация электронных аккаунтов сотрудников, уволенных из компании. Третью причину можно назвать косвенной, но она не менее значительна с точки зрения нанесения ущерба: наличие (или разрешение) в компании средств коммуникации, опасных для использования. К таким средствам относятся, например, интернет-пейджеры и бесплатные почтовые сервисы (mail.ru, rambler.ru и т.п.). Кроме того, электронная почта и Интернет, если их использование не регламентируется соответствующими политиками и не контролируется специальными средствами, способны нанести непоправимый ущерб не только корпоративным сетям, но и бизнесу в целом.

Практика показала, что единственным средством борьбы с этим видом угроз являются фиксирование и тщательная проверка содержимого данных, отправляемых сотрудниками внешним адресатам, вне зависимости от того, каким способом осуществляется такая передача информации: электронной почтой, через веб, с использованием интернет-пейджеров и т.п.

Самый распространенный путь утечки конфиденциальной информации — электронная почта. Причем не важно, используется ли в компании собственная корпоративная система электронной почты, услуги, предоставляемые провайдером, или бесплатный почтовый сервис. Ее доля составляет 22% от общего количества случаев утечки данных. Это объяс-

няет то большое внимание, которое уделяется средствам контроля содержимого электронной почты. Такие средства, как правило, устанавливаются «на выходе» из компании и позволяют проводить анализ всего трафика на наличие «запрещенного содержимого».

Основным методом проверки передаваемой информации на конфиденциальность по прежнему является фильтрация по тексту. Содержимое текста позволяет со всей определенностью установить его «запрещенный» характер. Некоторые средства контентной фильтрации обладают такой функциональностью и позволяют эффективно бороться с утечками конфиденциальной информации. Как правило, к таким средствам относятся системы мониторинга электронной почты, контроля веб-трафика и т.п.

Действия пользователей, связанные с нарушением конфиденциальности данных, могут быть как случайными, так и умышленными. В 85% случаев такая утечка происходит случайно, чаще всего из-за неаккуратного обращения пользователей с адресными списками. И только 15% — это целенаправленные неправомерные действия сотрудников.

Борьба с утечками конфиденциальной информации через бесплатные почтовые сервисы проводится путем контентной фильтрации HTTP-трафика. Современные системы контроля веб-трафика обладают достаточной функциональностью, чтобы обеспечить полный контроль над передачей информации внешним адресатам. При этом нет необходимости блокировать весь трафик. Благодаря применению гибких политик, можно разрешать использование ресурсов, однако следует сразу блокировать трафик, если содержание текста является конфиденциальным в соответствии с политикой безопасности компании.

Общение корпоративных пользователей через интернет-пейджеры также должно контролироваться, поскольку приложения типа ICQ, AOL, MSN и AIM способны передавать не только текстовую информацию, но и файлы в виде вложений. А это, в свою очередь, создает потенциальную возможность утечки конфиденциальной информации. Положение усугубляется тем, что применение таких приложений сотрудниками на своих рабочих местах становится обычной практикой, однако должного контроля за их использование нет в большинстве компаний. Хотя рынок информационной безопасности давно предлагает целый ряд средств, способных обеспечивать контроль за действиями сотрудников, использующих интернет-пейджеры, многие работники отделов информационных технологий и информационной безопасности недооценивают необходимость их внедрения. Средства фильтрации обладают способностью не только проверять текст в сообщениях, но и обеспечивать анализ передаваемых файлов. Как и в предыдущих случаях, основной технологией, позволяющей осуществлять проверку данных на наличие конфиденциальной информации, является контентная фильтрация.

Атаки на сети с использованием социальной инженерии

В условиях значительного усиления противодействия вирусным и хакерским атакам злоумышленники вынуждены активно развивать методы социального инжиниринга, позволяющие проникнуть даже на самый защищенный пользовательский компьютер.

Социальная инженерия представляет собой технологию использования человеческого фактора для взлома информационной безопасности. Именно человек является наиболее слабым звеном в системах защиты. Даже если корпоративная сеть оснащена самой совершенной техникой и программным обеспечением, виновником взлома может стать неопытный сотрудник, который поддался на мошеннические действия злоумышленника (Рис. 3).

Один из приемов использования социальной инженерии — методика введения пользователя в заблуждение путем сообщения ему важных для него данных, оказывающихся на самом деле ложными. Среди наиболее ярких примеров подобной методики следует назвать фишинг-атаки.

Фишинг

Фишинг[1] — вид онлайнового мошенничества, целью которого является получение идентификационных данных пользователей. Организаторы фишинг-атак рассылают электронные письма от имени популярных брендов и вставляют в них ссылки на фальшивые сайты. Оказавшись на таком сайте, пользователи рискуют сообщить преступникам информацию сугубо конфиденциального характера.

[1] Термин произошел от словосочетания «ловля и сбор паролей» (password harvesting fishing)

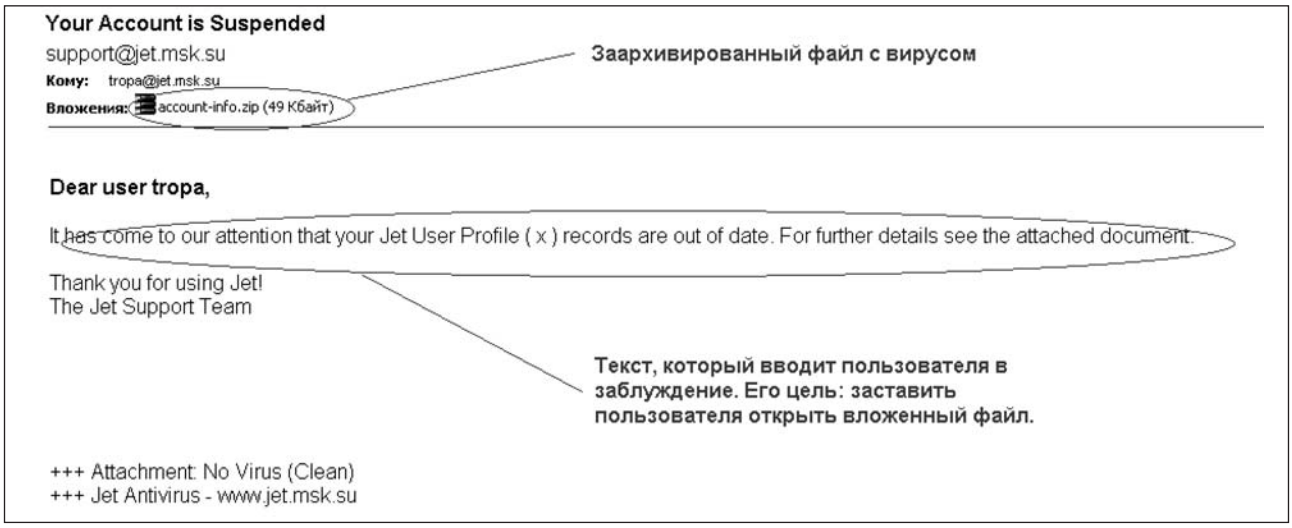

Рис. 3. Пример использования социальной инженерии в рассылке писем с вирусом

В мае 2004 г. владельцы кредитных карт Ситибанка получили письма от «администрации банка» с просьбой уточнить личные данные — номер карты и PIN-код. Поскольку держателей таких карт в России — десятки тысяч, рассылка этих писем была поставлена на поток и проводилась в течение трех месяцев. Мошенники действовали по отработанной схеме: все ссылки из писем вели на фальшивый сайт Ситибанка. В самом Ситибанке утверждают, что ни одного пострадавшего не было. Через несколько дней после начала скандала банк разослал заявление о своей непричастности к хакерской рассылке, подписанное президентом Алланом Херстом. Атаки на Ситибанк продолжались до осени. В конце сентября клиенты банка получили последнее письмо, в котором сообщалось, что на их счет пришла некоторая сумма, и для ее зачисления нужно подтвердить свои реквизиты. В России это был первый случай мошенничества, известного как фишинг.

Чаще всего фишинг-атакам подвергаются пользователи различных банковских и платежных систем. Злоумышленники рассылают им письма с троянскими программами, осуществляющими кражу банковских реквизитов, номера и PIN-коды платежных карт и другие персональные данные. Не остаются без внимания преступников даже происходящие в мире трагедии. Декабрьское цунами 2004 г. в Юго-Восточной Азии, унесшее жизни сотен тысяч людей, вызвало внедрение многочисленных вирусов и краж конфиденциальной информации. Были зафиксированы рассылки троянских программ, выдаваемых за «фотографии цунами», «секретные отчеты о численности жертв» и т.п.

Фишинг-атаки осуществляются следующим образом: предварительно злоумышленники подготавливают сайт-двойник или специальный сайт с вредоносной страницей[2]. Затем при помощи так называемых ботнетов[3] осуществляется массированная спам-рассылка электронных писем и сообщений для интернет-пейджеров, призывающих получателя зайти на подготовленный инфицированный сайт. Рассылка может быть осуществлена не только по электронной почте, но и при помощи других средств коммуникации, например, через интернет-пейджеры.

Статистика: в декабре 2004 г. количество активных подставных сайтов, используемых фишерами, составило 1,7 тыс. Большинство из них имели хостинг на территории США. Средняя продолжительность жизни подставного сайта равна 5,9 суток, а максимальное время составляет 30 суток.

Чтобы заманить пользователей на зараженный сайт, необходимо добиться, чтобы они поверили полученному сообщению. Здесь вступает в действие технология социальной инженерии. Текст письма составляется так, чтобы у читающего не возникло сомнений в правдивости написанного. Предложения, содержащиеся в нем, создают мотивированную реакцию пользователей. В данном случае такой реакцией является посещение сайта по указанной в письме

[2, 3] См. стр. 8

ссылке. При этом злоумышленник, как правило, подменяет DNS на целевой сайт (DNS poisoning) или каким-либо другим способом перенаправляет сетевой трафик[4], чтобы скрыть истинный адрес взломанного сайта.

Затем на сайте пользователю предлагается ввести персональную информацию (банковские реквизиты, пароли, PIN-коды и т.п.) или изменить пароль для онлайновых операций в целях безопасности. Таким образом, в руках злоумышленников окажутся персональные данные пользователей банковских систем. Дальнейшее их применение с целью кражи финансовых средств со счетов становится «делом техники».

Основой защиты от фишинг-атак является, как это ни покажется странным, «обучение» пользователей. Ведь принесло же свои плоды антивирусное просвещение пользователей, позволившее значительно снизить ущерб от атак почтовых червей! Своевременное и полное информирование сотрудников о данной угрозе и о необходимости тщательной проверки источника запроса конфиденциальных или персональных данных устранит основное условие существования фишинг-атак. С этой целью в компаниях вводится специальная политика, которая регламентирует действия пользователей, получающих подобные письма.

Другой способ борьбы с фишингом — предотвращение проникновения писем атакующей стороны в корпоративную сеть. Этого можно добиться с помощью специализированных средств контентной фильтрации, таких как анти-спам-фильтры, системы контроля электронной почты, фильтры, обеспечивающие фильтрацию сообщений интернет-пейджеров и т.п. Данные системы выделяют из потока фишинг-сообщения, применяя следующие способы:

- Блокирование спама. В большинстве случаев фишинг-сообщения распространяются с помощью массированных спам-атак через каналы электронной почты и средства диалогового обмена сообщениями (интернет-пейджеры). При этом применяются различные технологии определения спама.
- Проверка содержимого писем на наличие признаков фишинг-сообщений.
- Проверка наличия адреса сайта в списках «фальшивых» веб-ресурсов. Данные списки составляются компаниями-производителями средств контентной фильтрации и антивирусов и распространяются по подписке наряду с другими базами данных.
- Применение технологии анти-спуфинга (anti-spoofing), то есть создание системы аутентификации интернет-адресов для проверки соответствия введенного пользователем адреса настоящему серверу. Данная технология повзоляет бороться с подменой DNS на целевой сайт или другими способами перенаправления сетевого трафика.
- Эвристический анализ. Позволяет выявить в поступившем пользователю сообщении признаки, совокупность которых дает возможность установить принадлежность к фишинг-атаке. (Например, установить факт того, что сайт является незаконным, возможно по расположению сервера с сайтом, на который указывает ссылка в письме, за пределами зоны Рунета, хотя пользователь и организация, куда он обращается, являются российскими).

Антивирусная фильтрация и проверка на наличие шпионских программ позволяют значительно снизить уровень воздействие фишинг-атак на сеть. Целью многих подобных атак является установка на компьютере пользователя троянцев или программ-шпионов, дающая возможность злоумышленнику в последующем получить доступ к персональным данным пользователя. Поэтому средства, которые способны

[2] Взламывается, как правило, какой-нибудь относительно популярный веб-сайт. Известность подобного сайта играет немаловажную роль в привлечении к нему внимания пользователей. Кроме того, сайт с вредоносной страницей может быть создан на любом доступном хостинге. На практике подобные сайты существуют недолго: их закрывают сами хостинг-провайдеры при полученни запроса от антивирусных компаний или правоохранительных органов. Третий способ создания вредоносного сайта — это заражение сервера владельца сайта или хостинговой компании с последующим доступом к аккаунтам для управления взломанными сайтами.

[3] «Ботнет» или «зомби»-сеть — сеть из зараженных компьютеров и серверов, централизованно управляемых злоумышленниками. Существуют различные способы создания таких сетей: в основном, для проникновения на компьютер-жертву применяются различные уязвимости в системе Windows, способы подбора паролей к открытым на доступ сетевым ресурсам, а также рассылка почтовых червей, которые открывают на зараженной системе определенные порты и позволяют злоумышленнику получить полный доступ к системе. В дальнейшем «ботнеты» используются для рассылки спама, организации DoS-атак, а также распространения вредоносных программ. По оценкам специалистов, в настоящее время общее количество компьютеров, входящих в какой-либо «ботнет», составляет несколько миллионов, а их число ежемесячно увеличивается на 300-350 тысяч.

[4] Метод, часто называемый фармингом, от английского слова pharming.

выявлять вредоносный код, являются неотъемлемой частью системы безопасности, предназначенной для защиты от фишинга.

Фарминг

Фарминг — метод хищения идентификационных данных интернет-пользователей. Суть его сводится к автоматическому перенаправлению пользователей на фальшивые сайты. В отличие от фишинга, этот способ хищения данных почти не требует участия потенциальной жертвы. Пользователи могут стать жертвой фарминга в силу уязвимостей браузеров, операционных систем и DNS-серверов. Механизм фарминга вступает в действие, когда жертва открывает почтовое сообщение с троянской программой (как правило, рассылаемое по спамерским спискам) или посещает веб-узел с исполнимым файлом, который тайно запускается в фоновом режиме.

Когда пользователь набирает интернет-адрес, чтобы получить доступ к веб-странице, адрес должен быть конвертирован в реальный IP-адрес в следующем формате: 000.000.000.000. Обычно требуется DNS-сервер, так как браузер не может совершить конвертацию. Эти серверы администрируют имена, соответствующие каждой из таких цифровых последовательностей и доставляют пользователя на запрашиваемую страницу.

Атаки фарминга могут проводиться напрямую против DNS-сервера таким образом, что изменение адреса повлияет на всех пользователей, обращающихся к серверу, или они могут быть выполнены локально, т.е. на отдельных компьютерах. Последний способ предполагает изменение на компьютерах, работающих под управлением ОС Windows файла hosts. Здесь хранится информация о серверах и соответствующих им IP-адресах, наиболее часто используемых, чтобы не нужно было обязательно обращаться к DNS-серверу для конвертации интернет-адресов (URL) в IP-адреса. Если этот файл перезаписан, и в него вносятся фальсифицированные адреса страниц, то каждый раз, вводя имя сайта в браузере, пользователь попадет на страницу, созданную хакером, которая выглядит так же, как истинная страница. Ничего не подозревающая жертва затем может ввести конфиденциальные данные. При этом злоумышленник имеет возможность редактировать hosts-файл напрямую (осуществляя удаленный доступ к системе) или используя вредоносный код, обычно — троянцев.

При пользовании браузером надо принимать дополнительные меры безопасности для защиты от фарминг-атак. Они должны включать подтверждение всех интернет-адресов, набранных в строке браузера. Необходимы протоколы аутентификации, согласно которым каждый веб-сайт будет публиковать свой IP-адрес для проверки его браузером. Другими словами, предлагается ввести инструмент, подобный уже созданным протоколам аутентификации почтовых электронных сообщений. Кроме того, следует создать протоколы идентификации веб-ресурсов, аналогичные тем, что используются при идентификации электронных почтовых адресов. Усложнение процедуры идентификации пользователя при работе с онлайновыми формами регистрации дает дополнительную гарантию защищенности.

Принимая во внимание имеющиеся на рынке информационной безопасности продукты, наиболее эффективными средствами борьбы с фармингом можно назвать антивирусные системы, а также межсетевые экраны, средства контроля содержимого электронной почты и анти-спамерские программы. Антивирусные системы выполняют главную задачу — осуществляют поиск троянских программ, межсетевые экраны детектируют подозрительную активность, происходящую на компьютерах, средства контроля электронной почты обеспечивают мониторинг подозрительных писем, анти-спамерские программы предотвращают поступление пользователям спама, в котором содержится вредоносный мобильный код.

Вредоносные программы

Вредоносные программы включают в себя вирусы, черви, троянские программы, а также различные скрипты и исполнимые программы.

Черви

Почтовые черви — это вредоносные программы, которые распространяются по каналам электронной почты во вложениях к почтовым сообщениям. Они запускаются при открытии пользователями вложенных файлов и используют уязвимости в почтовых клиентах. Почтовые черви снабжены механизмами саморазмножения и используют для распространения списки рассылки почтовых клиентов.

В настоящее время эпидемии почтовых червей происходят значительно реже. Это объясняется активной деятельностью антивирусных компаний, стараниями производителей ПО, постоянно пытающихся найти и закрыть уязви-

мости в своих операционных системах и прикладных программах, возросшим уровнем подготовленности ИТ-специалистов, а также просветительской работой, проводимой среди пользователей. Однако на замену почтовым червям приходят черви для интернет-пейджеров (IM-черви, Instant Messaging) и файло-обменных сетей (P2P-черви, peer-to-peer), защищенных гораздо хуже современных почтовых программ.

Распространение IM-червей осуществляется следующим образом: на атакуемые компьютеры рассылаются (как правило, по записям контакт-листов заранее взломанных интернет-пейджеров) сообщения, содержащие ссылку на специально подготовленный веб-сайт. Используя технологию социального инжиниринга, злоумышленник заставляет пользователя пойти по указанной ссылке. На сайте находится вредоносная программа. В момент ее загрузки червь (либо через эксплойты различных уязвимостей в Internet Explorer и клиентах интернет-пейджеров, либо путем прямой загрузки и запуска) проникает в систему.

Инсталляция P2P-червей на компьютер-жертву осуществляется в момент закачки файлов по файло-обменной сети. При этом вредоносные программы внедряются в загружаемый файл и используют различные способы маскировки, чтобы не быть замеченными в момент передачи данных.

Большинство P2P и IM-червей способны устанавливать в систему и другие вредоносные программы. Так, например, существуют черви, устанавливающие троянские программы на зараженные компьютеры. С помощью троянцев с компьютера жертвы осуществляется кража конфиденциальной информации или персональных данных. Сам же компьютер превращается в «зомби-машину» и включается в «ботнет».

Политика безопасности является необходимым атрибутом любой продуманной стратегии защиты от червей. Продуманная и внедренная на административном уровне политика позволяет уменьшить риск заражения вредоносной программой в несколько раз. Простой пример — запрет на открытие вложенных файлов из электронных писем снижает риск заражения почтовыми червями практически до нуля.

Наиболее эффективными средствами борьбы с червями являются антивирусные программы, которые активно используют технологию контентной фильтрации. В частности, благодаря детектированию червей в запакованных и архивных файлах (в том числе закрытых паролями), а также применению различных способов предварительного анализа сообщений с исполняемыми файлами, удается перехватывать зараженные письма на самых ранних стадиях распространения. Сегодня для борьбы с червями широко применяются различные методики борьбы со спамом (или spim), поскольку все последние массовые атаки производились при помощи спам-рассылок.

Троянские программы

Падение интереса к вирусам и почтовым червям объясняется не только повышением эффективности защитных средств и просветительской работой среди пользователей (что, конечно же, приносит ожидаемые плоды), но и возросшей среди киберпреступников популярностью троянских программ. Соображения тут чисто экономические: авторам троянских программ нет необходимости разрабатывать механизмы саморазмножения, поэтому создание программы удешевляется, сокращаются сроки этой работы. Кроме того, уменьшается размер программы, что облегчает рассылку троянцев.

Троянские программы интенсивно используются злоумышленниками для осуществления атак на корпоративные сети. В зависимости от задач, которые выполняют троянские программы, различают соответственно: троянцы-шпионы и бекдоры (от английского trojan-backdoor — «черный ход»), предназначенные для кражи конфиденциальной информации и персональных данных, рассылки спама и осуществления атак типа «отказ в обслуживании»; троянцы-прокси, используемые злоумышленниками для построения «ботсетей»; уведомляющие троянцы, (от английского Trojan-Notifier), сообщающие злоумышленнику о том, что компьютер инфицирован; троянцы-загрузчики (от английского downloader), целью которых является установка и постоянное обновление вредоносных программ на инфицированных машинах; PSW-троянцы (от английского password), используемые для поиска, а также кражи паролей и кодов доступа. Основным способом распространения троянских программ являются массовые спам-рассылки, а также почтовые и IM-черви.

Борьба с «троянскими конями» эффективно ведется с помощью антивирусного программного обеспечения, работающего как на сетевом, так и на пользовательском уровнях. Эти средства обнаруживают большинство троянцев и пресекают их распространение. Основными методами их обнаружения являются: проверка сигнатуры кода, эвристический анализ и блокировка подозрительного поведения программ.

Однако необходимо иметь в виду, что для сокрытия своего присутствия в системе некоторые троянские программы применяют специальные stealth-технологии, благодаря которым их действия практически незаметны для антивирусных средств. Примером является так называемая rootkit-технология[5].

Кроме того, существуют троянские программы, для которых практически невозможно создать эвристические методы детектирования, а разовость их применения дает им шанс никогда не попасть в антивирусные базы — в отличие от червей, расходящихся по миру миллионами копий.

Потенциально опасные программы

В последнее время специалисты в области информационной безопасности проявляют серьезную тревогу по поводу применения программ, относящихся к классу «riskware» или «greyware» («потенциально опасные программы»). С одной стороны, они являются легитимными и созданы во благо, с другой — в руках злоумышленников могут причинить значительный вред информационной системе. Сюда входят: программы дозвона (dialers), программы-загрузчики (для скачивания файлов из Интернета), IRC-клиенты, FTP-серверы, серверы-посредники (proxy), telnet-серверы, web-серверы, программы мониторинга, PSW-утилиты, утилиты удаленного администрирования и т.п.

Полезность всех вышеназванных программ и утилит трудно переоценить, некоторые из них даже поставляются по умолчанию с операционными системами и различного рода приложениями. Однако в связи с коммерциализацией Интернета их начали (сначала легально) использовать, например, в поисках информации о предпочтениях пользователей в целях маркетинга, для продвижения собственных сетевых ресурсов любыми доступными средствами (в том числе с помощью фальсификации результатов поиска в Интернет). Затем злоумышленники стали применять эти программы в целях сбора и кражи конфиденциальных и персональных данных, изменения и уничтожения информации и т.д.

Программы-шпионы

Среди потенциально опасных особенно выделяются программы-шпионы (spyware). Данное программное обеспечение позволяет собирать сведения об отдельном пользователе или целой организации без ведома тех, за кем ведется слежка.

Первыми такими программами были сетевые сниферы. Снифер представляет собой программу-жучок, который следит за действиями пользователя и протоколирует все, что видит. Спрос на сниферы довольно устойчивый. Набор таких программ представлен в Сети в богатом ассортименте — тут и софт для протоколирования сообщений ICQ в локальной сети, и средства контроля электронной почты, и инструменты отслеживания вводимых паролей.

Spyware — это, по сути, тот же снифер, только устанавливается он объектом слежки на свой компьютер добровольно. Среди программ-шпионов выделяют следующие типы:

- **Считыватели клавиатуры (монитора) — key/screen loggers.** Специальные программы, обеспечивающие сбор и отправку информации, которую пользователь набирает с клавиатуры (выводит на экран).
- **Сборщики информации.** Программы-шпионы, которые осуществляют поиск на жестком диске определенных данных (пароли, персональные данные, конфиденциальную информацию и т.п.) и отправку их внешнему адресату.
- **Программы-загрузчики.** Специальный код, позволяющий проделать бреши в системе защиты и загружать на инфицированный компьютер дополнительные вредоносные программы.

Такие программы распространяются разными способами, но чаще всего — массовой спам-рассылкой. В этом случае можно выделить два варианта: одноэтапный и двухэтапный. Для первого характерно, что в качестве распространяемого спам-рассылкой файла выступает одна из разновидностей шпиона, во втором — сначала на компьютер-жертву устанавливается троянская программа-загрузчик, которая затем осуществляет загрузку одной или нескольких шпи-

[5] Термин rootkit, который сейчас часто используется для обозначения stealth-технологий, применяемых авторами троянских программ под Windows, пришел из мира UNIX. Изначально он обозначал набор программ, позволяющих хакеру закрепиться на взломанной машине и предотвратить свое обнаружение. Для этого подменяются системные исполняемые файлы (login, ps, ls, netstat и т.п.) или системные библиотеки (libproc.a), либо устанавливается модуль ядра — все с той же целью: перехватить попытки пользователя получить истинную информацию о том, что происходит на его компьютере.
В последнее время использование rootkit-технологий для сокрытия присутствия вредоносного ПО становится все более популярным, что подтверждается стабильным ростом количества обнаруживаемых новых rootkit-программ.

онских программ рассматриваемой группы. Другой способ распространения — с почтовыми червями. Такие черви, попадая на компьютер, либо сами загружают шпионскую программу, либо устанавливают на инфицированной машине троянца-загрузчика, который впоследствии осуществляет инсталляцию шпионского ПО. Некоторые версии программ-шпионов используют для распространения HTTP и FTP-трафики.

Все вышеперечисленные способы распространения программ-шпионов объединяет одна, пожалуй, главная причина — неправомерные и небезопасные действия пользователей. Как правило, spyware пападают во внутренние корпоративные сети:

- путем пересылки во вложениях к электронной почте;
- через уязвимости в интернет-браузерах, при загрузке вредоносного содержимого с инфицированного сайта;
- через уязвимости в IM и P2P-клиентах;
- с мобильными накопителями (компакт-диски, USB-накопители);
- во время on-line игр.

Очевидно, что с потенциально опасными программами надо бороться, но делать это необходимо корректно. Например, если заставить каждую штатную anti-spyware программу реагировать на любую потенциально опасную программу, то пользователь столкнется с массой ложных срабатываний, поскольку многие представители класса riskware поставляются по умолчанию с операционной системой. Часто такого рода утилиты бывают очень полезны. Примером может служить программа telnet, без которой сегодня трудно представить ОС Windows, Unix и Linux.

Наиболее корректно применение отдельных утилит в составе специализированных anti-spyware программ. По умолчанию данные утилиты выключены, а при необходимости системный администратор может их включить.

Борьба с программами-шпионами должна вестись постоянно. Вне зависимости от того, установлена в системе anti-spyware или нет, необходимо регулярно проверять жесткие диски корпоративных пользователей на наличие потенциально опасных программ. Если они есть на компьютере, то администратору придется в каждом отдельном случае принимать решение о том, является ли данная программа вредоносной. Есть несколько параметров, влияющих на такое решение: устанавливал ли пользователь ее самостоятельно, или она поставляется в составе операционной системы, существовала ли какая-нибудь подозрительная активность данной программы и т.п. После проведения такой инспекции необходимо поставить под контроль установку всех новых программ и на постоянной основе осуществлять мониторинг активности утилит данного класса.

Пути защиты от программ-шпионов:

1. Блокировка доступа к инфицированным сайтам. Многие специализированные средства борьбы с программами-шпионами и антивирусные программы имеют в своем составе базы данных соответствующих ресурсов в сети.
2. Контроль за действиями пользователей, обеспечивающий инсталляцию и применение только авторизованного программного обеспечения.
3. Фильтрация HTTP, FTP, SMTP трафиков, мониторинг использования IM и P2P-приложений с целью блокировки загрузки потенциально опасных программ в момент передачи данных по каналам Интернета.
4. Анализ и блокировка подозрительной активности программ.

Spyware — это не одна, а совокупность нескольких угроз, поэтому требуется многоуровневая защита, которая должна предусматривать введение в компании политики безопасности, обучение пользователей, постоянный мониторинг всех процессов, происходящих в корпоративной сети, внедрение как по периметру корпоративной сети, так и на отдельных рабочих станциях средств защиты от программ-шпионов. К таким средствам относятся: межсетевые экраны, входящие, как правило, в их состав системы предотвращения вторжений (Intrusion prevention systems), антивирусные программы, а также специализированные программы-детекторы.

Рекламные коды

Рекламные коды (adware) — это программное обеспечение, которое проникает на компьютер в рекламных целях. Данное ПО относится к разряду потенциально опасных. Формально adware-программы являются легальными, что позволяет производителям открыто их разрабатывать, а рекламным компаниям — свободно распространять. Появившись несколько лет назад в виде простейших скриптов, автоматически открывавших множество дополнительных окон в браузере, сейчас они окончательно перешагнули грань между нежелательным, но все-таки легальным, софтом и вредоносными программа-

ми. Сегодня рекламные компании стремятся всеми доступными средствами выполнить заказ и показать рекламу как можно больше раз максимальному количеству пользователей.

Более изощренными и нелегальными становятся приемы доставки рекламного контента на компьютеры пользователей. Некоторые современные adware-программы используют вирусные технологии для проникновения и скрытия себя в системе. Все больше обнаруживаемых программ данного класса содержат черты троянцев. Это отражается в способе инсталляции в систему (например, при помощи уязвимостей в браузерах) либо в поведении на компьютере пользователя. Adware-программы серьезно затрудняют свое обнаружение и деинсталляцию из системы (rootkit-технологии, запись собственного кода в системные файлы или подмена собой системных приложений), ищут и удаляют программы-конкуренты, занимая их место. В них могут содержаться модули для сбора и отправки третьим лицам информации о посещаемых сайтах и вводимых владельцем компьютера данных. Кроме того, представители класса adware могут конфликтовать с установленным программным обеспечением, а это, в свою очередь, чревато серьезными негативными последствиями для информационной системы.

Еще одним свойством adware-программ является подмена результатов поиска. По результатам действий они имеют сходство с вредоносным кодом, осуществляющим фарминг-атаки. Используя уязвимости в браузерах, такие программы перенаправляют пользователя на нужный рекламодателю сайт вне зависимости от того, какой адрес интернет-ресурса он набрал.

Технические средства борьбы с adware существуют. В большинстве случаев помогает применение программ-чистильщиков. Антивирусные же средства не помогают, поскольку adware — не вирусы, они не распространяются самостоятельно. Надеяться на законодательный запрет таких программ тоже не приходится, так что детектирование adware-программ — довольно сложная задача, поэтому они могут очень долго существовать на компьютере пользователя.

Единственно эффективное противодействие состоит в соблюдении правил личной компьютерной гигиены. О наличии spyware на своей машине пользователь может и не догадываться, но adware не заметить невозможно. Данный софт, распространяющийся точно так же, как и программы-шпионы, подвергает пользователя принудительной демонстрации рекламы. Этим и надо пользоваться. После появления такой рекламы необходимо постоянно запускать программы-чистильщики, которые локализуют adware-программу. Кроме того, помощь в детектировании рекламных кодов могут оказать межсетевые экраны, способные установить отправку третьим лицам информации о посещаемых сайтах и вводимых владельцем компьютера данных.

Спам

В последние годы специалисты в области информационной безопасности начали заниматься, казалось бы, не свойственной им задачей: бороться со спамом. Дело в том, что такие рассылки наносят серьезный ущерб информационным системам. Если во времена своего появления спам был просто назойливой рекламой, то сегодня он составляет отдельный и крайне опасный вид угроз.

> По данным ведущих отечественных провайдеров, объем спама в русском сегменте Интернета на конец 2004 г. составлял 75-80% от общего количества входящей электронной почты. Ущерб от спама в России в этом же году составил более 150-200 млн евро.

Распространение спама приобрело угрожающие масштабы. С начала 2005 г. его рост превзошел самые пессимистичные прогнозы, дававшиеся в конце прошлого года. Если в конце 2002 г. спам составлял 30-40% от общего числа электронных писем в мире, то уже в 2003 г. его доля превысила 50%. По сведениям ведущих провайдеров России, к концу 2004 г. 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 впечатляющи. По разным оценкам, на спаме предприятия теряют от $50 до $200 в год в расчете на одного офисного сотрудника. В результате в 2003 г. ущерб от спама по порядку величины стал сравним с потерями, нанесенными мировому сообществу компьютерными вирусами и хакерами. По данным европейских источников, убытки во всем мире составляют $10 млрд ежегодно. В России этот показатель оценивается в 150-200 млн евро.

И наконец, самое печальное — сегодня при помощи спам-рассылок осуществляется основная масса атак на сети. Такие рассылки являются наиболее распространенным способом до-

ставки вредоносных и потенциально опасных программ, фишинг-атаки также проводятся с использованием спама. Все это ставит спам во главе всех вышеперечисленных угроз!

Эволюция способов рассылки спама определялась совершенствованием средств фильтрации. Как только один из методов рассылки начинает преобладать, появляются эффективные средства борьбы с ним, и спамерам приходится менять технологию. В результате, сегодня спам-почта (по меньшей мере, спам, нацеленный на российский рынок) имеет ряд технологических особенностей.

- **Распределенность спам-рассылок.** Существенная доля спам-сообщений рассылается через «ботнеты». Как правило, отдельный инфицированный компьютер используется для посылки небольшой доли сообщений, при этом в рассылке участвуют сотни и тысячи пользовательских машин. Спамерам удалось наладить сквозной мониторинг доставки сообщений, в результате письмо, отвергнутое при попытке доставки с одного IP-адреса, отправляется заново только с другого IP. Это делает отражение (reject) почты по DNSBL-спискам[6] неэффективным — попытки доставки сообщения повторятся с других IP-адресов.
- **Уникальность спам-сообщений.** Спам-сообщения, рекламирующие один и тот же товар или услугу, но отправленные разным пользователям, уникальны. Другими словами, в каждое отдельное письмо вносятся случайные последовательности символов (часто невидимые для читателя), персональные обращения, анекдоты, большие куски связного текста и так далее, что делает спам-сообщения невидимыми для фильтров, основанных на технологии проверки сигнатуры или одинакового текста. Случайные последовательности символов добавляются автоматически, с применением специализированных программ[7]. В противном случае стоимость и время изготовления индивидуальных сообщений будут слишком большими.
- **Маскировка 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.

К другим особенностям относятся:

- Использование технологии социальной инженерии. Уже не секрет, что тексты спамерских писем составляются специалистами в области психологии.
- Использование технологий обхода антиспам-фильтров. Появление средств обнаружения спама, основанных на анализе содержания письма (контентный анализ), привело к эволюции содержания спамерских писем — их составляют таким образом, чтобы автоматический анализ был затруднен. Кроме того, спамеры стараются фальсифицировать адреса отправителя, заголовки писем, модифицировать сообщения так, чтобы обмануть антиспамерские фильтры. Рекламное сообщение приходит пользователю в виде графического файла, а это крайне затрудняет автоматический анализ.

Борьба со спамом

Каждый из методов борьбы со спамом, особенно сразу после появления, достаточно эффективен, однако ни один из них не является «абсолютным оружием». Технически возможно сделать абсолютно «легальное» (с точки зрения рассматриваемых методов) спам-сообщение. Поэтому воспринимать маркетинговые заявления компаний-производителей о том, что их средства способны блокировать до 99,9% спама, необходимо с осторожностью.

Главное — понять, что со спамом можно бороться достаточно эффективно. Но для этого недостаточно использовать лишь одну технологию или метод фильтрации. Необходимо применять комплексный подход, включающий целый ряд мер не только технического, но и организационного характера. Борьба со спамом должна быть частью корпоративной политики безопасности. Подбор средств фильтрации должен отвечать общекорпоративным задачам.

Обнаружить спам помогают следующие моменты:

- Спам-сообщение содержит информацию (рекламу) от заказчика рассылки, то есть произвольного текста в нем быть не может, там будет описан рекламируемый продукт или услуга.
- Спам-сообщение должно легко читаться. Оно не может быть зашифровано, основной объем содержится в составе сообщения. Количество случайных последовательностей («мусора»), видимых пользователем, долж-

[6] DNSBL-DNS Black lists — черные списки доменных имен Интернета. Содержат базу адресов, наиболее часто используемых спамерами.

[7] Данный метод получил название obfuscating text — буквально «текст, сбивающий с толку».

но быть небольшим. При нарушении этих правил снижается читаемость, а следовательно, и отклик на рекламу.

Среди основных технических средств, обеспечивающих фильтрацию спама, наиболее эффективными являются специализированные антиспам-фильтры и системы контроля электронной почты. При этом последние, как правило, имеют в своем составе отдельные модули, позволяющие рассматривать спам как одну из категорий писем, которые необходимо определить и отфильтровать.

Интернет-пейджеры

Интернет-пейджеры (в английской терминологии Instant messaging, далее сокращенно – IM) – это средства диалогового обмена сообщениями. К таким средствам относятся:

- AOL (AOL IM – AIM, AIM Express (web-based), Trillian, Apple iChat, SameTime Connect, как правило, использует для соединения tcp 5190-5193);
- ICQ[8] (ICQPro, ICQ Lite, ICQ2GO (web-based);
- Microsoft (MSN Messenger, Windows Messenger, Trillian, как правило, использует для соединения tcp 1863, tcp 6891);
- Yahoo! (Yahoo! Messenger, Yahoo! Web Messenger, Trillian, как правило, использует для соединения tcp 5050).

Существуют две модели интернет-пейджеров: первая построена на классической «клиент-серверной» архитектуре и предполагает, что клиент подключаясь к IM-серверу, после аутентификации получает возможность обмениваться сообщениями или данными с другими клиентами, которые подключены к данному серверу. Вторая предполагает поддержку архитектуры «клиент-клиент» (связь между равноправными узлами, в английской терминологии peer-to-peer, далее сокращенно P2P). Обмен ведется не только текстовыми сообщениями (как это было в самом начале развития данного сервиса), но и файлами, в том числе большого объема. В настоящее время с помощью IM-клиентов также возможна поддержка потокового аудио и видео (в том числе видеоконференцсвязь), on-line игр и даже компьютерной телефонии.

Использование интернет-пейджеров сотрудниками является небезопасным. Так как наличие уязвимостей в IM-клиентах (активные элементы ActiveX, эксплойты JPEG-файлов и т.п.) позволяют злоумышленникам похищать пароли и конфиденциальную информацию, получать несанкционированный доступ к внутренним корпоративным сетям, а также устанавливать троянские программы, которые дают возможность удаленно управлять компьютером или сервером в собственных целях, включать его в «ботсеть», рассылать через него спам и вредоносные программы.

Как спам, рассылаемый по каналам электронной почты, является серьезной проблемой для безопасности корпоративных сетей, точно также спим[9] становится угрозой номер один для интернет-пейджеров. Подобно своему собрату спим является не только свободно распространяемой рекламой, но и способом рассылки вредоносных программ через IM-канал. Именно поэтому борьба со спимом также актуальна сегодня, как и защита от вирусов и червей.

Важнейшей особенностью IM-сетей является то, что в настоящее время не существует каких-либо общих стандартов и протоколов, описывающих их архитектуру[10]. При этом из-за жесткой конкуренции между основными игроками на рынке развитие IM-сетей и их возможностей происходит поражающими темпами. Это осложняет контроль использования данных приложений на корпоративном уровне. Межсетевые экраны и прокси-серверы не в состоянии обеспечить должный контроль IM-трафика. Последние версии IM-клиентов способны, например, добавлять HTTP-заголовки к каждому передаваемому пакету, обманывая фильтры протоколов межсетевых экранов. Более того, очень частый выпуск обновлений IM-протоколов и клиентов (практически каждый месяц) не позволяет компаниям, производителям анти-вирусных программ выпускать соответствующие продукты, способные обеспечивать защиту от вредоносных программ (IM-червей, троянцев и т.п.).

Существует еще одна проблема на пути обеспечения безопасного обмена данными по IM-сетям – это появление множества других сетей и IM-клиентов. Среди них можно назвать Trillian (для ОС Windows), Fire (для ОС Mac) и даже очень популярный в open-source-среде кросс-платформенный gaim и другие клиенты.

[8] «I seek you», наиболее распространенная в России сеть

[9] Рекламные сообщения, распостраняемые по IM-трафику, называются SPIM (unsolicited instant messages, по аналогии со SPAM). Объемы SPIM всего 5% от IM-трафика, но он увеличивается с ростом популярности данного вида коммуникации.

[10] См. стр 16

Интернет предлагает большое количество различных бесплатных продуктов, обеспечивающих обмен данными по IM-сетям.

Необходимо также отметить, что популярность IM-клиентов «произвела на свет» множество вспомогательных утилит для них, которые содержат нежелательные с точки зрения обеспечения безопасности компоненты, создавая в IM-приложениях дополнительные уязвимости.

Таким образом, поскольку контроль использования IM-клиентов является в настоящий момент трудно осуществимой задачей, поэтому, по мнению автора статьи, общение корпоративных пользователей посредством IM-сетей на корпоративном уровне должно быть запрещено. Необходимо предварительно провести проверку рабочих станций на наличие программного обеспечения для обмена данными по IM-сетям и в дальнейшем обеспечить постоянный контроль загрузки нового программного обеспечения на рабочие станции. Важнейшим мероприятием и гарантией такого контроля является передача системных прав от пользователя к администратору.

Приложения класса peer-to-peer

Peer-to-peer (сокращенно P2P) — это технология построения распределенной сети, где каждый узел может одновременно выступать в роли и клиента (получателя информации), и сервера (поставщика информации). Как правило, сеть состоит из равноправных узлов, причем каждый из них взаимодействует лишь с некоторым подмножеством узлов сети, так как установление связи «каждый с каждым» невозможно из-за ограниченности вычислительных и пропускных ресурсов. При этом передача информации между узлами, не связанными в данный момент непосредственно, может осуществляться как по своеобразной эстафете — от узла к узлу, так и путем установления временной прямой связи. Все вопросы маршрутизации и авторизации сообщений, передаваемых по эстафете, лежат не на едином сервере, а на всех этих отдельных узлах. Такое определение также известно под названием Pure P2P.

P2P-приложения — это класс приложений, совместно использующих распределенные ресурсы (дисковое пространство и файлы, вычислительные ресурсы, каналы связи и т. д.). Сегодня P2P приобретает все большую популярность. Доказательством этого служит то, что многие производители программного обеспечения объявили о поддержке P2P в своих новых продуктах.

Области применения P2P.

- **Файловые обменные сети (file-sharing).** P2P выступают хорошей альтернативой FTP-архивам, обладая при этом целым рядом преимуществ: балансировкой нагрузки, более широкой полосой пропускания, высокой «живучестью» и широкими возможностями по публикации контента. Примеры — Napster, Gnutella, eDonkey, KaZaa, BitTorrent, FastTrack, IRC, WinMX и их производные.
- **Распределенные вычислительные сети.** Например, SETI@HOME. Этот проект продемонстрировал большой вычислительный потенциал для хорошо распараллеливаемых задач. В настоящий момент в нем принимают участие свыше трех миллионов пользователей.
- **Службы сообщений (Instant-messaging).** Как было сказано раннее, некоторые IM-клиенты способны обеспечивать поддержку архитектуры «клиент-клиент».
- **Сети групповой работы (P2P Groupware).** Подобные приложения еще мало распространены, но развиваются большими темпами. Одними из самых перспективных считаются Groove Network — сеть, предоставляющая защищенное пространство для коммуникаций, и OpenCola — технология поиска информации и обмена ссылками на наиболее интересные источники, где в роли поискового сервера выступает не сервер, а каждый из пользователей сети.

Как уже неоднократно отмечалось, P2P являются потенциально опасными приложениями. Через P2P-каналы возможна утечка конфиденциальной информации, распространение вредоносных программ и кодов (P2P и IM-черви, различные троянские программы), рассылка спама и т.п. А поскольку применение этих приложений сегодня практически не контролируется, то их использование создает реальную угрозу корпоративным информационным сетям.

P2P-приложения, такие как KaZaa или Gnutella (клиент Limewire) могут соединяться с

[10] Каждая IM-сеть имеет свою архитектуру. Клиенты AOL/ICQ, MSN, Yahoo! не могут взаимодействовать напрямую друг с другом. Попытка договориться о едином стандарте (Session Initial Protocol - SIP, RFC 3261, опубликованный IETF в 2002) не дала пока никаких результатов. Каждая сеть продолжает поддерживать свой собственный протокол: AOL/ICQ разработала протокол OSCAR, Microsoft - MSN Messenger Service Protocol (на настоящий момент существует уже10 версия, при этом не поддерживаются старые версии и отсутствуют публикации об обновленных версиях), Yahoo! - YMSG Messenger Protocol

другими клиентами мгновенной отправки сообщений, используя любой открытый TCP или UDP-порт. К тому же данные приложения способны передавать файлы по HTTP-протоколу, который является типичным для веб-трафика и разрешается для прохождения любым межсетевым экраном или прокси-сервером. Это делает фильтрацию P2P-трафика крайне затруднительной.

Другой проблемой, связанной с применением P2P-приложений, является социальная. Часто бывает, что с помощью данных продуктов сотрудниками осуществляется незаконный обмен пиратским контентом и программным обеспечением, что приводит к нарушению авторских прав, а значит, и к возможным юридическим проблемам для компаний.

Основу защиты от угроз, связанных с использованием P2P-приложений, является введение в организации соответствующей политики безопасности. Данная политика должна предусматривать:

1. Запрет использования неавторизованного программного обеспечения в корпоративной сети.
2. Запрет соединения через определенные порты, характерные для некоторых P2P-приложений (см. Таблицу № 1).
3. Применение специализированных средств для обеспечения мониторинга использования интернет-ресурсов, а также сканирования корпоративных сетевых ресурсов и рабочих станций на наличие и использование неавторизованного ПО и материалов.

Napster	eDonkey	Gnutella	KaZaa
tcp 8888	tcp 4661	tcp/udp 6345	tcp 80 (WWW)
tcp 8875	tcp 4662	tcp/udp 6346	tcp/udp 1214
tcp 6699	udp 4665	tcp/udp 6347	
		tcp/udp 6348	

Таблица 1. Порты, характерные для некоторых P2P-приложений

В качестве средств, препятствующих загрузке и исполнению P2P-приложений, могут служить установленные системы предотвращения вторжений (Intrusion prevention Systems), которые осуществляют мониторинг трафика внутри корпоративной сети. Они проводят мониторинг P2P-трафика и блокировку портов соединения. Межсетевые экраны способны обеспечить мониторинг загрузки определенных типов файлов, характерных для P2P-трафика (*.mp3, *.wma, *.avi, *.mpg, *.mpeg, *.jpg, *.gif, *.zip, *.torrent, а также *.exe). С помощью антивирусного ПО сканируется P2P-трафик на наличие вредоносных программ и червей. Значительно помогает мониторинг свободного дискового пространства корпоративных файловых систем и рабочих станций пользователей. Резкое сокращение объемов хранения данных является одним из признаков работы P2P-приложений.

On-line игры

Злоумышленники не могли не использовать онлайновые игры, популярность которых бурно растет. Современный рынок этого вида электронных продуктов сейчас переживает период максимального расцвета. С увеличением объемов и качества рынка онлайновых игр не заставили себя долго ждать и вредоносные программы, предназначенные для кражи пользовательской информации. В начале 2003 г. появились первые троянские программы, ворующие учетные данные пользовательских аккаунтов к играм. Российские «умельцы» также участвуют в процессе кражи данных пользователей-игроков. В частности, в зону их внимания попала популярная российская игра «Бойцовский клуб».

Поскольку on-line игры в большинстве своем не имеют ничего общего с бизнесом, то наиболее эффективным способом борьбы с вредоносными программами, передаваемыми во время игры в режиме онлайн, является их категорическое запрещение. Такой подход должен быть в первую очередь отражен в политике безопасности и донесен до каждого сотрудника (при необходимости — под роспись). Кроме того, необходимо внедрить в компании специализированные средства контроля за выполнением данного положения политики. К ним относятся межсетевые экраны с возможностью контентной фильтрации и специализированные системы контроля веб-трафика, обеспечивающие фильтрацию HTTP-трафика.

Средства контентной фильтрации

Объективная потребность вызвала к жизни множество программных продуктов, предназначенных для защиты от вышеназванных угроз. Все они в той или иной степени выполняют возложенную на них задачу. Однако практика показала, что наиболее эффективными, с точки зрения борьбы с ними, являются средства, которые используют технологию контентной фильтрации.

Следует отметить, что никакая автоматическая система не дает 100% гарантии безопасности без деятельного участия человека в процессе фильтрации. От того, насколько система адекватна задачам, которые ставит перед собой администратор, будет зависеть, удастся ли снизить уровень рисков, связанных с использованием Интернета.

Кроме того, необходимо сделать очень важное допущение. Оно предполагает, что средства контентной фильтрации применяются после того, как приняты все базовые меры по обеспечению безопасности, которые включают в себя: принятие в организации политики безопасности, приведение в соответствие с ней всей корпоративной инфраструктуры, установку необходимых обновлений операционных систем и прикладных программ, а также выполнение других действий, требуемых политикой безопасности. Только тогда внедрение специализированных средств контентной фильтрации позволит достичь желаемого результата.

ИТ-рынок предлагает различные средства фильтрации содержимого информационного обмена по каналам Интернет. Их можно условно разделить по типам и методам фильтрации. В настоящее время известно три типа средств, обеспечивающих контроль использования интернет-ресурсов на корпоративном уровне. К первому типу относятся межсетевые экраны, система обнаружения вторжений, прокси-серверы, маршрутизаторы и подобные им средства фильтрации. Второй тип — это современные антивирусные программы, обладающие базовыми возможностями контентной фильтрации.

К третьему типу относятся специализированные средства, разработанные непосредственно для контроля использования интернет-ресурсов: системы мониторинга электронной почты, средства контроля веб-трафика, анти-спам-фильтры, анти-шпионские программы и т.п.

Межсетевые экраны

Возможности проверки информационных потоков, заложенные в современных межсетевых экранах, расширяют функции анализа данных до уровня контентной фильтрации. Это позволяет защитить корпоративные сети от различных рисков, описанных в предыдущих главах, а также обеспечить достаточный уровень контроля доступа пользователей в Интернет.

В межсетевых экранах используются два не исключающие друг друга подхода к выявлению сетевых атак. Они осуществляют как анализ сетевого трафика, так и анализ контента. В первом случае анализируются только заголовки сетевых пакетов, во втором — их содержимое (включая заголовки и области данных), что обеспечивает полный контроль информационных взаимодействий.

Необходимо, однако, отметить, что межсетевые экраны являются средствами потокового анализа, которым приходится обрабатывать очень большие объемы данных. Время обработки данных является для них критичным параметром. Контентная фильтрация оказывает существенное влияние на производительность, поэтому с практической точки зрения эта задача трудновыполнима из-за огромного объема данных, которые приходилось бы анализировать. В современных межсетевых экранах начинают возникать серьезные проблемы с производительностью уже в сетях, обладающих пропускной способностью 100 Мб/с. Поэтому в большинстве случаев целесообразно использовать для выявления атак методы анализа сетевого трафика и только в некоторых случаях при крайней необходимости сочетать их с анализом контента.

Антивирусная проверка

Своевременное выявление вредоносного мобильного кода жизненно важно для безопасности предприятия. Борьба с вирусами, червями и троянскими программами не может быть успешной, если ограничиться только сканированием на наличие вирусов персональных данных пользователей на серверах и в файловых системах их компьютеров. Наиболее надежную защиту от компьютерных вирусов удастся обеспечить лишь в том случае, если проверка на их наличие производится во всех точках доступа в сеть предприятия.

Механизмы проверки содержимого потоков данных, реализованные в современных межсетевых экранах, предоставляют интегрированное решение для борьбы против вирусов с использованием специальных антивирусных

приложений. Данные приложения могут быть развернуты как непосредственно на сервере, где установлен межсетевой экран, так и на выделенном сервере, специально предназначенном для выполнения задач по антивирусной фильтрации. Такой подход позволяет администратору информационной безопасности предприятия легко реализовать оптимальную схему борьбы с компьютерными вирусами, быстро развернуть ее и администрировать весь комплекс из общего центра управления.

Например, организации требуется обеспечить проверку всех вложений электронной почты на наличие вредоносных программ. Для этого почту проводят через шлюз с межсетевым экраном, который перехватит все потоки данных и перенаправит их на сервер антивирусной проверки. Прежде чем вернуть полученные данные, этот сервер выполнит необходимые действия по сканированию вложений почты на наличие в них вирусов и лечению зараженных данных. Получив данные обратно, межсетевой экран отправляет их получателю. Таким образом, ни одно соединение не будет организовано напрямую без соответствующей проверки.

Сканирование URL

Возможность анализа URL позволяет компании гибко регулировать пропускную способность каналов и экономить рабочее время, ограничивая посещение сотрудниками нежелательных сайтов. Администратор безопасности может создать гибкую политику использования интернет-ресурсов, разрешив доступ только в соответствующее время и к «разрешенной» политикой безопасности информации. Кроме того, этот механизм используется для накопления статистики обращений к определенным информационным ресурсам, что полезно при подготовке различных аналитических отчетов.

В современных межсетевых экранах, как правило, предусмотрено несколько способов определения механизмов сопоставления запрашиваемых URL:

- описание с помощью символов шаблона;
- шаблоны содержатся во внешнем файле;
- внешние базы данных и средства сопоставления.

Каждый из этих механизмов разработан для предоставления администратору исчерпывающего и гибкого инструмента настройки политики безопасности. Наиболее развитые возможности управления достигаются при применении специальных средств третьих производителей, использующих внешние базы данных. Обычно такие производители предоставляют возможность подписки на обновленные версии своих баз.

Блокирование активного контента

Межсетевые экраны позволяют эффективно бороться с различными атаками, связанными с использованием Java и ActiveX. Администратор безопасности контролирует прохождение кода Java и ActiveX в соответствии с определенными условиями, как, например, сетевой адрес компьютера клиента и сервера, запрашиваемый URL или зарегистрированное имя пользователя.

Межсетевой экран может производить следующие действия над обнаруженным кодом Java и ActiveX:

- удаление Java-аплетов, встречающихся в тексте HTML-страницы;
- удаление Java-аплетов из всех потоков между сервером и клиентом, даже если информация содержится в архивном файле;
- блокирование Java-атак путем запрещения подозрительных обратных соединений;
- удаление ActiveX-аплетов, встречающихся в текстах HTML-страниц;
- анализ кода JavaScript, встречающегося в текстах HTML-страниц.

Поддержка почтового протокола SMTP

Современные межсетевые экраны обеспечивают эффективную защиту корпоративных сетей, благодаря возможности проведения детального анализа SMTP-соединений. При этом они могут выполнять следующие действия:

- разрыв непосредственного соединения с сервером бесплатного почтового сервиса;
- замена в исходящей почте адресов в поле From_ на некоторый общий адрес, что позволяет полностью скрыть внутреннюю сетевую структуру (так называемый маскарад);
- перенаправление почты, отправленной определенному пользователю, например, пользователю root;
- блокирование электронной почты от определенных адресатов;
- удаление вложений определенного типа, например, исполнимых файлов;
- модификация служебной информации, например, удаление полей Received в исходящей почте, что предотвращает распространение информации о маршрутах прохождения почты внутри организации;
- блокирование почтовых сообщений, превышающих заданный размер;

- сканирование электронной почты на наличие вредоносных программ.

В дополнение к этому отметим, что межсетевые экраны поддерживают только необходимый набор команд протокола SMTP, и это тоже способствует безопасности обмена, поскольку нетривиальные команды часто используются злоумышленниками во враждебных целях.

Фильтрация HTTP

Ресурсы, адресуемые через URL, определяют метод доступа (например, GET, POST и т.п.), сервер, где расположен ресурс, путь доступа непосредственно к этому ресурсу на сервере и, возможно, специфический запрос к нему. Все приведенные выше способы обработки потоков информации могут быть применены к таким ресурсам, описания которых созданы с использованием символов шаблона. Возможно также размещение этих описаний во внешнем файле.

Обработка протокола FTP

Сервер безопасности FTP обеспечивает не только проверку подлинности пользователя, но и проверку безопасности информации, обмен которой происходит по этому протоколу. Управление осуществляется как на уровне команд FTP-протокола (PUT/GET) и внесения ограничений на возможные имена файлов, так и путем перенаправления потоков данных на внешние серверы антивирусной проверки.

Антивирусные программы

В антивирусных программах широко применяется технология контентной фильтрации, которая значительно расширяет возможности по борьбе с вредоносными программами.

Антивирусы способны:

- обеспечивать защиту от вирусов, червей, троянских программ, различных вредоносных скриптов и кодов, распространяемых по каналам электронной почты, через веб, интернет-пейджеры, P2P-сети, мобильные устройства (карманные компьютеры и смартфоны);
- определять и при необходимости блокировать активный код (Java-аплеты и элементы ActiveX);
- обеспечивать защиту от представителей класса spyware;
- предотвращать фишинг/фарминг-атаки.

Для решения последних двух задач антивирусное программное обеспечение, как правило, использует дополнительные утилиты, которые при необходимости включаются и настраиваются администратором безопасности заказчика.

Основным методом обнаружения вредоносных программ по-прежнему остается анализ сигнатуры проверяемых данных. Однако скорость распространения вредоносных программ гораздо выше скорости обновления антивирусных баз данных. На анализ нового вируса требуется определенное время. Поэтому от обнаружения новой вредоносной программы до выхода обновлений корпоративные сети остаются беззащитными. Выходом из данной ситуации является так называемый превентивный подход. Он включает в себя следующие методики обнаружения вредоносных программ:

1. **Эвристический анализ.** Анализ, основанный на поиске в исполняемых файлах отдельных записей кода, присущих вредоносным программам. Эвристический метод предназначен для выявления неизвестного вредоносного ПО. Хотя, уровень обнаружения новых вирусов, червей и троянцев не превышает 25-30%, но эвристический анализ эффективен в сочетании с другими методами.
2. **Анализ поведения программ.** Анализируется последовательность действий вредоносной программы и блокируется выполнение любых опасных действий. (Например, блокировка отправки большого числа неавторизованных электронных сообщений лицам из адресной книги.) Возможно обнаружение любого типа вредоносного ПО. Имеет высокий уровень эффективности (до 70%).
3. **Выявление формальных признаков вредоносной программы.** Для защиты почтового трафика могут использоваться методы, основанные на анализе почтовых сообщений, проходящих через почтовый сервер. С помощью такого анализа можно остановить эпидемию в самом ее начале. При этом к формальным признакам относятся: массовая рассылка или прием одинаковых вложений (одинаковых писем с различными вложениями), наличие двойного расширения у вложений и т.п. Кроме того, возможен лингвистический анализ тел писем.
4. **Блокировка доступа пользователей к «запрещенным» интернет-ресурсам.** Списки таких ресурсов составляются компаниями-производителями средств контентной фильтрации и антивирусных и распространяются по подписке.

При выборе антивирусных программ важно выяснить, могут ли они обнаруживать и удалять rootkit на Windows-системах. Для этого нужно многофункциональное антивирусное решение, способное работать с операционной системой на самых низких уровнях и контролировать все системные функции.

В настоящее время наблюдается некоторый уклон в сторону анализа почтового трафика, поскольку все последние значительные эпидемии были организованы через каналы электронной почты. Однако в сегодняшней ситуации обязателен анализ всего сетевого трафика. Например, для HTTP-протокола важно осуществлять анализ всех скриптов HTTP-серверов (в первую очередь, пользовательских) и поиск в них разнообразных уязвимостей: SQL-инъекций, инъекций кода, запуска произвольных программ, получения файлов, межсайтовый скриптинг (XSS), HTTP Response Splitting.

И наконец, большое значение при выборе антивирусной системы имеет их способность эффективно осуществлять разбор объектов информационного обмена на составляющие их компоненты вне зависимости от протокола передачи, кодировки и сложности их структуры. Если в почтовом сообщении находится вложенный архивный файл, то в любом случае такая система должна быть способна «прочитать» данный файл. На помощь приходит технология распаковки и выявления реального содержимого упакованных и архивированных файлов, в том числе наиболее популярных форматов ZIP, ARJ, RAR и CAB. Кроме того, проблема множественности кодировок приводит к осложнению анализа текстов. Принимая это во внимание, разработчики некоторых антивирусных программ, например, включают в состав своих продуктов поддержку кодировки UNICODE.

Системы контроля веб-трафика

Системы контроля веб-трафика способны обеспечить:

- предотвращение утечки конфиденциальной информации;
- мониторинг подозрительной и запрещенной активности пользователей;
- защиту от атак с использованием социальной инженерии (фишинг/фарминг);
- защиту от вирусов и другого вредоносного кода;
- защиту от воздействия потенциально опасных программ (программ-шпионов, рекламных кодов и т.п.).

Системы контроля веб-трафика (далее СКВТ) широко представлены на рынке информационной безопасности. Основным отличием данных систем являются применяемые методы фильтрации, то есть набор параметров, по которым производится проверка содержимого информационного обмена. СКВТ используют различные наборы проверок, в зависимости от возложенных на средства фильтрации задач.

Наиболее типичными являются системы, в которых основной способ фильтрации веб-трафика — проверка адресов интернет-ресурсов (URL). Такие системы, как правило, фильтруют только запросы пользователей, не проверяя загружаемые сайты на наличие запрещенного политикой безопасности содержимого. Однако URL-фильтрация не гарантирует, что, разрешив доступ на сайт, находящийся в белом списке, пользователь не будет подвержен атаке, поскольку нет уверенности в том, что сайт не был прежде атакован злоумышленниками и на него не внедрены троянские программы и т.п. Это говорит о неэффективности простой URL-фильтрации. Вывод один — необходима проверка содержимого, загружаемого со всех без исключения сайтов. При этом надо иметь в виду, что фильтрация веб-трафика на основе адресов интернет-ресурсов по-прежнему является одной из основных, и списывать ее со счетов ни в коем случае нельзя. Здесь важно помнить, что фильтрация должна быть комплексной и включать в себя всевозможные проверки, которые обеспечат полный контроль веб-трафика.

В настоящее время существуют системы, в которых проверки равноценны по значимости, а состав их набора определяется задачами, возлагаемыми на систему контроля. Такие СКВТ обладают наиболее широким набором проверок, среди которых одной из важнейших является проверка содержания текста запросов и сайтов. Данный контроль подразумевает проверку текста на наличие ключевых слов и выражений. Очень важно, чтобы анализировалось содержание не только страниц сайтов, но и запросов пользователей или любой другой передаваемой ими по сети информации. Это необходимо, например, при контроле переписки сотрудников, использующих бесплатные почтовые ресурсы.

Одна из важнейших задач, возлагаемых на контентную фильтрацию, это защита от вредоносных программ. Такая защита может осуществляться как встроенными средствами, так и с помощью внешних систем. При этом необходимо учитывать, что проводится проверка трафика на наличие не только вирусов червей, но и дру-

гих вредоносных кодов, среди которых скрипты, Java-аплеты и элементы ActiveX.

Ограничение по типам передаваемых данных имеет существенное значение для многих организаций. Так, можно установить запрет на отправку за пределы организации данных в форматах, отличных от простого текста, например, файлов Microsoft Word и Excel. При этом тип файла не должен определяться по информации, указанной в запросе или ответе, т.е. по расширению файла или MIME-типу, указанному сервером. Для точной обработки данных система контроля веб-трафика должна определять тип файла по его сигнатуре. Такое требование обусловлено еще и тем, что большинство веб-серверов при передаче данных объявляют MIME-тип, ориентируясь на расширение файла, что может содержать ошибку из-за неверного указания типа в файле соответствий или переименования файла пользователем.

Чтобы создаваемая политика доступа к интернет-ресурсам была эффективной, средства контроля должны обеспечивать возможность задавать разные условия проверки для различных направлений передачи данных и команд протоколов. Это позволит, например, запретить передачу документов Microsoft Word из организации, разрешая, однако, загружать документы данного формата. Эту функциональность можно использовать не только для контроля типов данных, но и для проверки содержимого на наличие конфиденциальной информации.

Многие из имеющихся на рынке систем (в том числе и от ведущих производителей, таких как Websense, SurfControl) обеспечивают фильтрацию лишь исходящего трафика, т.е. запросов пользователя, совершенно не уделяя внимания проверке информации, загружаемой на стороне клиента. Это в значительной степени снижает гибкость реализуемой политики использования интернет-ресурсов, поскольку требует жесткого ограничения доступа пользователей к сайтам. Существуют сайты, на которых часть информации относится к категории «запрещенной», а часть — к «разрешенной». Именно на этапе ответа на запрос пользователя возможно разделение на «запрещенное» и «разрешенное» содержание.

Иногда полезно предоставить пользователю доступ к данным, например, к странице на веб-сервере, но удалить из этих данных какую-либо часть, нарушающую политику безопасности или приводящую к проникновению вредоносного кода в корпоративную сеть. Хороший пример такого подхода — анализ на предмет потенциальной опасности JavaScript, находящегося на странице, и удаление соответствующих частей страницы. Чтобы исключить вероятность описанных выше нарушений, системы контроля должны иметь в своем составе средства замены и модификации передаваемых данных.

Системы контроля электронной почты

Системы контроля веб-трафика способны обеспечить:

- предотвращение утечки конфиденциальной информации по каналам электронной почты;
- защиту от атак с использованием социальной инженерии (фишинг/фарминг);
- защиту от спама;
- защиту от вирусов и другого вредоносного кода.

Системы контроля электронной почты в качестве основной используют технологию контентного анализа. Данные системы проверяют содержимое каждого электронного письма. Анализ осуществляется по всем составляющим их компонентам: атрибутам конверта, заголовкам сообщения, MIME-заголовкам, телу сообщения, присоединенным файлам. Поэтому системы контроля электронной почты должны хорошо разбирать почтовые сообщения на составляющие их компоненты. Это должен быть полный разбор, вне зависимости от сложности строения письма и уровней вложенности.

Требование полного разбора письма следует дополнить требованием устойчивости. Во-первых, структура письма подчиняется определенным правилам. Разбор письма на составляющие контенты основан на применении этих правил к конкретному письму. Вообще говоря, возможны случаи, когда почтовая программа автора сообщения формирует письмо с нарушением этих правил, тогда оно не будет корректно разобрано. Система должна быть устойчивой по отношению к обработке таких писем.

Во-вторых, система должна надежно определять типы файлов-вложений. Под «надежностью» понимается определение, основанное не на имени файла или на информации, вписываемой в письмо почтовым клиентом при прикреплении файла (MIME-тип). Такая информация может быть недостоверна в результате либо сознательных попыток обмануть систему контроля, либо неправильных настроек почтовой программы отправителя. Бессмысленно запрещать пересылку файлов типа JPEG, если файл

picture.jpg после переименования в page.txt пройдет незамеченным.

В-третьих, большое значение для системы имеет полнота проводимых проверок, то есть количество и разнообразие критериев анализа электронной почты. Система должна осуществлять фильтрацию по любым атрибутам сообщений, по объему сообщений и вложенных файлов, по количеству и типу вложений, по глубине вложенности, а также уметь анализировать содержимое прикрепленных файлов вне зависимости от того, являются ли эти файлы сжатыми или архивными.

Современные системы контроля электронной почты защищают от спама. Как правило, в их состав входят дополнительные модули, обеспечивающие данную задачу. Применяются в них три основные методики определения, какое письмо относится к спаму, а какое нет. Первая методика выявляет наличие в письме определенных признаков, таких как ключевые слова или словосочетания, характерное написание темы письма (например, все заглавные буквы и большое количество восклицательных знаков), а также специфическая адресная информация.

Вторая методика связана с определением адреса отправителя и его принадлежности к «черным спискам» почтовых серверов DNS Black List или Open Relay Black List. В эти списки заносятся серверы или компьютеры, замеченные в массовых рассылках спама. Идея заключается в том, чтобы вообще не принимать и не транслировать почту, исходящую с этих машин.

Третья методика позволяет автоматически настроить фильтры согласно особенностям индивидуальной переписки, а при обработке учитывает признаки как «плохих», так и «хороших» фильтров. Она основывается на теории вероятностей и использует для фильтрации спама статистический алгоритм Байеса. По имеющимся оценкам, этот метод борьбы со спамом является весьма эффективным. Так, в процессе испытания через фильтр были пропущены 8 тыс. писем, половина из которых являлась спамом. В результате система не смогла распознать лишь 0,5% спам-сообщений, а количество ошибочных срабатываний фильтра оказалось нулевым.

Большое значение в современных системах контроля электронной почты имеет гибкость реагирования системы на результат анализа содержимого почтовых сообщений. Системы должны «уметь» блокировать (совсем или на время) доставку писем, помещать письма в карантинную зону для последующего анализа, посылать уведомления администратору или другим адресатам о событиях, происходящих в системе и т.п.

В последнее время при обеспечении безопасности информационных систем большое значение получил такой фактор, как наличие в компании архива почтовых сообщений. Некоторые разработчики систем контентного анализа предусматривают в новых продуктах использование специальных модулей архивирования. Именно наличие архива электронной почты определяет полнофункциональность продуктов этой категории. Ведение архива — это не просто автоматическая архивация почтовых сообщений в файл, но способность системы регистрировать сообщения и вести учет необходимой информации на протяжении всего жизненного цикла сообщения, возможность получения любых выборок и статистики из архива по запросам, созданным с использованием любых критериев.

Кроме того, долговременный архив предоставляет возможность ретроспективного анализа почтовых потоков и не только позволяет найти виновных, например, в утечке конфиденциальной информации по прошествии определенного времени, но и содержит материал для построения объективной и обоснованной политики использования электронной почты.

Одним из основных критериев оценки систем контекстного анализа для российского рынка является поддержка продуктом различных кодировок кириллицы (CP1251, CP866, ISO88595, KOI-8R, MAC), что позволяет проводить анализ русскоязычных текстов. Большинство продуктов иностранного производства не поддерживают кодировки кириллицы, а это в значительной степени ограничивает их использование на территории Российской Федерации. Все осложняется тем, что разные части письма, включая почтовые заголовки, могут быть написаны в различных кодировках, которые не всегда указаны или указаны не верно.

Средства фильтрации IM- и P2P-трафиков

В настоящее время на рынке информационной безопасности появились продукты, которые позволяют обеспечить фильтрацию IM- и P2P-трафиков. Они проводят мониторинг трафика, управление доступом пользователей, протоколирование их действий, а в некоторых случаях и архивирование передаваемых данных.

Действие этих продуктов основано на применении следующих технологий:

- детектирование протокола передачи данных;
- мониторинг соединений на портах, характерных для IM- и P2P-трафиков;
- проверка сигнатуры передаваемых файлов;
- антивирусная проверка (как правило, с помощью интегрированных средств);
- фильтрация на основе смыслового анализа текстов сообщений, передаваемых по IM-протоколу;
- блокировка спима (спам для IM).

Полезной мерой, например, является блокировка доступа сотрудников к интернет-ресурсам, содержащим в URL ключевые слова «aim:» or «ymsgr:». Это предотвратит использование злоумышленниками уязвимостей в URI-обработчиках. Другим действием может быть удаление данных записей из реестра «HKEY_CLASSES_ROOT».

Кроме того, для защиты от угроз помогает блокировка активных элементов ActiveX, которые эксплуатируют уязвимости в IM- и P2P-клиентах. Данная уязвимость позволяет злоумышленникам получать удаленный доступ к компьютерам и проводить атаки типа «переполнение буфера» (buffer overflow).

Фильтрация по типам файлов также является важной мерой по обеспечению безопасности использования IM- и P2P-трафиков. К примеру, в последнее время злоумышленники стали часто эксплуатировать уязвимость Интернет-пейджеров при закачке JPEG-файлов.

Эффективность данных средств достаточно высока, но важно иметь ввиду, что эти продукты предназначены для фильтрации определенных протоколов и, к сожалению, не в состоянии перекрыть весь трафик. Пользователю достаточно перейти на использование другой IM- и P2P-сетей (коих, как было сказано ранее, появилось большое количество), как его соединение останется незамеченным фильтром. Поэтому необходимо совмещать все меры технического и административного характера, которые позволят контролировать как факт загрузки нового программного обеспечения и использования конкретного IM- и P2P-приложений, так и проводить анализ передаваемых через них данных.

Анти-спам-фильтры

Большинство средних и крупных компаний имеют свой корпоративный почтовый сервер, установленный в офисе компании. 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 возможность 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.

Средства фильтрации спама, реализуемой на корпоративном сервере, предлагают многие производители. 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 применяют контентную фильтрацию электронной почты, то есть содержимое письма для них является одним из важнейших критериев, по которому его можно отнести к спаму.

Современные средства фильтрации спама применяют следующие методы:

- **Проверка по DNSBL-спискам.** Данный способ отличается невысокой эффективностью, если применять его отдельно. Кроме того, существует большая вероятность потери легальной почты.
- **Сигнатурный анализ.** По каждому спамерскому письму может быть автоматически создана так называемая лексическая сигна-

тура, позволяющая распознать это письмо даже с небольшими модификациями.

- **Анти-спуфинг (anti-spoofing)** — система проверки подделки адресов отправителя (Sender Policy Framework, Sender ID).
- **Аутентификация отправителей почтовых сообщений.** Одним из способов является добавление к письмам электронной цифровой подписи (DomainKeys, Trusted Email Open Standard).
- **Анализ заголовков сообщения.** В частности, массовые рассылки спама могут быть обнаружены по содержимому заголовков.
- **Формальные признаки.** К таким признакам можно отнести: отсутствие адреса отправителя, отсутствие или наличие большого количества получателей, отсутствие IP-адреса в системе интернет-адресов DNS, определенный размер и формат сообщения и т.п.
- **Фильтрация на основе смыслового анализа текста.** Широко применяются детерминированные или статистические методы анализа. Фильтрация по содержимому текста является на сегодня достаточно эффективным способом борьбы с ним. С ее помощью возможна блокировка до 95% спам-сообщений.
- **Эвристический анализ.** Позволяет выявить в поступившем пользователю сообщении признаки, совокупность которых дает возможность установить принадлежность к спаму.

Средства защиты от шпионских программ

Специализированные средства защиты от шпионских программ позволяют проверять уже установленное программное обеспечение, а также защитить компьютер от попадания новых riskware-продуктов. Данные средства устанавливаются на рабочих станциях пользователей либо в виде отдельного приложения, либо в виде агента, который централизованно устанавливается и управляется с сервера.

Средства защиты:

- проверяют наличие адресов сайтов, содержащих шпионские объекты; данные списки составляются компаниями-производителями средств контентной фильтрации и антивирусов; распространяются по подписке;
- выявляют активные элементы (ActiveX, Java-аплеты);
- ведут мониторинг запущенных на компьютере процессов;
- управляют программами, запущенными на старте операционной системы;
- обеспечивают контроль за теми приложениями, которые имеют доступ к статистике сетевых соединений, настройкам системы, браузера и доступа к Интернету;
- выявляют подключение и работу средств удаленного администрирования (Remote Administration Tool).

Однако необходимо иметь в виду, что борьба со шпионским ПО является многоуровневой и комплексной задачей. Одни лишь специализированные средства не в состоянии справиться с проблемой, а являются лишь дополнительным элементом в общей системе информационной безопасности, включающей антивирусную фильтрацию, контроль на уровне приложений и т.п.

Другие средства контентной фильтрации

Среди средств контентной фильтрации некоторые решают очень специфичные задачи, например, такие:

- оптическое распознавание символов (Optical Character Recognition);
- распознавание лиц;
- распознавание логотипов, торговых марок, знаков и символов;
- классификация изображений;
- классификация текста;
- идентификация обнаженного тела;
- цифровые изображения отпечатков пальцев и др.

Они имеют довольно узкую область применения и не влияют на общие тенденции развития средств контентной фильтрации. Однако необходимо отметить, что используемые в них технологии со временем обязательно будут востребованы. Например, некоторые спам-сообщения присылаются пользователю в виде графических файлов, что крайне затрудняет автоматический анализ. Классификация изображений или оптическое распознавание символов помогут в решении этой задачи, а способность идентифицировать изображение обнаженного тела позволит определять порнографию на страницах загружаемых сайтов и т.п.

Таблица 2. Угрозы и средства защиты от них

Средства защиты / Виды угроз	Межсетевые экраны	Антивирусные программы	Системы контроля веб-трафика	Системы контроля электронной почты	Анти-спам-фильтры	Средства защиты от шпионских программ	Средства контроля IM-клиентов	Средства контроля P2P-приложений
Утечка конфиденциальной информации			+ контроль содержимого текстов POST-запросов и передаваемых файлов	+ контроль содержимого текстов всех компонентов письма и вложенных файлов			+ контроль содержимого текстов исходящих сообщений	
Атаки на сети с использованием социальной инженерии				+ контроль содержимого текстов письма	+ блокировка массовых рассылок мошеннических писем			
Фишинг/ фарминг	+ • проверка подлинности веб-ресурса; • блокировка троянских программ, активных элементов ActiveX	+ • проверка подлинности веб-ресурса; • анти-DNS-poisoning; • блокировка троянских программ, активных элементов ActiveX		+ контроль содержимого текстов письма	+ блокировка массовых рассылок фишинг-сообщений		+ • проверка содержимого текстов на наличие фишинг-сообщений • блокировка spim	
Вредоносные программы	+ с использованием интегрированных антивирусных программ	+ см. главу «Антивирусные программы»	+ с использованием интегрированных антивирусных программ	+ с использованием интегрированных антивирусных программ	+ блокировка массовых рассылок писем с вредоносными программами		+ с использованием интегрированных антивирусных программ	+ с использованием интегрированных антивирусных программ
Черви	+ с использованием интегрированных антивирусных программ	+ см. главу «Антивирусные программы»	+ с использованием интегрированных антивирусных программ	+ с использованием интегрированных антивирусных программ	+ блокировка массовых рассылок писем с червями		+ с использованием интегрированных антивирусных программ	+ с использованием интегрированных антивирусных программ

Троянские программы	+ с использованием интегрированных антивирусных программ	+ см. главу «Антивирусные программы»	+ с использованием интегрированных антивирусных программ	+ с использованием интегрированных антивирусных программ	+ блокировка массовых рассылок писем с троянскими программами		+ с использованием интегрированных антивирусных программ	+ с использованием интегрированных антивирусных программ
Программы-шпионы	+ • блокировка троянских программ, активных элементов (ActiveX, Java-аплеты и т.п.); • блокировка соединений с «фальшивыми» сайтами»; • блокировка аномального исходящего трафика	+ • блокировка троянских программ, активных элементов (ActiveX, Java-аплеты и т.п); • контроль исполнения шпионского ПО (с использованием поведенческого анализатора)				+ см. главу «Средства защиты от шпионских программ»		
Спам	+ по спискам DNSBL и ORBL	+ по спискам DNSBL и ORBL		+ блокировка по: - формальным признакам; - спискам DNSBL и ORBL - содержимому текста	+ см. главу «Анти-спам-фильтры»		+ блокировка spim по: - UIN пользователей; - тексту	

Таблица 3. Сервисы/приложения и средства контроля за их использованием

Средства контроля / Сервисы	Межсетевые экраны	Антивирусные программы	Системы контроля веб-трафика	Системы контроля электронной почты	Анти-спам-фильтры	Средства защиты от шпионских программ	Средства контроля IM-клиентов	Средства контроля P2P-приложений
Электронная почта	+	+		+	+			
HTTP-трафик	+	+	+					
FTP-трафик	+	+	+					
IM-трафик	+	+	+				+	+
P2P-трафик	+	+					+	+
On-line игры, потоковые аудио и видео	+	+	+					

Варианты применения средств контентной фильтрации

В компании «Инфосистемы Джет» накоплен большой опыт внедрения средств контентной фильтрации. С 1998 г. здесь реализовано более 300 крупных проектов, где в той или иной мере использовались такие средства. Являясь системным интегратором, «Инфосистемы Джет» широко применяют продукты ведущих западных производителей, таких как Symantec, Internet SecURLty System, Clearswift и т.п. Однако в арсенале компании есть и собственные разработки в области контентной фильтрации. К ним в первую очередь относятся:

- система контроля веб-трафика «Дозор»;
- система мониторинга и архивирования почтовых сообщений «Дозор-Джет».

Кроме того, «Инфосистемы Джет» производят собственный межсетевой экран Z-2, который так же, как и продукты крупнейших вендеров, имеет в своем составе необходимые модули контентной фильтрации.

Межсетевой экран Z-2

Межсетевой экран Z-2 осуществляет контентную фильтрацию средствами прикладных шлюзов протоколов SMTP, HTTP и FTP. При этом возможны различные варианты политики фильтрации, такие как подмена содержимого, блокировка определенных типов данных, а также использование внешних средств контроля.

Антивирусная проверка содержимого производится внешним сервером, к которому шлюз обращается на этапе проверки. Антивирусная проверка для протоколов HTTP и FTP реализована средствами шлюза протокола HTTP, а для протокола SMTP — средствами шлюза протокола SMTP. Для шлюзов этих протоколов реализовано подключение внешних средств контентной фильтрации посредством протокола ICAP, который поддерживает, например, антивирусные продукты компании Symantec, «Лаборатории Касперского» и другие.

HTTP-gw — прикладной шлюз, предназначенный для осуществления и контроля обмена по протоколу HTTP. HTTP-gw поддерживает протоколы HTTP 1.0 и 1.1 (последний с поддержкой транспортных сессий). HTTP-gw осуществляет:

- ограничение доступа по IP-адресу и порту сервера;
- ограничение доступа по URL;
- необходимую поддержку для блокировки баннеров;
- туннелинг SSL с отдельной настройкой прав доступа по IP-порту;
- одностороннее ограниченное отображение FTP в http;
- блокировку данных по MIME-типам;
- поддержку прозрачного режима;
- возможность работы через родительский прокси-сервер;
- блокирование заданных команд HTTP-протокола.

Кроме того, для протокола HTTP возможно формирование списков шаблонов, при соответствии которым выдается запрет на доступ.

SMTP-gw — прикладной шлюз, предназначенный для осуществления и контроля обмена электронной почтой по протоколу SMTP. SMTP-gw осуществляет:

- прием сообщений по SMTP-протоколу;
- проверку допустимости передачи письма по набору правил, учитывающих почтовые адреса отправителя и получателя и IP-адрес отправителя;
- проверку IP-адреса отправителя через доступные в интернет (по протоколу ORBS) базы данных спамеров и открытых релеев;
- проверку допустимости почтового обмена в соответствии с SMTP-протоколом;
- фильтрацию по заголовкам;
- использование метода greylisting (борьба со спамом).

FTP-gw — прикладной шлюз, предназначенный для осуществления и контроля обмена по протоколу FTP. FTP-gw осуществляет:

- ограничение доступа по IP-адресу и порту сервера и/или клиента;
- блокирование заданных команд FTP-протокола;
- журналирование заданных команд FTP-протокола;
- аутентификацию пользователей на сервере аутентификации и авторизации.

Рассмотрим примерную конфигурацию шлюза HTTP-gw (Рис. 4).

Настройки фильтрации зависят от списков доступа (ACL), которые определяются адресом источника, адресом назначения, а также используемым протоколом. Шлюзов может быть

несколько, все они предполагают разные настройки. Каждый шлюз обслуживает несколько ACL, в зависимости от выбора которых применяются различные правила фильтрации (Рис. 5).

Закладка block MIME-type позволяет сформировать список типов, которые не будут пропущены через шлюз.

Закладка trans MIME-type определяет список замены. Данные этих типов будут заменены при передаче на данные из указанного администратором источника, что дает возможность произвести замену активного содержимого на заведомо безопасное.

Система мониторинга и архивирования почтовых сообщений «Дозор-Джет»

Системы мониторинга и архивирования почтовых сообщений «Дозор-Джет», (СМАП «Дозор-Джет») — это собственная разработка компании «Инфосистемы Джет». Возможности данной системы рассмотрим на примере ее работы в качестве средства реализации политики использования электронной почты, внедренного в одной из компаний-заказчиков.

Политика безопасности при фильтрации почтовых сообщений представляет собой набор *правил* фильтрации системы «Дозор-Джет», эксплуатирующейся в качестве почтового фильтра.

Условия применения системы фильтрации почтовых сообщений

Необходимым условием применения системы фильтрации почтовых сообщений является четко сформулированная политика безопасности, доведенная до сведения каждого пользователя электронной почты. Составители должностных инструкций пользователя должны учитывать, что политика безопасности изначально не несет в себе карательных функций и лишь отражает точку зрения руководства предприятия на организацию делового процесса. С основными ее положениями в части фильтрации почтовых сообщений сотрудники могут быть ознакомлены при приеме на работу одновременно с инструктажем по правилам техники безопасности.

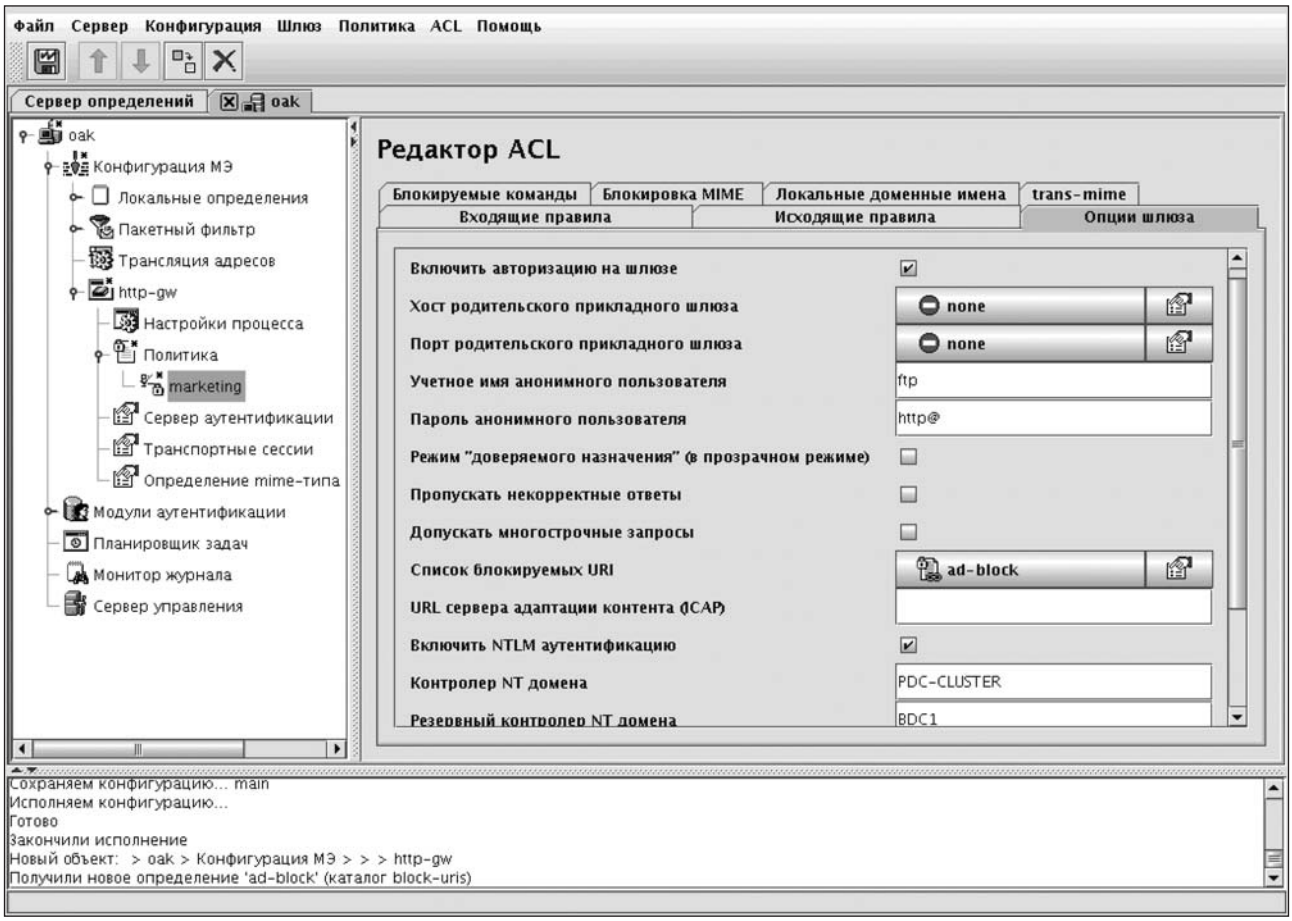

Рис. 4. Настройка ACL шлюза HTTP

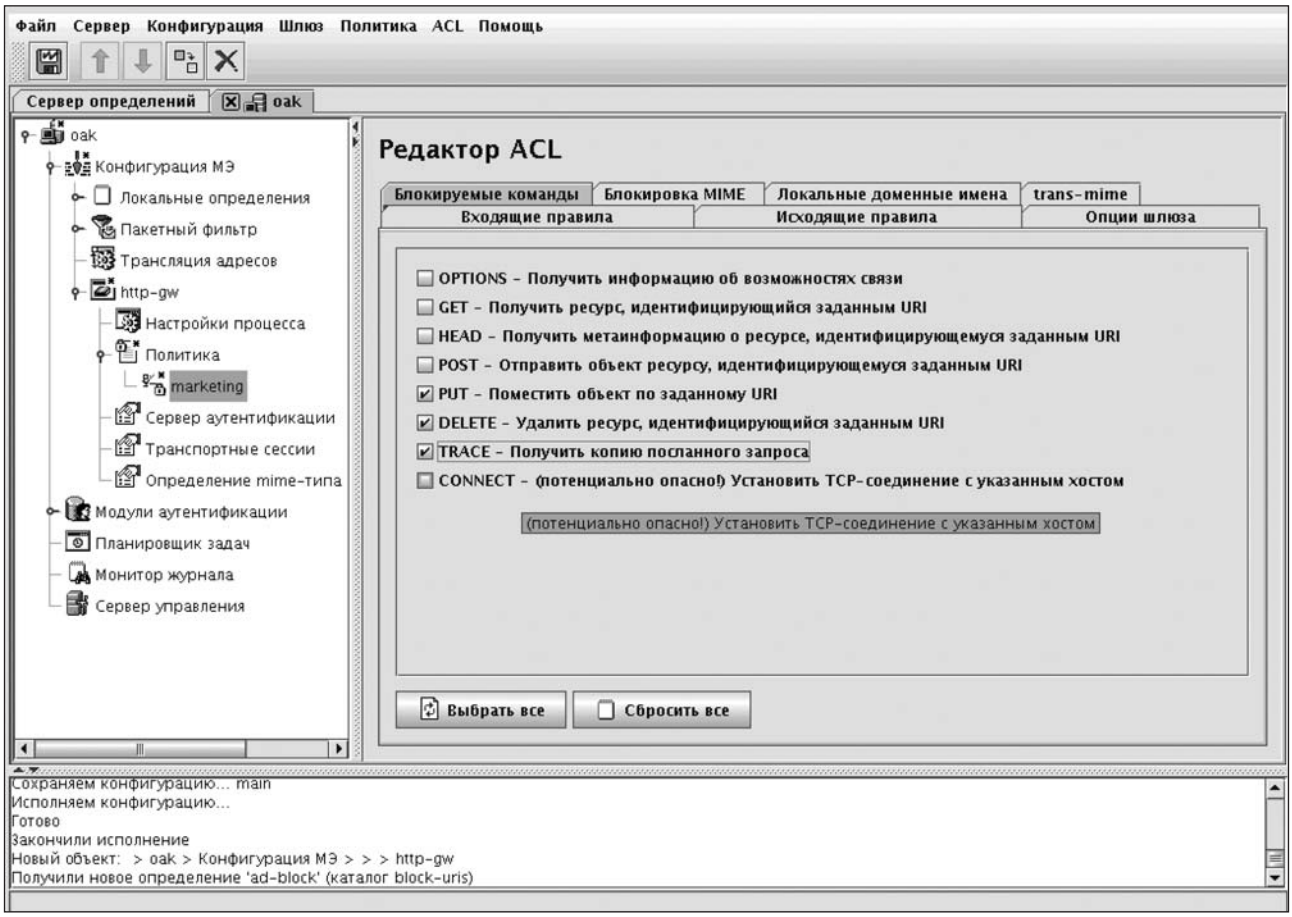

Рис. 5. Опции политики HTTP-шлюза

Цели и задачи применения системы фильтрации почтовых сообщений

Для выработки набора *правил* необходимо, прежде всего, определить цели применения системы фильтрации почты. Они могут быть следующими:

- организация упорядоченной доставки писем, разделение почты на входящую, исходящую и внутреннюю;
- архивирование почтовых сообщений для обеспечения их сохранности;
- ограничение объема почтовых сообщений;
- блокировка спама;
- блокировка доставки писем из нежелательных для организации списков рассылки;
- блокировка или ограничение доставки писем, содержащих исполняемые элементы (Java-script, ActiveX control) и/или почтовые вирусы;
- защита от случайной посылки изнутри конфиденциальной информации;
- блокировка доставки писем, имеющих нежелательное для организации содержание.

Исходные данные для выработки правил фильтрации почтовых сообщений

Перечень исходных данных для выработки *правил* фильтрации почтовых сообщений выглядит следующим образом:

1. Список пользователей электронной почты с указанием фамилии, имени, отчества пользователя, его почтового адреса и полного имени, предназначенного для указания в заголовке электронных писем.
2. Почтовый домен организации, например, fbi.gov.
3. Список ключевых слов, появление которых в тексте писем является нежелательным (список запрещенных слов).
4. Список внешних почтовых адресов или почтовых доменов, сообщения из которых должны блокироваться или задерживаться для анализа.
5. Список внутренних доверенных почтовых адресов пользователей, для которых входящие и исходящие почтовые сообщения не подлежат контролю.

6. Список недопустимых видов почтовых вложений или присоединенных файлов.
7. Конфиденциальная информация, запрещенная для отправки на внешние почтовые серверы.
8. Список внешних почтовых серверов, на которые запрещена отправка писем из организации.

Кроме сбора вышеперечисленных исходных данных следует образовать неформальные группы пользователей электронной почтой, имеющих сходные функциональные обязанности в различных подразделениях. Такие объединения пользователей мы будем в дальнейшем называть *функциональными группами*, а объединения пользователей в группы согласно штатному расписанию — *административными группами*. Создание *административных групп* крупнее отдела вряд ли целесообразно в силу специфики задачи. Обычно в состав крупной административной единицы входят разнородные по выполняемым задачам подразделения.

Полезным может оказаться также объединение всех пользователей, наделенных почтовыми адресами и имеющих право отправлять почту во внешний мир, в группу, которую в дальнейшем будем называть *универсальной*.

Следует отметить, что перечисленные списки не являются окончательными и должны дополняться и модифицироваться по мере необходимости.

Общие рекомендации по выработке правил фильтрации

При определении нового набора *правил* целесообразно предусмотреть посылку уведомлений о задержании отправителям исходящих писем и получателям входящих. Уведомления должны также содержать указание на причину, по которой доставка письма не была произведена. Это необходимо для отладки вновь введенных *правил*, а также для того, чтобы пользователи знали о происходящих изменениях в политике безопасности предприятия.

Для разделения почтового потока на входящий, исходящий и внутренний следует определить почтовый домен организации.

Чтобы уменьшить общий поток писем, целесообразно организовать службу централизованной подписки пользователей на списки рассылки, т.е. вести всю подписку от имени одного пользователя, а на самом предприятии организовать внутреннюю рассылку. Это позволяет, во-первых, минимизировать и упорядочить почтовый трафик, во-вторых — заблокировать доставку нежелательных писем.

Правила формирования списка запрещенных слов

Основную проблему для фильтрации почтовых сообщений представляет анализ содержания в письмах конфиденциальной информации.

Первоначально надо внести в список запрещенных слов следующее:

1. Телефонные номера:
   Не предназначенные для звонков клиентов или посторонних лиц:
   - внутренней АТС;
   - мобильных телефонов сотрудников, предназначенные исключительно для внутреннего пользования.
2. Номера внутренних банковских счетов, не отражаемые в балансовом отчете.
3. Номера документов.
4. Реквизиты налоговых и иных контролирующих органов.
5. Номера пластиковых карт.
6. Фамилии сотрудников организации.
7. Устойчивые словосочетания типа «штатное расписание», «докладная записка», «служебная записка», «распоряжение», «регламент», «должностная инструкция», «маршрут движения», «путевой лист», «частотное расписание» и т.п.
8. Словосочетания, характерные для конфиденциальной информации, циркулирующей в организации.

Поскольку система фильтрации «ДозорДжет» позволяет использование регулярных выражений, то, например, правило поиска номеров выпущенных пластиковых карт VISA может быть записано в следующем виде: *четыре группы по четыре десятичные цифры, возможно, разделенные пробелом*.

Точно так же можно распознавать номера счетов или номера внутренних приказов и распоряжений, имеющие устойчивую структуру.

Защита от вирусов, распространяющихся почтовыми сообщениями

Основную опасность распространения вирусов несет входящая почта. Хорошо организованная и поддерживаемая система анализа писем на содержание вирусов существенно снизит вероятность распространения их внутри организации.

Для защиты от такого рода вирусов необходимо применять фильтрацию почтовых сооб-

щений по полям заголовка, по содержанию и по форматам присоединенных файлов.

Для фильтрации по содержанию в *список запрещенных слов* заносят фразы и слова, характерные для писем, несущих тот или иной вирус. Например, наличие в письме фразы *VERY JOKE..! SEE PRESIDENT AND FBI TOP SECRET PICTURES*, указывает на наличие в нем также почтового вируса **VBS/Loveletter.as**.

Так как почтовые вирусы появляются регулярно, то *список запрещенных слов* необходимо постоянно пополнять новыми *ключевыми словами*, следя за анонсами CERT и/или сообщениями фирм, занимающихся антивирусной защитой. Например, компания *Лаборатория Касперского* располагает большой и оперативно обновляемой базой вирусов, информация о которых доступна посетителям веб-сайта компании.

Для выявления писем, содержащих вирусы, следует производить фильтрацию сообщений по полю *тема* (**Subject:**) в заголовке письма. Например, известен вирус *ILOVEYOU*. Он рассылался в письме, содержащем фразу *ILOVEYOU* в качестве заголовка.

Анализ других полей заголовка (например, поля To:) не эффективен для фильтрации почтовых вирусов. Кроме того, для антивирусной защиты применяются интегрированные программы третьих производителей, таких как Symantec, «Антивирус Касперского» и Dr. Web.

Правила построения фильтра полей заголовка почтового сообщения

Фильтрация по полю From:
Для исходящих сообщений почтовый адрес в поле *отправитель* должен входить в *универсальную группу*. Письма, отправленные с адреса, не содержащегося в этом списке, должны задерживаться до выяснения причин появления постороннего адреса.

Следующая проверка поля *отправитель* определяет принадлежность адреса отправителя к группе доверенных пользователей. Если это подтверждается, то дальнейшие проверки в отношении письма следует прекратить и переслать письмо адресату. То же *правило* действует и для входящей почты.

Поскольку изначально предполагается, что входящая корреспонденция может иметь любой адрес отправителя, то создавать *правила* фильтрации входящей почты по этому параметру не целесообразно. Исключение стоит сделать для систематической массовой рассылки рекламных писем с одного и того же адреса. Сообщения с таким адресом отправителя должны блокироваться.

Можно также создать *правило*, согласно которому будут задерживаться письма с неуказанным адресом отправителя. Обычно они рассылаются массовым порядком и имеют явно рекламное содержание (spam). Чаще всего организаторы несанкционированных коммерческих рассылок не указывают в письме ни адрес отправителя, ни адрес получателя и используют определенные особенности системы доставки почты.

Фильтрация по полю To:
Для исходящей почты фильтрацию почтовых сообщений по адресу получателя целесообразно проводить в редких случаях. Например, если организация выбирает из нескольких поставщиков одного, и работу с этими поставщиками ведут разные менеджеры компании, то можно составить список почтовых адресов, на которые данному сотруднику запрещено отсылать почту (чтобы предотвратить случайную отправку писем). Для входящей корреспонденции должно действовать *правило доверенных лиц*, т.е. доверенным лицам почту надо доставлять, безусловно, без проверок.

Выше отмечалась возможность задержки писем с неуказанным адресом отправителя. То же правило действует и в отношении адреса получателя для входящих писем.

Организаторы списков рассылки чаще всего указывают в поле To: посторонний адрес (обычно свой внутренний, например, *null@subscribe.ru*), а адреса получателей (подписчиков списка рассылки) перечисляют в поле BCC:, чтобы адресат не мог узнать из заголовка письма, кто еще входит в этот список. Для блокировки доставки сообщений из нежелательных списков рассылки следует создать *правило*, блокирующее доставку писем, имеющих в качестве адресов получателя служебные адреса почтовых роботов.

Фильтрация по полю Subject:
Правило фильтрации по *Subject*: необходимо как для входящей, так и для исходящей почты. Выше уже говорилось о пользе такой фильтрации для выявления вирусов. Желательно также организовать фильтрацию писем по теме на предмет задержки писем из несанкционированных массовых рассылок.

Групповые ограничения

Мы уже упоминали о групповом ограничении для пользователей, входящих в *универсальную группу* и в группу доверенных пользователей.

Необходимо также создать *функциональную группу* технических специалистов и разрешить только членам этой группы получать почту с вложенными исполняемыми файлами (тип вложения — **application/octet%stream**). Для технических специалистов можно допустить «отключение» правила, ограничивающего размер принимаемых почтовых сообщений.

Если организация производит официальную рассылку от имени предприятия, то целесообразно создать группу пользователей, имеющих право отсылать официальные письма. Обычно в заголовке или теле официального почтового сообщения содержится ключевая фраза, по которой данные письма могут быть однозначно идентифицированы.

Официальную корреспонденцию, отправленную с адреса, не входящего в указанную группу, следует задерживать до выяснения обстоятельств отправки.

Если в организацию приходят письма из оплачиваемых списков рассылки или из списков рассылки ограниченного распространения, то следует определить группу пользователей, имеющих право на получение почты из указанных списков рассылки и определить отличительные формальные признаки подобных сообщений. Необходимо создать правило, разрешающее доставку писем с ограниченным распространением только членам указанной группы.

Система контроля веб-трафика «Дозор»

Представляем один из вариантов применения Системы контроля веб-трафика «Дозор» (СКВТ «Дозор») производства компании «Инфосистемы Джет»в качестве средства реализации политики использования интернет-ресурсов .

Политика использования интернет-ресурсов

Политика безопасности при фильтрации веб-запросов пользователей и ответов на них представляет собой набор *правил* фильтрации СКВТ «Дозор», эксплуатирующейся в качестве веб-фильтра (протоколы HTTP и FTP).

Цели и задачи применения системы фильтрации веб-трафика

Для выработки набора правил необходимо определить цели применения СКВТ «Дозор». Таковыми являются:

- организация упорядоченного использования Интернет-ресурсов сотрудниками компании, разделение трафика по направлениям на «запросы пользователей» и «ответы на запросы пользователей»;
- контроль доступа пользователей к Интернет-ресурсам;
- предотвращение утечки конфиденциальной информации;
- осуществление мониторинга подозрительной и запрещенной активности пользователей;
- обеспечение защиты от вирусов и другого вредоносного мобильного кода.

Исходные данные для выработки правил фильтрации веб-трафика

Исходными данными для выработки правил фильтрации веб-трафика являются:

1. Списки пользователей по группам «white» (пользователю полностью открыт доступ ко всем реусрсам), «black» (пользователю полностью закрыт доступ ко всем ресурсам), «all» (общие для всех пользователей настройки), «default» (политика безопасности применяется ко всем пользователям, не включенным явно в какую-либо группу) и другие списки (например, по отделам компании или по применяемой политике).
2. Список ресурсов (URL, IP-адресов серверов).
3. Список ключевых слов и словосочетаний, появление которых в тексте запросов и ответов на запросы является нежелательным или запрещенным (конфиденциальная информация).
4. Список форматов файлов (расширений) и типов данных (MIME-типов и т.п.).

Исходные данные необходимы также для авторизации пользователей, которая производится на основании информации из разных источников данных:

- сервисов каталогов (LDAP);
- данных из доменов Windows NT (используя протокол NTLM);
- баз данных;
- пользовательских данных из обычных файлов.

Проверка прав доступа осуществляется по имени и паролю пользователя. Кроме того, доступ можно разграничить по IP-адресу компьютера.

Информация о ресурсах может быть получена из внешних источников (баз данных URL, файлов и т.п.).

Следует отметить, что все перечисленные списки не являются окончательными и должны

дополняться и модифицироваться по мере необходимости.

Рекомендации по выработке правил фильтрации

Общие рекомендации

При определении нового набора правил целесообразно предусмотреть оповещение по электронной почте администратора безопасности.

Создание правил фильтрации

При помощи консоли управления СКВТ «Дозор» создаются наборы правил, обеспечивающих контроль сеансов доступа к сети Интернет.

Применяются следующие правила фильтрации:

- контроль форматов загружаемых файлов;
- анализ текста на содержание определенных слов и выражений;
- ограничение доступа к веб-сервисам на основе URL;
- разграничение доступа к внешним интернет-ресурсам по группам пользователей.

Контроль форматов файлов

Контроль форматов проводится в несколько этапов, а именно:

- контроль расширений файлов;
- контроль MIME-типов передаваемых данных;
- контроль типов по сигнатурам файлов.

Контроль содержания текстов

Контроль содержания текстов включает в себя следующее:

- поиск по ключевым словам, с учетом весомых коэффициентов для разных слов;
- поиск по шаблонам (регулярные выражения);
- автоматическая категоризация ресурсов (например, бесплатных почтовых ящиков);
- антивирусная проверка.

При анализе текста автоматически определяется кодировка передаваемых данных и, если требуется, производится перекодирование русскоязычного текста в ту кодировку, в которой хранятся списки слов для проверки.

СКВТ «Дозор» позволяет использовать ключевые слова и выражения в следующих ситуациях:

- как признак для запрета передачи данных — «черный» список;
- как признак для разрешения передачи данных — «белый» список.

Следует отметить, что при использовании «черных» списков слова могут обрабатываться двумя способами: либо наличие запрещенного слова сразу запрещает передачу данных, либо передача запрещается при наличии сочетания слов, веса которых складываются, и полученный результат служит признаком запрета передачи данных. Именно использование блокировки доступа по результатам подсчета весов слов является наиболее эффективным способом блокировки доступа пользователей к серверам, реализующим функции работы с почтой (сервисами бесплатной почты).

Кроме этого, СКВТ «Дозор» может сравнивать получаемые данные с образцом, который автоматически создан в результате сравнения «плохих» и «хороших» сайтов. При анализе «плохих» сайтов специальная утилита извлекает из страниц ключевые слова и выражения, отсутствующие на «хороших» сайтах, а затем эта информация может использоваться для анализа страниц, проходящих через систему контроля веб-трафика.

Ограничение доступа к веб-сервисам на основе URL

Адреса для контроля могут браться из различных источников — это и адреса, распространяемые компанией «Инфосистемы Джет» в составе дистрибутива, и адреса, формируемые на основе поиска в Интернете через сравнение передаваемых данных с заранее подготовленным образцом. Адреса проверяются для всех запросов, в том числе и для тех, адреса которых передаются при использовании команды CONNECT протокола (правда, в этом случае можно ограничить доступ только ко всему сайту, а не к его части). При работе с серверами, не использующими протокол HTTPS, можно запрещать или разрешать доступ как ко всему сайту, так и к его частям, поскольку существуют порталы, предлагающие разные сервисы, в том числе и бесплатные почтовые ящики, доступ к которым необходимо запретить, оставив при этом доступ к остальным сервисам сайта.

Защита от вредоносных программ

Антивирусная проверка производится с использованием внешних антивирусных программ. В настоящее время поддерживаются «Антивирус Касперского» версии 4, Dr.Web, Sophos. Антивирусная поддержка оформлена в виде подгружаемых модулей, так что поддержка новых антивирусов может добавляться без переустановки всей подсистемы фильтрации.

НОВОСТИ

Новый программный комплекс для продуктов линейки «Дозор» компании «Инфосистемы Джет»

Контентная фильтрация предполагает анализ всех объектов, передаваемых при информационном обмене по каналам Интернет. Одним из таких объектов являются файлы. Для обеспечения эффективной защиты корпоративной инфраструктуры от современных угроз необходимо осуществлять качественный анализ передаваемых или загружаемых на стороне клиента файлов. Он должен предусматривать гарантированное определение типа файлов, что позволяет в дальнейшем без каких-либо сложностей их разобрать, проанализировать и принять решение о блокировке или доставке адресату.

С учетом этого обстоятельства в компании «Инфосистемы Джет» создан новый программный комплекс для определения типов файлов. Он используется в продуктах:

- система мониторинга и архивирования почтовых сообщений «Дозор-Джет»;
- система контроля веб-трафика «Дозор».

Данный комплекс позволяет:

1. Повысить эффективность системы и избежать ошибок при определении типов файлов за счет:
   - более корректной работы в русскоязычных кодировках;
   - использования одной базы условий для выдачи как текстового описания типа, так и MIME-типа, что гарантирует от ошибок при ведении двух аналогичных баз данных.
2. Описывать более сложные условия определения типов данных:
   - проверка значений (байты, строки, целые числа) по заданным смещениям с помощью условий <,>,= и их сочетаний;
   - вычисление значений и смещений с использованием арифметических и битовых операций, что позволяет применять косвенную адресацию данных;
   - проверка размера файла;
   - комбинирование условий проверки с помощью логических операторов;
   - использование условных операторов для проверки конкретных значений;
   - уточнение типов с помощью модулей расширения.
3. Расширять функциональность систем с помощью специальных модулей:
   - модуль определения текстов и методов их кодирования (ASCII, EBCDIC); очень важен, поскольку для текстовых файлов не существует сигнатур, по которым можно определять типы;
   - модуль определения исполняемых файлов MS-DOS – .com-файлы; для таких файлов также не существует стандартных сигнатур, поэтому детальный анализ их содержимого необходим;
   - модуль определения главного типа OLE-контейнера – MS Visio, MS Project, MS Word, MS Excel, MS Powerpoint.

Система определения типов для Cerberus for Lotus Notes

В качестве технического обеспечения документооборота российские предприятия и организации используют продукты компании Lotus Notes. В их состав, как правило, входит ПО ND. Cerberus производства ASENSYS GmbH, которое позволяет осуществлять анализ почтовых сообщений, передаваемых внутри организации. Данный продукт позволяет управлять почтовым потоком, ограничивать размер сообщений, выполнять антивирусную проверку писем и др. Недостаток этого решения – слабая система определения типов передаваемых в сообщениях данных.

Специалисты компании «Инфосистемы Джет» создали систему определения типов для ПО Cerberus for Lotus Notes, предназначеную для определения типов данных и обработки файлов. Она значительно расширяет спектр функций Cerberus. Этот программный комплекс создан на базе новой системы определения типов файлов, разработанной для продуктов контентной фильтрации линейки «Дозор» – системы мониторинга и архивирования почтовых сообщений и системы контроля веб-трафика.

Чтобы избежать проблем при определении типов данных в компании «Инфосистемы Джет» разработан программный комплекс, позволяющий точно определять тип передаваемых данных и принимать решение о запрете или разрешении передачи сообщения. При интеграции с Cerberus данный комплекс управляется конфигурационными файлами, в которых перечислены разрешенные MIME-типы, а также могут указываться программы-обработчики, выполняющие извлечение текста, распаковку архивов и пр. Программы корректно обрабатывают файлы, закрытые паролем, файлы с нарушенной структурой и позволяют передать полученную в результате обработки файлов информацию в Cerberus, который и выполняет блокировку или передачу сообщения.

Данная технология предоставляет в распоряжение администраторов безопасности мощный инструмент, обеспечивающий повышение качества работы системы Cerberus. Применение успешно функционирующей системы определения типов файлов в качестве основы для последующих разработок свидетельствует о существенных резервах технологий, используемых в продуктах компании «Инфосистемы Джет».

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

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Лапина И.К. *(lapina@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**