СРЕДСТВА ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ АНТИВИРУСОМ CLAMAV В КОРПОРАТИВНОЙ СРЕДЕ

А.С. Гаврилов, В.П. Петлинский

Электронная почта в настоящее время является привычным для множества людей способом обмена информацией. Она в состоянии обеспечить нужную оперативность и надежность для деловой или частной переписки. Основная проблема, связанная с использованием электронной почты - это вирусы и спам, доля которых в почтовом трафике достигает на сегодня 85% и постоянно растет. Связано это с тем, что рассылка спама и вирусов - это сложившийся бизнес со своей инфраструктурой, обслуживающими компаниями и клиентской базой. Методы, применяемые для их распространения, разнообразны и постоянно совершенствуются. На сегодняшний день основная часть вредоносного кода(приблизительно три четверти) доставляется с помощью пользовательских компьютеров, зараженных вирусами, владельцы которых ничего не подозревают. Количество таких "зомби", используемых для ретрансляции спама и вирусов, измеряется сотнями тысяч. С другой стороны, одним из основных каналов распространения вирусов является массовая рассылка сообщений с зараженными вложениями. Эпидемии почтовых червей достигли потрясающих масштабов. Например, в разгар эпидемии MyDoom, число зараженных систем достигало 500000, и каждое двенадцатое письмо содержало этот вирус. Для борьбы с ними используют разные антивирусные комплексы, в том числе и антивирусный пакет Clam AntiVirus. Например, он используется в корпоративной сети НИИАР для защиты почты и прокси трафика [1]. Растёт потребность в его использовании и для защиты клиентских компьютеров, в связи с ростом популярности ОС семейства Unix (различные клоны Linux, FreeBSD).

На данный момент процент обнаружения вирусов разными антивирусами примерно одинаков. Отличаются антивирусы в основном ценой и ресурсами, используемыми во время работы. С точки зрения надёжности обнаружения и технологии использования антивирусных пакетов немалаважное, а зачастую и определяющее значение имеют развитие обслуживающей и поддерживающей инфраструктур, обеспечивающих легкость управления и наблюдения за состоянием антивирусных средств в масштабах всей корпоративной сети. В пакете Clam AntiVirus - впечатляет легкость интеграции с серверами электронной почты для проверки почтового трафика. В пакет включены: масштабируемый многопоточный демон - clamd, управляемый из командной строки сканер - clamc, демон обновления сигнатур из Интернет-репозитария – freshclam, а также демон, обеспечивающий взаимодействие через milter-интерфейс между clamd и агентом пересылки почты (агент MTA), там где это надо, - clam-milter[2]. Выделим основные преимущества ClamAV:

- бесплатность;
- возможность использования с большинством почтовых серверов, включая реализацию milter-интерфейса для Sendmail;
- сканер в виде библиотеки Си;
- сканирование файлов и почты "на лету", высокая скорость сканирования;
- распределенная структура центрального репозитория антивирусных баз;
- определение свыше 100 000 вирусов, червей, троянов, сообщений фишинга;
- анализ сжатых файлов RAR (2.0, 3.0), Zip, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM (сжатый HTML) и MS SZDD;
- поддержка сканирования mbox, Maildir и "сырых" почтовых файлов;
- анализ файлов формата Portable Executable, упакованных UPX, FSG или Petite.

К недостаткам ClamAV следует отнести отсутствие программного комплекса для централизованного управления "сетью" антивирусов и ведения локального репозитория антивирусных баз, так называемого "Центра управления". Необходимо отметить, что в большинстве коммерческих продуктов этого класса такая возможность уже реализована. По этой причине нами было принято решение создать такие средства собственными силами.

Центр управления имеет клиент-серверную архитектуру и включает в себя ряд модулей:

- Клиентскую часть центра (реализована на языке С).
- Серверную часть центра (реализована на языках С и интерпретатора bash).
- Модуль информирования (реализован на PHP, имеет web-интерфейс администратора и пользователя).

- Подсистему обновления антивирусных баз из локального репозитория (реализована на языке интерпретатора bash).

Клиентская часть центра выполняет сбор информации о работе модулей Clamav на отдельных узлах сети (их целостности и работоспособности, результатах плановых антивирусных сканирований, on-line сканировании сетевых потоков, версиях пакета и антивирусных баз и датах их обновлений и т.п.) и передачу её на сервер. Серверная часть центра выполняет накопление полученной информации в общей базе данных для выдачи отчётов администратору по запросу, а также выполняет оперативное оповещение администратора в случаях повышения вирусной активности. Модуль информирования обеспечивет интерфейс администратора для выдачи отчётов и оперативного управления(например, рестарт антивируса на нужном узле). Этот молуль имеет также интерфейс для пользователя на любом узле корпоративной сети, на котором пакет Clamav может быть вовсе не установлен, - он обеспечивает возможность проверки подозрительных файлов по заявке пользователя через сеть.

Более подробно рассмотрим подсистему обновления антивирусных баз, в функции которой входит ведение локального репозитория антивирусных баз, их обновление и контроль версий антивирусных программ. Вначале рассмотрим стандартный механизм обновлений антивирусных баз (см.схему на Рис.1).

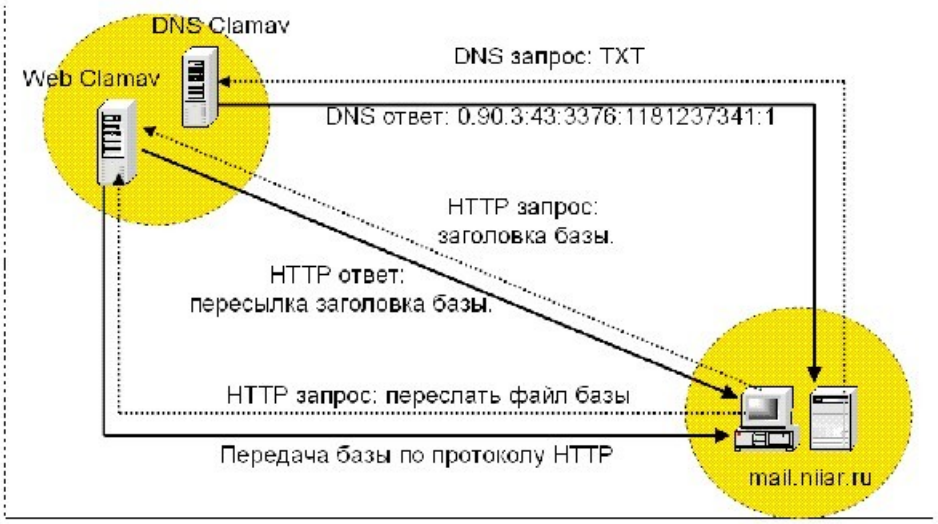

Рис. 1. Стандартный механизм обновлений антивирусных баз

Стандартно процесс обновления состоит из трех этапов. На первом этапе демон обновлений - freshclam (программа, осуществляющая периодические обновления базы антивирусов может запускаться и не в режиме демона, по cron) запрашивает запись типа TXT из DNS-базы current.cvd.clamav.net, в которой хранится номер текущей версии антивируса, номер версии антивирусной базы, времени создания записи. Если номер версии базы в полученной записи больше номера версии имеющейся базы, процесс обновления продолжается. На втором этапе следует запрос по протоколу HTTP на получение заголовка базы. В нём содержатся версия базы, даты выхода, сигнатура базы и дополнительная служебная информация. Основная цель этого этапа - подтверждение факта выхода новой версии базы. Если подтверждение получено, демон обновлений переходит к заключительному этапу обновления - загрузке базы из центрального репозитория Clamav. Репозиторий имеет распределенную структуру и тем самым обеспечивает более высокий уровень отказоустойчивости за счёт резервирования. После того как базы загружены, процесс обновления считается завершенным. В других антивирусных продуктах (Nod32, Symantec, DrWeb и т.д.) процесс обновления состоит только из двух последних этапов. Такая реализация обеспечивает более высокую степень доступности центрального репозитория Clamav, как в силу распределенного характера хранения самих файловых хранилищ, так и в силу распределенного характера базы данных DNS (репликация выполняется примерно на 30 узлов в интернет).

Механизм обновления баз из локального репозитория, реализованный нами, приведен ниже (см.схему на Рис.2).

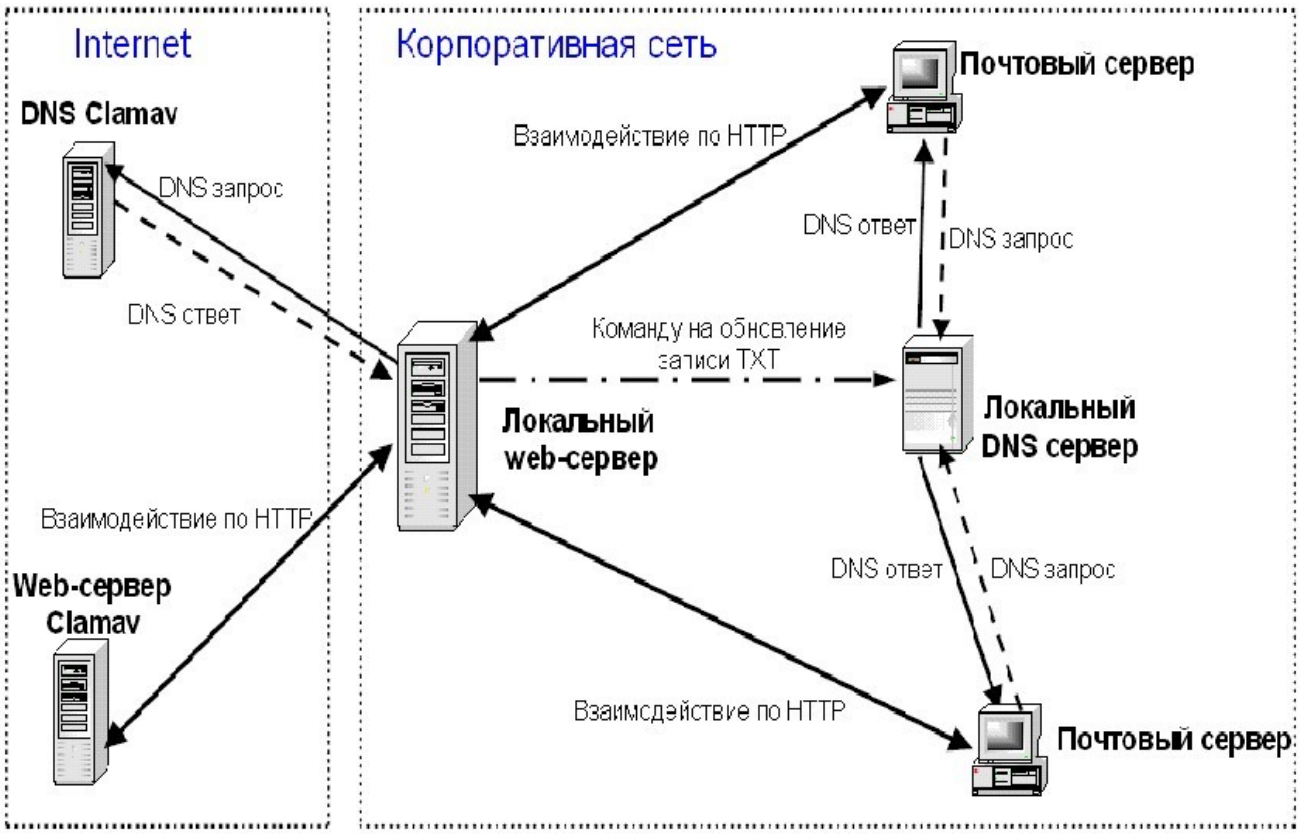

Рис. 2. Подсистема обновлений из локального репозитория

Для функционирования данной системы необходимы локальный Web-сервер (выполняет функции локального репозитория антивирусных баз), и локальные DNS-серверы, настроенные следующим образом. На локальном DNS-сервере заводится специальная служебная зона (в нашем случае clamav.niiar.ru). Для нее создается запись TXT, в которой будет храниться строка, аналогичная находящейся в базе DNS Clamav - current.cvd.clamav.net (в нашем случае current.clamav.niiar.ru). Также нужно настроить эту зону для выполнения динамических обновлений. На Web-сервер установливается и демон обновлений - freshclam. Он настраивается таким образои, чтобы обновления баз Clamav из центрального репозитория Clamav загружались в корневую директорию нашего Web-сервера. После успешного обновления локального репозитория синхронно на нём запускается программа, динамически обновляющая TXT запись current.clamav.niiar.ru локального DNS-сервере. Демоны обновления на остальных узлах сети настраиваются таким образом, что DNS-запросы отправляются на локальный DNS-сервер, а базы загружаются с локального Web-сервера. Отметим, что настройка на локальный DNS-сервер в freshclam уже предусмотрена, но она подразумевает несколько другой смысл. По задумке авторов пакета предполагается, что это публичный DNS сервер Clamav, например, для региона - Россия. Наша реализация экономит трафик от использования данной системы пропорционально числу узлов в сети, которым необходимы обновления базы. Главное же преимущество данной схемы, на наш взгляд, заключается в том, что позволяет обновлять базы на тех узлах корпоративной сети, на которых по определенным причинам, обычно оговариваемым в политике безопасности организации, не допускается выход в интернет.

При разработке центра нами учитывались вопросы безопасности. Для обеспечения безопасности функционирования применяются следующие средства:

- Использование протокола SSL для безопасного прохождения www-трафика при передаче данных по протоколу HTTPS.
- Base-аутентификация Web-сервера при работе с Web-интерфейсом.
- Использование парольной аутентификации в процессе взаимодействия клиентской и серверной частей центра управления.
- Использование электронной цифровой подписи при обновлении записи TXT локального DNS-сервера.

Рассмотренные в данной работе средства находятся в промышленной эксплуатации с начала 2007г. и в основном удовлетворяют поставленным целям разработки. Авторы полагают, что вследствие возрастающего в последнее время интереса к open-source продуктам во всём мире, в том числе и в России, опыт и практика применения таких продуктов и их интеграции в существующие корпоративные IT-технологии могут быть полезными и другим организациям.

ЛИТЕРАТУРА:

1. Петлинский В.П. Использование открытого антивирусного пакета "Clamav" в целях защиты корпоративной сети ГНЦ РФ НИИАР. Научный сервис в сети Интернет – 2005, Изд-во МГУ, 2005.288 с.
2. Ресурс Интернета, http://www.clamav.org